Faculty of Science and Technology

MASTER'S THESIS

Study program/Specialization: M.Sc. in Offshore Technology/Risk Management Specialization	Spring semester, 2016 Open / Restricted access
Writer: Jesse Ebubechukwu Inoma	………………………………………… (Writer's signature)
Faculty supervisor: Eirik Bjorheim Abrahamsen	
Thesis title: **Assessing Stochastic and Intelligent Threats in the Norwegian Petroleum Industry, Current approach(s) and enhancement with Game Theory influenced Risk Assessment Approach (GIRA)**	
Credits (ECTS): 30	
Key words: Threats, Intelligent threats, Stochastic threats, game theory	Pages: 66 + enclosure: Appendix Date/year: Stavanger, 15th of June 2016.

ABSTRACT

In the Norwegian petroleum industry quantitative risk assessments QRA’s are carried out to assess risk as well as for accounting for uncertainties given the strength of background knowledge available to the assessors. The NORSOK Z-013 standard is used as a guideline for doing this in practice. This thesis focuses on enhancing the current quantitative risk assessment approach being used in the industry by combining it with the game theory. It is from this synergy that a new approach termed ‘GIRA’ game theory influenced risk assessment was suggested in this research work. As the boundaries for innovation are pushed in the industry, likewise are the threats from petroleum activities increasing. These threats can be stochastic or intelligent in nature, because of this increase in risk there needs to be improvement in the methodology to unravel these threats. The GIRA approach provides the necessary robustness to combat the increasing complex nature of threats facing the industry. Previous research has been carried out in this field by notable researcher’s such as Vicki Bier and Terje Aven. Vicki Bier suggests a strategy for allocating resources efficiently in combating intelligent threats. Also, the research work carried out by Prof. Aven in the correct use of QRA’s in the industry is exemplary. However, there exist some gaps in these researches, the work done by Bier is a justification for investment to combat intelligent threats such as terrorism and does not cover much about stochastic threats. As for the research work done by Prof Aven, with the increase in the threat level exposure in the industry there is need to see the limitations of a QRA, hence why it should be improved upon. The GIRA approach is a strategy that will be able to address the limitations of the QRA because of the two-step analyses process, first by a QRA then analysis of the QRA result with the GIRA approach. A case study about an ignited process leak was carried out to show how the GIRA approach will be used in practice.

It is believed that by applying the GIRA approach extensively in the Norwegian petroleum industry, a more robust analysis will be available to present a complete picture of risk from intelligent and stochastic threats to decision makers.

PREFACE

The safety records on the Norwegian Continental Shelf has been a benchmark in the oil and gas industry for the last 20 years. This was not always the case, especially in the early years of petroleum discovery and production on the NCS. There was a considerable amount of accidents with casualties during the early years, the Alexander Kielland accident with 123 casualties being the most significant. However, conscious efforts were implemented by the Norwegian Petroleum Directorate (NPD) to prevent any reoccurrence of events of this magnitude and it can be said that the measures implemented by the NPD and later the Petroleum Safety Authority (PSA) have been successful.

In the early 2000's the annual NPD report showed that there was a reverse in the positive trend of safety in the petroleum industry. This report was published 3 years after the Brønnøysund helicopter accident which was the last major accident on the NCS at the time (PSA, 2014). This warning was a precursor for the industry to make changes to prevent any major accident occurrences. Between 2015-2016 there has been two accidents with fatalities on the NCS. The first occurred on the 30th of December during a shutdown and evacuation operation for the COSL Innovator due to bad weather. A massive wave hit the platform and shattered the windows of the living quarters, there was one casualty from this accident and it was the first accident on the NCS since 2009. Also, on the 29th of April there was a helicopter accident with 13 casualties in Fjell when the helicopter was carrying personnel from the Gullfaks B platform to Bergen. This is a worrying trend, considering the successes that had been attained prior to these accidents resulting in 14 casualties. These events are treated as part of a systemic problem termed as a **'rising tide'** in this thesis. The objective of this thesis is to examine this **'rising tide'** by evaluating stochastic and intelligent threats in the petroleum industry, modelling methods and improvements to these methods.

This master thesis is submitted as part of the requirements for being awarded a master's degree the University of Stavanger. It is time constrained assignment with 30 Ects for the Offshore Technology Risk Management specialization degree.

Working on this thesis has been very demanding and challenging for me. From the research I carried out during the course of this thesis, I have been able to grasp the big picture on the safety success of the Norwegian Petroleum Industry. I express my sincere appreciation to my friends and colleagues for their input and support while writing this thesis. I also want to thank my faculty supervisor Professor Eirik B. Abrahamsen for his guidance and counsel.

Lastly, I will like to dedicate this thesis to my late father Obi Inoma, who provided me with motivation to strive on and finish this research work.

Stavanger, June 15, 2016
Jesse Inoma

Table of Contents

Contents

TABLE OF FIGURES

ABBREVIATIONS

- NCS…………Norwegian Continental Shelf
- NPD…………Norwegian Petroleum Directorate
- PSA…………. Petroleum Safety Authority
- QRA…………Quantitative Risk Assessment
- HTO…………Human Technology Organization
- COSL………. Chinese Oilfield Services Limited
- SCADA……. Supervisory Control and Data Acquisition
- PST………….Norwegian Police Security Services
- NSM…………Norwegian National Security Authority
- PRA…………Probability Risk Analysis
- GIRA………. Game theory influenced Risk Assessment
- SoK…………. Strength of Knowledge
- NORSOK……Norsk Sokkels Konkurranseposisjon
- HAZID………Hazard Identification
- KPI…………. Key Performance Indicators
- WIF…………Well Integrity Forum
- FAR…………. Fatal Accident Rate
- IOGP…………International Oil and Gas Producers
- BORA………. Barrier and Operability Risk Analysis
- OMT…………Organization Man Technology
- FMECA……. Failure Modes, Effects and Criticality Analysis
- FTA…………Fault Tree Analysis
- CFD…………Computational Flow Dynamics

CHAPTER ONE: INTRODUCTION

1.1 Background

Oil production started on the Norwegian Continental Shelf in 1965 and from this time onwards the offshore oil and gas industry has been in constant exposure to risk ranging from activities in exploration, production and abandonment stages of the petroleum sector. The Alexander Kielland flotel capsize which occurred in 1980 was the first major fatal accident on the NCS with 123 casualties. This tragedy was a rude shock to the petroleum industry regulator (Norwegian Ministry of Petroleum) at the time and conscious efforts were made to improve understanding of the offshore petroleum activities with emphasis on properly capturing the risk picture in order to improve safety of operations. There has been significant improvement in strengthening of knowledge about petroleum activities, thereby enhancing decision making in view of the complex interactions from a HTO perspective and making barriers more robust and resilient in order to successfully manage the risk involved in petroleum activities offshore. It can be said that there has been significant success when making reference to trends and indicators in safety on the Norwegian Continental Shelf. However, there are still isolated incidents that occur from time to time. The accident on the COSL innovator which occurred on December 29th 2015 can be referred to as one of those incidents. According to the accident report provided by the PSA 'around 5 p.m. local time companies operating in the Norwegian Continental Shelf were informed about the impending stormy weather. This information was meant to provide operators and rig owners with adequate time to shut down operations and prepare for immediate evacuation. During an evacuation operation at the Troll field, a giant wave about 16- 17 meters hit the COSL (China Oilfield Services Limited) Innovator semi-submersible drilling rig which was operating in the Troll gas field under contract from Statoil. The resulting impact of the wave led to severe injuries for 2 personnel with one fatality during transportation to shore, there were also significant damages to the accommodation module'. The last time an accident with a fatality occurred on the Norwegian Continental Shelf was in 2009, making this accident of keen interest to the PSA and other relevant Petroleum activity regulatory organizations on the Norwegian Continental Shelf.(PSA, 2015). Also, on the 29th of April a helicopter transporting personnel from Gullfaks B to Bergen crashed at Turøy and killed all 13 personnel onboard. These two accidents are quite shocking considering the almost perfect record that existed for the past decade on the NCS.
However, there was a warning about this in an annual report published by the NPD in 2000, where it was outlined that efforts promoting safety were reversing in the negative direction. These two accidents will be viewed as examples of stochastic threats in this thesis.

There are not too many examples of sabotage in the petroleum industry on the NCS, the best examples being the 2014 curtailed cyberattacks on some major companies such as Statoil. Hackers going by names 'Energetic Bear' and 'Dragonfly' used an intrusive virus with the aims of industrial espionage as well as gaining control of SCADA industrial control systems in the petroleum industry. It is because of these incidents that a robust posture of continuous improvement has to be adopted by the PSA to maintain Norway as the foremost leader in petroleum safety. There have been several researches done in subject areas relating to threats from intentional acts such as sabotage and stochastic threats such as natural disasters (Aven, 2007; Jun

& Bier,2007) looked into the use of game theory to model attacker and defender strategies considering the model to be endogenous when describing the behaviors of both the attacker and defender. Their research was quite interesting looking at the sequential game they presented, where there is a continual improvement on the part of the attacker and defender to maximize their utilities. Another interesting article closely related to this subject area was done by (Aven & Renn, 2009), in this article Aven and Renn look into the use of QRA's (quantitative risk assessments) in describing risk, uncertainty and describing the risk management options that should be taken when encountering scenarios where there are large consequences and uncertainties as can be seen risk from sabotage. In this article they proposed the use of a qualitative uncertainty assessment and scenario building instruments when encountering such scenarios.

In this thesis, the literature and discussions will be on establishing the key differences between intelligent threats and stochastic threats in the petroleum industry as well as presenting their unique differences from a risk analysis perspective. The standard methods useful for analyzing both types of threats will be treated and compared while methods useful for treating each threat uniquely will also be presented and discussed. Also, the use of probability as a measure of uncertainty for intentional acts will be reviewed critically. The above mentioned papers by Zhuang et al and Terje Aven et al have key similarities with this topic and will provide a useful foundation upon which key issues will be presented in the literature review. The scope of this thesis will be limited to the intelligent and stochastic threats in the petroleum industry and not the Norwegian society as a whole. It is important to understand the key differences in these above mentioned threats and methods which can be implemented to reduce or combat these threats. With a thorough understanding of intelligent and stochastic threats in the petroleum industry, a risk analyst will be able to analyze these threats effectively with an integrated approach which will give a good overview of the risk picture when presenting findings to decision makers.

A threat is a scenario that cannot be controlled, but can be identified and the occurrence of such scenarios can be modelled using various methods such as probability risk analysis, game theory, Bayesian belief networks etc. It is important for the risk analyst to clearly state the level of uncertainty and to display that the analysis should go beyond the numbers or assumptions, only by doing this will it be possible for an informed decision to be made by decision makers.

Intelligent threats such as terrorist attacks or sabotage involve a high level of adaptability by the individual or medium through which these attacks are carried out. The probability of initiating events of intelligent threats depends largely on the risk management actions taken to mitigate such scenarios. They are more difficult to assess when compared to stochastic threats because of the high degree of epistemic uncertainty based on the attacker or saboteur's motivation or future behavior (Guikema & Aven, 2010).

Stochastic threats are characterized as having a high degree of randomness. The keywords that can be used in differentiating between intelligent threats and stochastic threats are uncertainty, ambiguity, modelling methods, intent &motivations and media (such as intelligent systems like software's, robots) etc. through which the attacks are carried out. The intent seen in intelligent threats has already been mentioned, as—– for the media used to carry out intelligent attacks, one can refer to cases of cyber terrorism, and economic warfare as key examples, they rely largely on human input to be implemented, meanwhile in the case of stochastic threats the chief sources of such threats can be found in technical failures from human errors, natural hazards or force majeure which refers to events beyond human control.

For the purpose of this research, the differences between intentional threats and stochastic threats will be identified and the approaches unique to analyzing each threat will be elaborated on. The following methods have been found to be suitable in analyzing intelligent threats: (1) Game theory, (2) Probabilistic risk analysis, (3) Semi quantitative risk analysis approach where uncertainties are accounted for and are assigned probabilities and (4) Allocation of resources to safeguarding the highest value targets

It should be noted that probabilistic risk analysis is useful in assessing both intelligent and stochastic threats while the other above mentioned methods are unique for analyzing intelligent threats. The key question is; what extent should probability be used as a measure of uncertainty for intentional acts? The use of probability to account for intelligent threats is limited and is based on the background knowledge from which the data is derived (Aven, 2013). It is paramount for a qualitative approach to be adopted where uncertainties about the data and strength of background knowledge are stated clearly. The other above mentioned methods take into account the high level of adaptability and commitment an attacker possesses in trying to overcome barriers set to counter intelligent threats, this will be discussed in detail in the next chapter.

1.2 Problem statement

As stated earlier, this master thesis will focus on intelligent and stochastic threats in the Norwegian petroleum industry. In order to fully understand what intelligent and stochastic threats in the petroleum industry are; the key differences between them will be shown. Also, the uniqueness between these threats from a risk analysis perspective will be sought out, with a keen focus on the standard methods useful in analyzing each of these threats.

Finally, the extent probability is applicable as a measure of uncertainty for intentional acts such as sabotage will be analyzed.

1.3 Aims & Objectives

Firstly, identification and discussion of key differences between intelligent threats (cyberterrorism, sabotage, etc) and stochastic threats (natural hazards, technical failures etc) in the Norwegian petroleum industry.

Furthermore, identification of differences between intelligent threats and stochastic threats from a risk analysis perspective. Also, identification of standard methods which are useful for analyzing intelligent threats and stochastic threats.

Finally, identification of what extent probability is applicable as a measure of uncertainty for intentional acts.

1.4 Scope

The scope of this thesis will aim to cover the key differences between intelligent threats and stochastic threats in the Norwegian petroleum industry, their differences from a risk analysis perspective will also be identified. The standard methods which can be useful for analyzing intelligent threats and stochastic threats will be identified taking note of the underlying principles in each approach. This thesis will show the extent that probability is applicable as a measure of uncertainty for intentional acts (intelligent threats).

1.5 Thesis Structure

The thesis will be structured with the aim of providing a good foundation about the underlying principles and theories that must be understood by students and researchers with keen interest in this field. This literature review will be the foundation upon which key argumentation and discussions will be based on in the further chapters and will make it possible to arrive at a valid and well-founded conclusion about the problems to be treated in this thesis

CHAPTER TWO: LITERATURE REVIEW

2.1 What is a Threat?

According to Merriam-Webster's dictionary a threat is defined "as an expression of intention to inflict evil, injury, or damage", "it is also an indication of something impending".

From a risk analysis perspective, a threat can be defined as a potential intent to inflict harm or damage to a system by severely altering its state (John Garrick et al., 2004). Generally, a threat involves an initiating event that can cause damage to a system or cause it to lose its functions and fail (Haimes Y.Y,2010). From the above definitions we can see a situation of a system functioning optimally, then its function impaired by virtue of a threat (intelligent or stochastic). The level of impairment suffered by the system can vary and this depends on the expected consequences of such a threat.

In the case of an intelligent threat, the following classification below by the Norwegian Police Security Service (PST) into four defined category levels is a useful guideline.

1. Low: The likelihood of an attack is low. One or more parties may have the intention of, but are not thought to have the capacity to strike at specific interests.
2. Moderate: The likelihood of an attack is moderate. One or more parties may have the intention of and capacity to strike at specific interests.
3. High: The likelihood of an attack is significant. One or more parties have the intention and capacity to strike at specific interests. There is an unspecified threat
4. Extreme: The likelihood of an attack is extremely high. One or more parties have the intention to strike at specific interests. There is a specific threat. No further warnings are to be expected before a strike is carried out.

A similar classification system is used in categorizing stochastic threats in the Norwegian Petroleum Industry with the strength of knowledge providing a useful reference for this classification.

In order to further understand what threats are? The classification system suggested by Klinke and Renn IRGC and Renn and Walker where they put 'risk problems' into categories based on their complexity, uncertainty and ambiguity will be useful. It should be noted that 'threats' are special types of 'risk problems'. A brief overview on the classification by Renn and Walker is as follows:

1. Complexity: Threats will be viewed from their level of linearity until when they become complex. In the case of linear threats there exists low complexity and there is little ambiguity and uncertainty with respect to such threats. Examples of threats that can be considered to be linear in nature include car accidents, regularly occurring natural disasters like typhoons and hurricanes. It is important to state the point that simplicity of the threat does not mean that the risks are low rather the uncertainties about the consequences of the event are relatively low making it easy to determine to a high degree of accuracy what these consequences will be. As threats become complex there is

difficulty when looking at the cause and effect of such threats. This is because of the complex interrelationships which exist between each causal agent such as; (synergism and antagonism), long delay periods between cause and effect, inter-individual variation, intervening variables, and others. Examples of such scenarios or systems that exhibit this level of complexity are sophisticated chemical plants and structures with a lot of interconnectivity like cross border railways (Klinke A; G. P. Renn O; W. K. Renn O, 2007).

2. Uncertainty: This is the difficulty involved in predicting the occurrence of an event and the consequences of such an event because of the lack of background knowledge about such a phenomena or occurrence. Such gaps that can lead to this lack of knowledge which arises in uncertainty, include incomplete databases and models. This discourse would not be complete without the mention of black swans. According to Taleb "a black swan refers to the inability to predict outliers (black swans), implies the inability to predict the course of history. An outlier lies outside the realm of regular expectations because nothing in the past can convincingly point at its occurrence". A black swan can also be defined as a surprising, extreme event relative to the present knowledge/beliefs (Aven, 2013). By referring to Terje Aven's Black Swans classification, there are three types of blacks swans which are as follows:
    - Known knowns: This refers to events that are known but the probability of occurrence is judged to be low and because of this they are not believed to occur.
    - Unknown knowns: This refers to events that were not considered when the QRA was carried out. They are unknown to the analyst but are known by the perpetuators for example cybercrime or a terrorist attack. It should be noted such events can be uncovered with a more thorough QRA.
    - Unknown unknowns: This refers to events that are completely unknown to the scientific environment. Such events are extreme in their consequences and are considered unthinkable for example a new type of virus. To unmask such events, the knowledge gap needs to be addressed to lessen the level of uncertainties

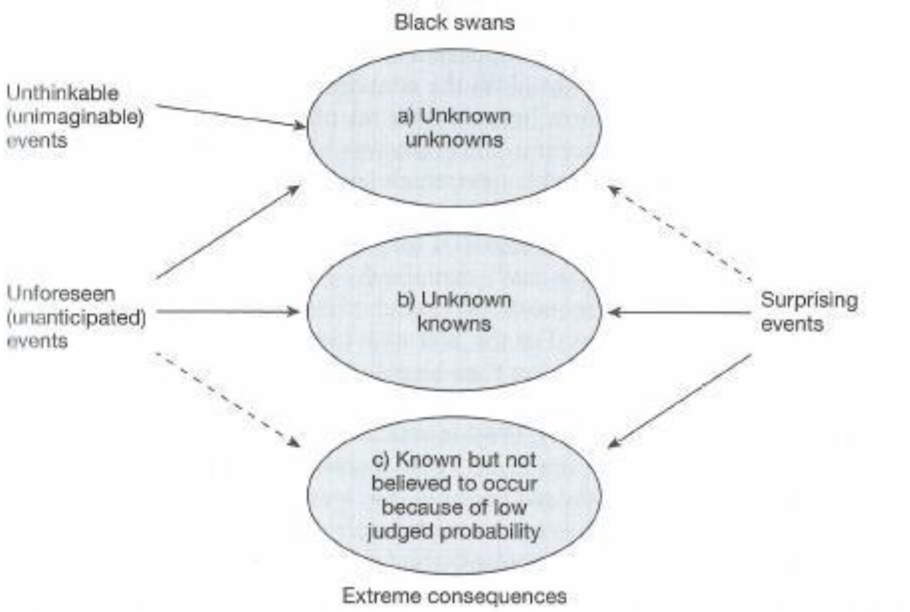

Black swans
Unthinkable (unimaginable) events
a) Unknown unknowns
Unforeseen (unanticipated) events
b) Unknown knowns
Surprising events
c) Known but not believed to occur because of low judged probability
Extreme consequences

Figure 1: Schematic representation of the concept of black swans: unknown unknowns, unforeseen events, surprising events and unthinkable events based on the ideas presented by Aven and Krohn (2014) and first presented in Aven (2013g)

Having covered this black swan concept, there is a better picture of the nature of uncertainties encountered when dealing with threats.

3. Ambiguity: There are two types of ambiguity in this context i.e. interpretative ambiguity and normative ambiguity.
   - Interpretative ambiguity with views pertaining to relevance, meaning and implications of the QRA for decision support.
   - Normative ambiguity with views pertaining to the values to be protected and the priorities to be made.

In general, ambiguity refers to the level of understanding of the threat based on the context in which it is being viewed from. Is it open to interpretation from different viewpoints? It covers aspects of the decision making like the allotment of resources in protecting valuable assets.

It can be seen in the discourse so far, that the classification of threats based on complexity, uncertainty and ambiguity is useful for an analyst in placing a threat in the right category.

2.1.1 Intelligent threats

Intelligent threats such as cyber-terrorist attacks or sabotage involve a high level of adaptability by the individual or medium through which these attacks are carried out. The probability for initiating events of an intelligent threat occurring depend largely on the risk management actions taken to mitigate such scenarios. They are more difficult to assess when compared to stochastic threats because of the high degree of epistemic uncertainty based on the attacker or saboteur’s motivation or future behavior (Guikema & Aven, 2010). Epistemic uncertainty refers to the uncertainty about knowledge on the part of the assessor. Intelligent threats are good examples of black swans and can be of the unknown knowns type i.e. it is unknown to the government protection agencies or petroleum companies, but known by the adversaries. However, it should be stated that not all intelligent threats are black swans. In order to uncover these threats, a quantitative risk assessment (QRA) needs to be carried out with the aim of addressing the knowledge gap (intelligence lag) and reduce the uncertainties.

In this context, risk is seen as uncertainty about the severity of consequences (outcomes) of an activity with respect to something humans value (Aven T, 2007). In a QRA, it is important to recognize the difference between risk agent (such as man, chemical or a technology) and the risk absorbing system (such as a building, an organism, or an ecosystem). When addressing complex structures of risk agents, the use of causal modeling or data analysis will be useful. In the case of risk absorbing systems, the emphasis is on vulnerability (IRGC, 2005). The extent to which the risk absorbing system reacts to the stress induced by the risk agent is called *vulnerability*. Following the same analogy as the risk definition, vulnerability is defined as uncertainty about the severity of the consequences given the stress induced by the risk agent for example a cyber-terrorist attack (Aven & Renn, 2009).

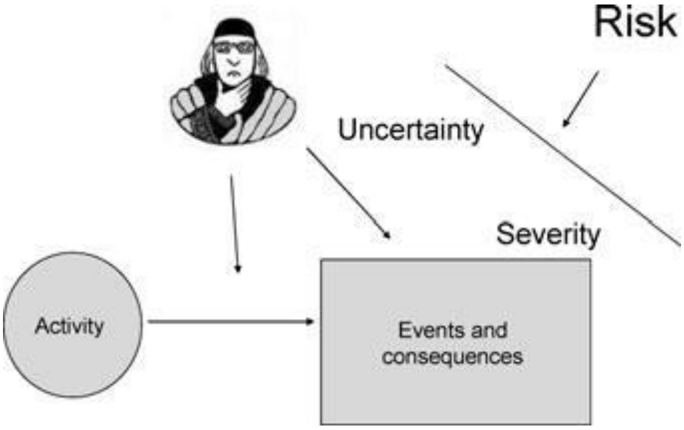


Figure 2 : Illustration of the risk definition employed in this thesis. (Aven & Renn, 2009)

When carrying out a QRA to identify intelligent threats, because of the high level of adaptability on the part of the adversary wherein he adapts to counter measures taken in order to maximize utility derived from perpetuating such an attack; there is a need to take into account vulnerability. Apart from the QRA which will be carried out to unearth the risks involved, a vulnerability analysis will also be undertaken to analyze the impact of the consequences of an intelligent threat (Aven, 2007).

To provide further understanding about this concept, a case study of an intelligent threat in the petroleum industry will be treated and key concepts elaborated on. The ‘Energetic Bear’ cyber-terrorist attack which occurred in the Norwegian Petroleum industry will provide some useful insights about intelligent threats.

2.1.1.1 Case Study: 2014 Curtailed *Energetic Bear* Cyber-attacks

On the 31st of August 2014, the Norwegian National Security Authority (NSM) gave a warning to 50 Oil and Gas companies that their systems had been jeopardized because of a serious cyber-attack. Further warning was given to an additional 250 companies as possible targets for further attacks. These attacks were the largest the oil and gas industry in Norway has ever been exposed to and they were carried out in a carefully well planned manner(Maxwell, October 6th 2014). According to Kaspersky, 'the cyber-terrorists aimed at specific functions within the oil companies and made use of 'Trojan back-doors' to extract information over an extended period'. They gained entry into the various company's networks via these three means: infected email attachments, 3rd party websites and business sites of suppliers.

Firstly, emails with infected attachments were spread with the attachments hidden with a layer of data which allowed them to install on the target machines and further contaminate the companies network.

Secondly, the occasional habits of employees at the affected companies were studied and poor 3rd party website security was taken advantage of. For instance, the website of a Chinese website was infected so that once an employee of an oil company downloads their menu they get the malware into their systems.

Finally, the cyber-terrorists made use of the business sites of suppliers the oil companies were dealing with. They infected driver and installation package updates that were needed for the SCADA devices, so once new updates were downloaded the SCADA devices were infected, thereby giving the cyber-terrorists access to them. This cyber-attack displayed the characteristics of an intelligent threat namely: the high level of complexity of motivations i.e. whether the attacks were an act of espionage or sabotage and the high level of epistemic uncertainty about such an event occurring because of its relative non-occurrence on the NCS from history.

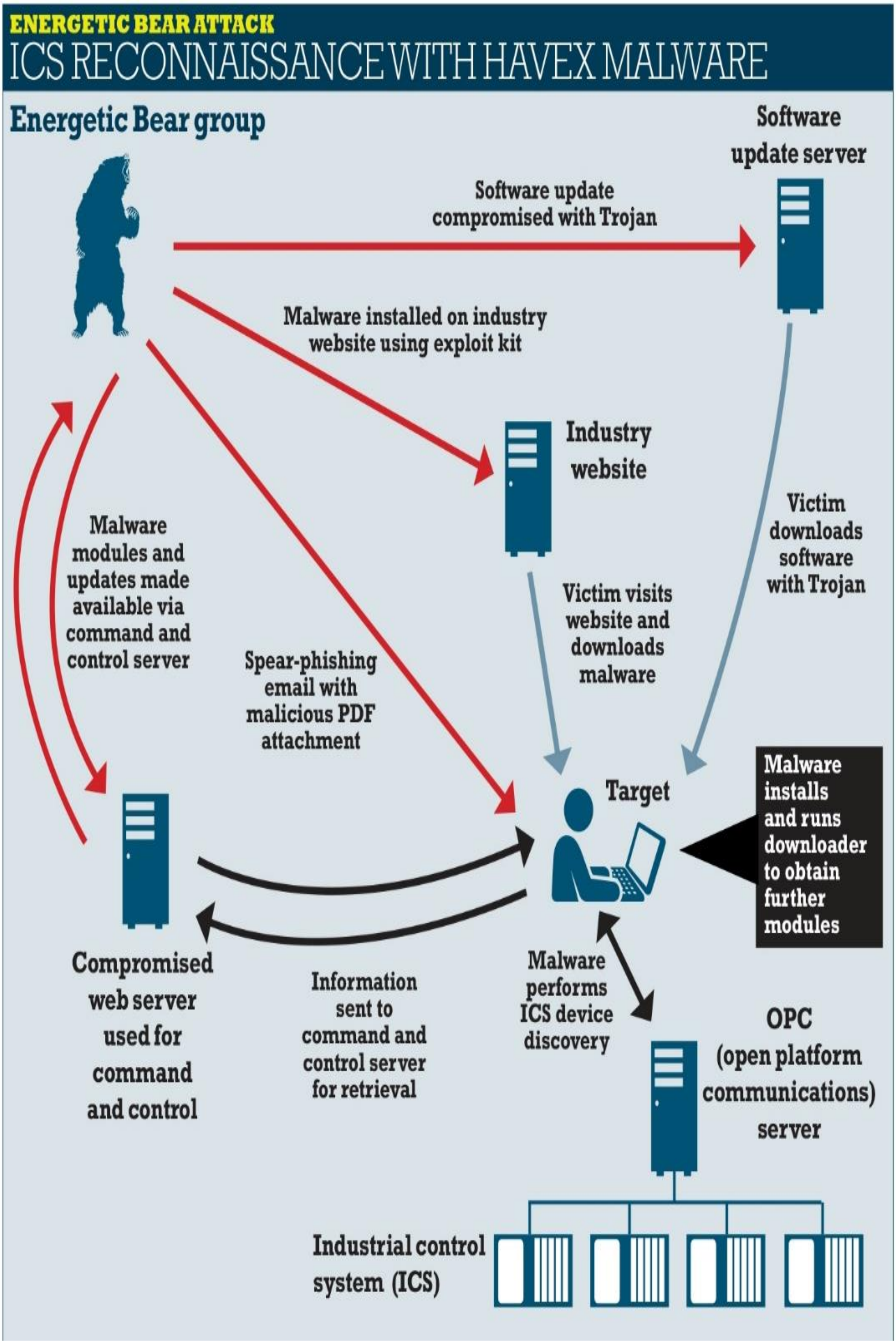

ENERGETIC BEAR ATTACK
ICS RECONNAISSANCE WITH HAVEX MALWARE
Energetic Bear group
Software update server
Software update compromised with Trojan
Malware installed on industry website using exploit kit
Industry website
Victim downloads software with Trojan
Malware modules and updates made available via command and control server
Victim visits website and downloads malware
Spear-phishing email with malicious PDF attachment
Target
Malware installs and runs downloader to obtain further modules
Compromised web server used for command and control
Information sent to command and control server for retrieval
Malware performs ICS device discovery
OPC (open platform communications) server
Industrial control system (ICS)

Figure 3: Showing how the Energetic Bear Cyber-Attack was carried out (Kaspersky Labs, 2014)

2.1.2 Stochastic threats

Stochastic threats are characterized as having a high degree of randomness i.e. there is an absence of a clear pattern or trend when trying to predict such threats. It should be clearly stated that although there is a high degree of randomness when treating such threats, it does not mean they cannot be predicted. It is just difficult to predict them because of uncertainty involved. The chief sources of such threats can be found in technical failures from human errors, natural hazards or force majeure which refers to events beyond human control. Drawing from the black swan metaphor, it should be stated that stochastic threats for example tsunami's, rogue waves etc are good examples of black swans (known knowns) type. These threats are known but the probability of occurrence is judged to be low and because of this they are not believed to occur. For this type of black swans, we assign a low subjective probability of occurrence based on our background knowledge and the large uncertainties that exist about the phenomena. And we address these type of threats by carrying out a QRA, which acts as a decision support tool to the decision makers on how to set up barriers to mitigate such threats.

2.1.2.1 Case Study: Fatal accident on COSL Innovator

This accident occurred during an emergency shutdown and evacuation operation that was initiated when companies operating in the Norwegian Continental Shelf were informed about the impending stormy weather. This information was meant to provide operators and rig owners with adequate time to shut down operations and prepare for immediate evacuation.

According to the accident report provided by the PSA, "at 4:38 p.m. local time, parts of the living quarters provided on the COSL innovator was struck by a giant wave 17meters in height from crest to trough. The facility was at this time disconnected from the well and thus raised the safety condition. The wave caused deformation of the frontal region of the living quarters and pressed into a total of 17 windows on the lower deck and between decks. Furthermore, water penetration led to the facility suffering extensive damage in staterooms and attached corridor area. There was one fatality and four people were bruised from the shattered windows during the wave impact.
If the incident had occurred at a time when several onboard stayed in cabins, there could have been more casualties"(PSA, 2015).

The PSA, also identified the following discrepancies as reasons why the accident occurred.

- COSL Innovator did not meet the air-gap/clearance requirements between the lower edge of the deck and the highest crest of wave which is 1.5 m.
- The semi-submersible platform was not dimensioned during its design to withstand horizontal wave loads.
- Counting system during patterning did not work satisfactorily.
- Proper quality bolts were not used for fixing windows.

This accident displayed the notable characteristic of randomness which is associated with stochastic threats and could have been avoided if the deficiencies identified in the PSA investigation were in place.

2.2 Differences between Intelligent and Stochastic Threats

In order to differentiate between intelligent threats and stochastic threats the following keywords and terms will be used: uncertainty, ambiguity, intent &motivations, modelling methods and media (such as intelligent systems like software’s, robots) etc. through which the attacks are carried out.

As mentioned in section 2.1 intelligent threats are in some cases good examples of black swans and can be of the known knowns or unknown knowns type. They are usually characterized by high uncertainty and normative ambiguity i.e. decisions on values to be protected and the priorities to be made on the part of the assessor. An overview of this difficulty was presented in the *Energetic Bear* cyber-terrorist attacks in section 2.1. This is not the same for stochastic threats, they are good examples of black swans of the known knowns type they also have large uncertainties, but because of their low subjective probability of occurrence based on the background knowledge we deem them to be acceptable.

By referring to ‘intent’, this covers areas such as the attackers’ utility functions; questions that typically arise here are: When to attack? Which targets to attack? And how much resources should be set aside for an attack? The final choice by an attacker will depend on factors such as how much the attacker values inflicting damage to various targets, the attacker’s level of resources and any other opportunities he has for use of those resources (Frey and Luechinger 2003). These questions are interrelated and pose significant complexity when trying to model motivations behind any attack. These complexity of attacker intent and utility choices is one key area that differentiates between intelligent threats and stochastic threats.

When carrying out an analysis to unearth intelligent threats, a QRA with a vulnerability analysis included are used. The use of game theory, probabilistic risk analysis, semi- quantitative risk analysis approach where uncertainties are accounted for and are assigned probabilities and allocation of resources to safeguarding the highest value targets are suitable methods for analyzing intelligent threats. Meanwhile, in the case of stochastic threats a QRA alone is sufficient to uncover stochastic threats as well as making use of probability risk analysis when trying to account for uncertainties about the assessment.

As for the media used to carry out intelligent attacks, one can refer to cases of cyber terrorism, and economic warfare as key examples, they rely largely on human input to be implemented meanwhile in the case of stochastic threats the chief sources of such threats can be found in technical failures from human errors, natural hazards or force majeure which refers to events beyond human control.

2.3 Standard Methods Useful for Analyzing Intelligent Threats and Stochastic Threats

The following methods are useful in analyzing intelligent threats where it’s only the Probability risk analysis that is useful for analyzing stochastic threats:

1. Game theory
2. Probabilistic risk analysis
3. Semi quantitative risk analysis approach where uncertainties are accounted for and are assigned probabilities
4. Allocation of resources to safeguarding the highest value targets

The concepts behind each approach will be explained in detail in the coming section.

2.3.1 Game Theory

Game theory was started by Princeton University mathematician John von Neumann. It is a strategy based principle that attempts to determine mathematically and logically the actions that “players” should take to secure the best outcomes for themselves in a wide array of “games.” (Nalebuff., 2008). There exist a lot of game models but for this discourse the following game models are more useful; zero-sum or non-zero-sum, sequential or simultaneous and co-operative or non-co-operative.

In the formative years of game theory, much emphasis was placed on zero-sum games i.e. games where the motivations and interests of the players are totally diverging such that one players gain is another player’s loss. Other games were considered in a cooperative form where the participants make choices and act together. Recent research in this field has centered on games were the players make choices and act separately but their interrelationship with other players involve elements of competition and cooperation, it should be noted that these games are neither zero sum nor cooperative but can either be sequential or simultaneous. The purpose of any game is the interdependence of the strategies the players adopt which can be either sequential or simultaneous.

Sequential game strategy involves the players making moves in a sequence, with each player aware of the others prior actions. Meanwhile in a simultaneous game strategy both players act at the same time, each unaware of the others actions. The general rule of thumb for a person in a sequential game is to look ahead and reason back, each player in this game should analyze how each player will respond to his current move, how he will respond in turn and so on. It is important for a player in a sequential game to see things from the eye of the eyes of the other player when modelling a response, it’s only by doing this he can achieve success.

Simultaneous game strategy involves a logical loop where the players act at the same time, although the player’s act unaware of the decision of the others, it is crucial that the players are aware that others are also unaware of each player’s decision. The thinking goes: “I think that he thinks that I think . . .” Therefore, each must figuratively put himself in the shoes of all and try to calculate the outcome. His own best action is an integral part of this overall calculation. (Nalebuff., 2008). The end of this reasoning loop is arrived by applying the equilibrium concept developed by John Nash “we look for a set of choices, one for each player, such that each person’s strategy is best for him when all others are playing their stipulated best strategies. In other words, each picks his best response to what the others do. Sometimes one person’s best choice is the same no matter what the others do. This is called a “dominant strategy” for that player. At other times, one player has a uniformly bad choice—a “dominated strategy”—in the sense that some other choice is better for him no matter what the others do. The search for an equilibrium should begin by looking for dominant strategies and eliminating dominated ones”. An outcome is in equilibrium when there is no belief among players that each player’s best choice will lead to an optimal result.

A good example of this can be seen in the Prisoner dilemma where the players get bad results when they act to maximize their individual utilities. Nash’s notion of equilibrium remains an incomplete solution to the problem of circular reasoning in simultaneous-move games because there are some games which have many equilibria while some have none, also the dynamic process that can lead to equilibrium is not specified in some games: despite these flaws, the concept has proven to be useful in strategic interactions (Nalebuff., 2008).

Game Theory Illustration: Prisoners Dilemma

Nalebuff provided a useful example on how to illustrate the game theory. ‘Here is the scenario in the “prisoner’s dilemma” Two suspects in a crime are questioned separately, each suspect has the option to confess or stay silent. If suspect A keeps silent, then suspect B can maximize his utility by confessing and vice versa. If suspect A confesses, it will be better for suspect B to also confess to increase his utility rather than losing in the game. Confession is A’s dominant strategy where he will maximize his utility, this also applies for suspect B. An equilibrium position will arise when both suspect A and B confess although it should be stated that they would have both maximized their utility by staying silent in this game scenario. Such cooperative behavior among players (suspects) can only be achieved by repeating the game scenario because the temporary utility the players will derive by confessing will be overshadowed by a disutility when cooperation breaks down’. The figure below provides a better understanding of this concept.

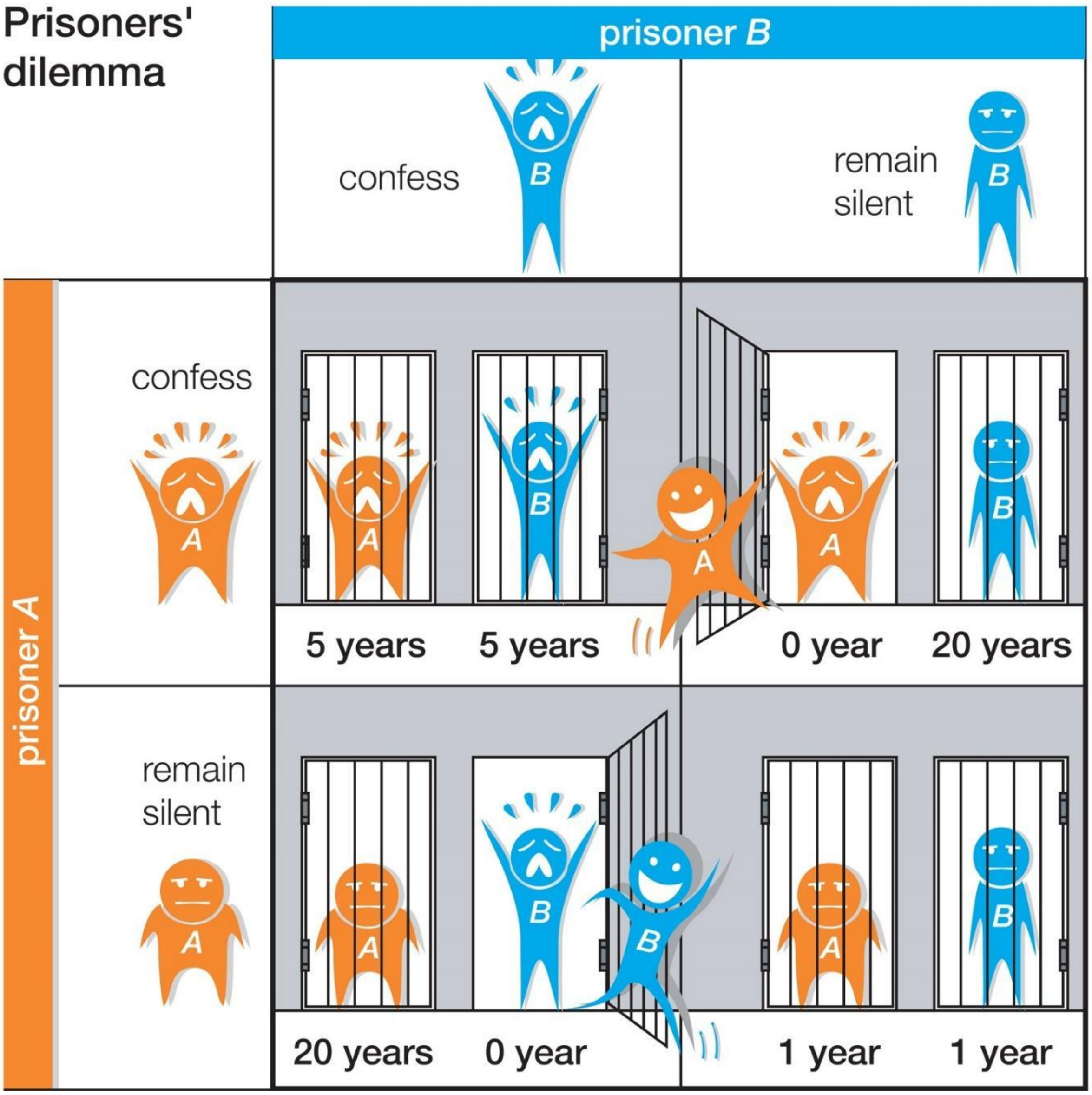


Figure 4: Illustration of the Prisoner Dilemma culled from Encyclopedia Britannica, 2010

An overview of the game theory has been provided thus far, in the next discourse we shall be going to the application of game theory in risk analysis for unearthing intelligent threats such as cyber-terrorism.

2.3.1.1 Game theory from a Terrorism Risk Analysis Perspective

A lot of research on the use of game theory in analyzing risk encountered from intelligent threats have been carried out; the work by Ezell et al, Zhuang &Bier and Guikema & Aven will provide a lot of insight about the intricacies of this approach as well as its shortcomings.

From a terrorism risk analysis perspective, the key assumption for the game theory is that each of the game scenarios are interdependent that is the outcome for any individual in the game depends on the choices of others in the game. Another key assumption in the game theory is that all the possible utilities and consequences of the outcomes of each choice must be derivable and usable within the game model. (Ezell, Bennett, Von Winterfeldt, Sokolowski, & Collins, 2010). This is only possible if the motivations and intent of each player is known. Meanwhile in the classical game theory one set of utilities is considered for each player and when there is uncertainty about intentions and motivations the player has then multiple utilities are modelled using games of incomplete information (Harsanyi, 1967, 1968a, 1968b). Furthermore, another key assumption of classical game theory is that the players are ***rational*** and ***intelligent*** enough to resolve and determine the consequence of their actions. (Binmore, 1990). There are limitations in this assumption for instance the players might not be as erudite as first assumed (e.g., they have misinterpreted the consequences of their actions).

An argument given to support the rationality and intelligence assumption in game theory is that in terrorist attacks the perpetuator's objective is to maximize his utilities (consequence or severity of attack) by following this analogy planning or defending against the most severe consequences of an attack is a good approach. However, there are some loop holes in this argument for example if a choice is made to protect a high value target and remove protection from a small value target an attacker might just decide to attack the small value target given he can optimize his utility by doing this with less expense of resources (Ezell et al., 2010). Bier et al also agree with this viewpoint although with some little differences. According to (Jun & Bier, 2007) to efficiently protect a target from a potential attack the defender must be able to predict how much effort an attacker will put into any attack not only the likelihood of the target of being attacked. A model to determine the probability of damage from an attack versus the attacker's motivation and defender's investment was also proposed by Zhuang &Bier. In this model the decision process of the defender and attacker were presented in a more simplified model where the following were analyzed:

- The technology available to both attacker and defender versus the amount of effort on the part of the attacker and the defensive investment on the part of the defender
- The valuation of the potential targets by the attacker and defender
- The utilities and disutilities available to the attacker and defender when considering severity of consequences

- The utilities and disutilities of attacker and defender with respect to attacker effort and defensive investment.

The following assumptions were made in establishing this model

- The probability of damage of an intentional attack is zero when the defender investment is at infinity, therefore the attacker marginal returns will decrease. The same applies vice-versa
- The utility of the attacker is increasing with total damage while that of the defender is decreasing with total damage. This also implies that the total expected utility is the sum of expected utility of total damage and the disutility of attacker effort and defensive motivation given that the attacker and defender are risk seeking or risk neutral or risk averse
- The attacker and defender have prior knowledge on the rules of the game where the game can either be simultaneous or sequential in nature (Jun & Bier, 2007).

Although this model presented some very interesting views on the use of an endogenous attacker, its shortcomings lie in its assumptions. As stated by (Guikema & Aven, 2010), ‘ the assumption of rationality that is players (attacker and defender) choose actions to maximize their utilities is inaccurate because rationality is a normative model and not a descriptive model that will account for attackers’ and defenders’ behavior. Individual’s might not act to maximize their subjective expected utility, but can decide to be spontaneous or act with honor both of which do not fit into the rationality decision making process (Hollis, 1991). This argument was further reinforced by Allais and Ellsberg in their paradoxes which shows deviations on a player’s choices from the predictions in the expected utility theory (Allais, 1953; Ellsberg, 1961).

Recent advances in game theory have succeeded in providing relevant strategies that can be applied for several situations of conflict and co-operation, it should be noted that even with this the theory still needs more development because in many cases the design of successful strategies by the players is more of an art rather than a science because of the normative nature of the game theory

2.3.2 Probabilistic risk analysis

The use of probability as a tool in QRA’s for analyzing stochastic threats and intelligent threats is very popular. Where in the case of intelligent threats a vulnerability analysis is further carried out alongside this QRA. According to (Aven, 2013) probability is a measure of expressing uncertainty following the rules of probability calculus where we can have a frequentist probability or a subjective probability. Frequentist probabilities express the fraction of times a given event occurs when this scenario is considered infinitely under the same conditions.

Meanwhile, subjective probabilities are assigned probabilities where an assessor assigns a probability relative to his background knowledge and level of uncertainty about the occurrence of such an event. This is the viewpoint that will be taken in this discourse although other views will be made mention with their shortcomings presented.

As stated in the discourse about threats; stochastic and intelligent threats can be good examples of black swans although not in all cases. The use of frequentist probabilities to model these threats is difficult because the conditions for each scenario differs and considering the underlying principle in frequentist probabilities is for the scenario to be carried out infinitely which is not logically possible.

As a result of this, subjective probabilities are assigned when uncovering threats using probabilities to account for uncertainty about the QRA. (Aven, 2013) argues that because of the economic limitations a balance should be made to account for cautionary measures and protection cost: This can be done with the use of subjective probabilities to aid the decision making process, key to this approach is accounting for the strength of background knowledge when deciding which targets to allocate more resources towards protecting. Where a target that the assessor has a strong background knowledge should be given more importance. And measures to increase strength background knowledge about attacker intents on other targets can be achieved through more robust intelligence gathering and modelling changes in attacker's effort due to defensive investment. The findings by (John Garrick et al., 2004) presents a different viewpoint on this issue, here an expert based approach is supported which is dependent on the knowledge of the experts carrying out the assessment. There are two arguments against this expert-based PRA approach presented by (Guikema & Aven, 2010) where they account for the difficulties in getting experts for problems that are classified and the inability of this approach to lead to a model that account for the strategic interactions between attackers and defenders. Rather the expert-based PRA approach develops a static view of attack probabilities representing the behavioral pattern of an attacker which is extremely difficult considering the infinite modelling scenarios of attacker and defender responses.

In view of all this arguments, there is need to see beyond these assigned probabilities and note that probability is just a support tool for decision makers to account for uncertainties about the QRA. There will be more details about this in the discussion part of this thesis.

So far, the application of probability in assessing intelligent threats has been shown, a similar approach is used in assessing stochastic threats the main difference being that the uncertainties are much easier to account for given that there are no constant changes and adaptability, as can be seen when accounting for intelligent threats.

2.3.3 Semi quantitative risk analysis approach where uncertainties are accounted for and are assigned probabilities

In this approach, probabilities and expected values are used to account for uncertainties and risk can be presented quantitatively by probabilities and expected values, because of this there might be over simplification of the risk picture with respect to assumptions made: this can result in important factors being left out or not given significant weight when trying to quantify risk. This approach also accounts for vulnerability, which is the common practice when analyzing intelligent threats. A QRA is done where subjective probabilities are used as a tool to express uncertainty in this analysis followed by a vulnerability analysis to identify the vulnerabilities that exist in the system or structure. The probability that a system function is reduced in reaction to a threat source and the expected consequences given a certain threat source are some of the indicators that are evaluated and measured when carrying out a vulnerability analysis. It is important to note all the probabilities assigned during this analysis are based on the assessor's background knowledge. And there exist some uncertainty about this knowledge, for example an assessor can say the likelihood of a terrorist attacking the Norwegian Embassy to be low based on the security measures and barriers set in place. This viewpoint (background knowledge) can change once a QRA and vulnerability analysis is carried out because there might be new information available after the analysis that might strengthen or weaken the background knowledge. According to (Aven & Renn, 2009) all assigned probabilities are conditioned on the background knowledge that is available at the time we quantify our uncertainty. Therefore, assumptions are an important aspect of the information and knowledge, because they act as frame conditions for the scope of the analysis and the produced probabilities must be seen from the overlying frame conditions.

The methodology for carrying out this analysis as stated by Aven in (Aven, 2007) involves carrying out a risk and vulnerability analysis together and this involves the following:

- Identify the relevant functions and sub functions to be analysed, and relevant performance measures (observable quantities)
- Define the systems to meet these functions.
- Identify relevant sources (threats, hazards, opportunities).
- Perform an uncertainty analysis of the sources
- Perform a consequence analysis, addressing uncertainties
- Describe risks and vulnerabilities.
- Evaluate risks and vulnerabilities.
- Identify possible measures, and return to identify relevant sources

In the case of the analysis being quantitative, assigned probabilities and expected values are used to express our uncertainty as mentioned in the earlier discourse.

Some key arguments for the use of this semi quantitative model rather than other approaches such as the probability of frequency by Garrick are presented in (Aven, 2007). Most notably, ‘the probability of frequency approach by Garrick presents two levels of uncertainty rather than one level of uncertainty presented in the semi quantitative approach. This premise arises, because fictional probabilities are introduced in probability of frequency approach, which are just mental constructions and in no way represent what exists in the real world because infinite scenarios cannot be repeated or defined to make these fictional probabilities operational’. A new element of uncertainty is introduced to account for the true frequency value, hence why we have two uncertainty levels in Garrick’s approach, which reduces the strength of the risk analysis process. Despite how appealing this concept sounds, it puts emphasis on measuring fictional quantities rather than trying to quantify risk and this is a wrong viewpoint to take.

Although this method provides a comprehensive risk picture, it still has some disadvantages for instance it is still strongly dependent on expert assumptions and it neglects the strategic interactions that are exhibited between an adversary and a defender: although it should be stated that it incorporates more information and knowledge when carrying out the assessment which makes it more reliable than the probability risk analysis approach. (Guikema & Aven, 2010)

2.3.4 Allocation of resources to safeguarding the highest value targets

As the name implies, this approach involves setting aside resources (protection and emergency preparedness) given the severity of an attack should it occur? By applying this methodology, the assessor can eliminate the problem of having to specify probabilities for different attack scenarios and also avoid making assumptions that are prevalent in behavioral models such as game theory. The main standpoint taken in this approach is that the limitations of probability and decision rules are accepted, because they are too difficult to determine accurately, therefore regardless of the probability of an attack, resources are only allocated based on the severity of such an attack. In view of this an assessor will assign more resources to be set aside to protecting assets that are considered by the defender to generate the most severity given a successful attack (G.E Apostolakis, 2005).

One of the arguments given in support of this strategy is that if allocation of defensive investment is done in a cost effective optimal way, then it will lead to a “mini-max” solution where the capability of an attacker to carry out a successful attack is minimized while the ability of a defender to protect a target is maximized. Casting a glance at the game theory this leads to a zero-sum game i.e. games where the motivations and interests of the players are totally diverging such that one players gain is another player’s loss and this “mini-max” stand-off poses a reasonable solution to this zero-sum game (Major, 2002)

Despite the ability of this approach to ensure highest value targets are protected adequately, there are strong arguments against this approach when looking at the efficiency of allocating resources especially when there is a shortage of resources to protect all high value targets. One of such arguments is raised by (Guikema & Aven, 2010) where they acknowledge the efficacy of this approach in protecting the targets of highest value to the defender and its non-dependence on game theory, however this strategy can be result in a “sub-optimal” protection plan when resources are limited. The consequence of this strategy is that small value targets are left unprotected because of this biased allocation of resources. Also this strategy does not take into account the dynamism that can be demonstrated in a strategic behavior between attacker and defender where they both value different things (economic, religious, life loss). For example, an attacker might value attacking a school rather than a government establishment or industrial plant, but based on this strategy it is assumed the attacker will go after the highest value target which in this case is the government establishment or industrial plant. This can lead to a very misleading assessment of terrorism risk with large consequences.

2.4 Unique Methods for Analyzing Intelligent Threats

From the discourse in 2.3 the methods for analyzing intelligent and stochastic threats were treated. It should be noted that among all the methods mentioned above the Probabilistic risk analysis approach is the only method suitable for assessing stochastic threats, while the others are more suitable for assessing intelligent threats. There exist other methods for analyzing intelligent threats such as logic trees (decision trees, fault trees, success trees), influence diagrams causal loop diagrams, Bayesian network analysis, but this thesis will be limited to the methods that have been treated so far.

2.5 Synopsis of Theoretical Background and Presentation of Game Theory Influenced Risk Assessments (GIRA) Framework

So far in this literature review, background has been laid to shed more light on the topic at hand about assessing stochastic and intelligent threats in the Norwegian Petroleum Industry. This theoretical background delved into previous research work carried out by notable researchers in the fields governing assessment of stochastic threats and intelligent threats. It has been shown how their proposed standalone methods are suitable in analyzing stochastic and intelligent threats. However, each of the standalone methods that were presented have their weaknesses which have been mentioned. It is because of these weaknesses that there is need for improvements. One of the ways of implementing an improvement on existing methods is by eliminating their weaknesses. In the next chapter a method termed game theory influenced risk assessments (GIRA) will be presented as a method to eliminate the weaknesses present in the standalone QRA and terrorism based game theoretical modelling methods. It is believed that by synergizing the QRA approach with the principles used in game theory, a more robust assessment on intelligent and stochastic threats will be achieved. It should be noted that so far game theory has been used as a standalone method for analyzing intelligent threats. The GIRA approach will go a step further by being able to assess both intelligent and stochastic threats. This will be possible because of the synergy with the QRA approach where uncertainties and strength of knowledge (SoK) are accounted for. This is a new line of thought built on the work carried out by Bier et al on the application of game theory in balancing investment when preventing terrorist attacks and natural disasters.

CHAPTER THREE

3.0 GAME THEORY INFLUENCED RISK ASSESSMENTS (GIRA APPROACH)

In section 2.3.1 of this thesis a lot of background information was given about the game theory, for this reason it is only aspects useful in this suggested approach that will be mentioned briefly. The use of game theory has grown since it was postulated, much of its application can be seen in the fields of economics, investment analysis, terrorism risk analysis and mathematics. However, its use in the petroleum industry has been limited to the area of investment decision making and economic analysis. This failing of the industry can be understood because of the difficult nature in applying this theory. Most researchers consider the application of game theory as an art form rather than a science. However, there are a lot of gains that can be made by applying this theory more extensively to cover areas such as risk management and assessments in the petroleum industry. As this discourse progresses a framework will be presented on how to successfully apply the game theory together with a QRA for risk assessments. This approach has been termed as 'GIRA' game theory influenced risk assessments which is a synergy of game theory and quantitative risk assessment methods.

Game theory influenced risk assessments (GIRA) simply involves applying the principles of game theory to carry out risk assessments in the petroleum industry. This risk management strategy will make use of probability, statistics, and logic to determine the multiple actions that can be taken by various players in the petroleum industry with the presupposition that all players will aim for their best outcomes in each game. The essence of applying GIRA in the petroleum industry will be to reduce the dominated strategies petroleum organizations encounter and increase their dominant strategies. This will create multiple Mini-Max (minimized losses and maximized benefits) solutions for different scenarios. The GIRA strategy is an addition to the current QRA process being used in the Norwegian petroleum industry, much of the thinking process applied while carrying out QRA's will be applied here. The only difference is that the output from the QRA process will be used as inputs into the GIRA model. In a nutshell, GIRA is a two-step analytic model, where the QRA carried out is step one and the results are inputted for further analysis with the GIRA strategy is step two.

This risk assessment strategy will employ the use of zero-sum, sequential and simultaneous games where the players co-operate to analyze stochastic threats. A similar approach will be used to analyze intelligent threats; the only difference is that here the players do not co-operate.

The following steps will be taken when using the GIRA approach:

1. **Identify the threat type:** This involves identifying the nature of the threat and then classifying the threat based on whether it is intelligent or stochastic in nature.

2. **Carry out a quantitative risk assessment:** This involves applying the QRA methodology stated in NORSOK Z-013 to assess the threat type.
3. **Determination of game type:** In this step the information on the threat type will be useful. As this will determine whether the game scenario should be simultaneous, sequential, co-operative and non-co-operative. For intelligent threats the game scenario's will be either simultaneous and non-co-operative or sequential and non-co-operative. Meanwhile for stochastic threats the game scenario's will be either simultaneous and co-operative or sequential and co-operative.
4. **Analysis of player actions and utilities:** In this step the actions that will be taken by the various players in the game will be analyzed. Historical data and trends in the industry will be useful in trying to model player behavior. You can see Appendix for data on accident and near-miss trends in the Norwegian petroleum industry, this is an example of data which can be used in modelling player behaviors when analyzing stochastic threats. The same rationale will be useful when analyzing intelligent threats, where prior attacks will be used to determine likely targets, attack vectors, player motivation and utilities etc.
5. **Developing Mini-max solution strategies:** in this step strategies to minimize losses and maximize benefits in the industry will be determined. This can be achieved by ensuring for the various threat scenario's the dominant strategies for the industry are more robust while their dominated strategies are diminished.
6. **Presentation of results from GIRA approach to final decision makers:** At this stage a good overview of the threats will be known and strategies to obtain dominance would have been determined. This will give more meaning to the final decision makers because they will be able to have a good picture of the threats involved and how dominance can be ensured.

To further enhance understanding of this concept, the methodology to be used in the GIRA approach will be used to solve a hydrocarbon leak scenario as a stochastic threat. This threat will be analyzed with the GIRA model showing how the results from the QRA will be further assessed with the GIRA approach.

3.1 Application of the GIRA Approach in the Norwegian Petroleum Industry

So far, the thought process behind the GIRA approach has been shown, but this is not enough the critical question is: how can the GIRA approach be applied in practice? An attempt will be made to try and answer this question by looking at a scenario involving a stochastic threat which will be an ignited gas leak in a process facility offshore. In this scenario the QRA methodology currently being used in the Norwegian petroleum industry will be used to analyze this threat type with a little overview on how strength of knowledge(SoK) is ranked. The results from the QRA will then be further assessed using the GIRA strategy.

3.2 Current QRA Process Being Applied in the Norwegian Petroleum Industry in Assessing a Scenario of an Ignited Hydrocarbon Leak on an Offshore Process Facility

3.2 A. Quantitative Risk Analysis Process

3.2.1 Traditional QRA Based on the NORSOK Z-013 standard

For the purpose of this discourse, a scenario of an ignited process leak will be considered. The following criteria should be met when carrying a QRA on an offshore facility based on the Z-013 standards.

- Identification of hazards (HAZID) and events that can lead to hazards taking into account the potential for occurrence of the identified hazardous scenarios.
- Identification of initiating events (A) and their potential causes.
- Analysis of accidental scenarios and description of the likely causes.
- Identification of barriers or measures that can be implemented to reduce risk.
- Presentation of an unbiased overall picture of the risk in a manner suitable and useful to decision makers and other relevant target groups.

The figure below shows the main elements and steps that need to be carried out in a QRA according to the NORSOK Z-013 standard.

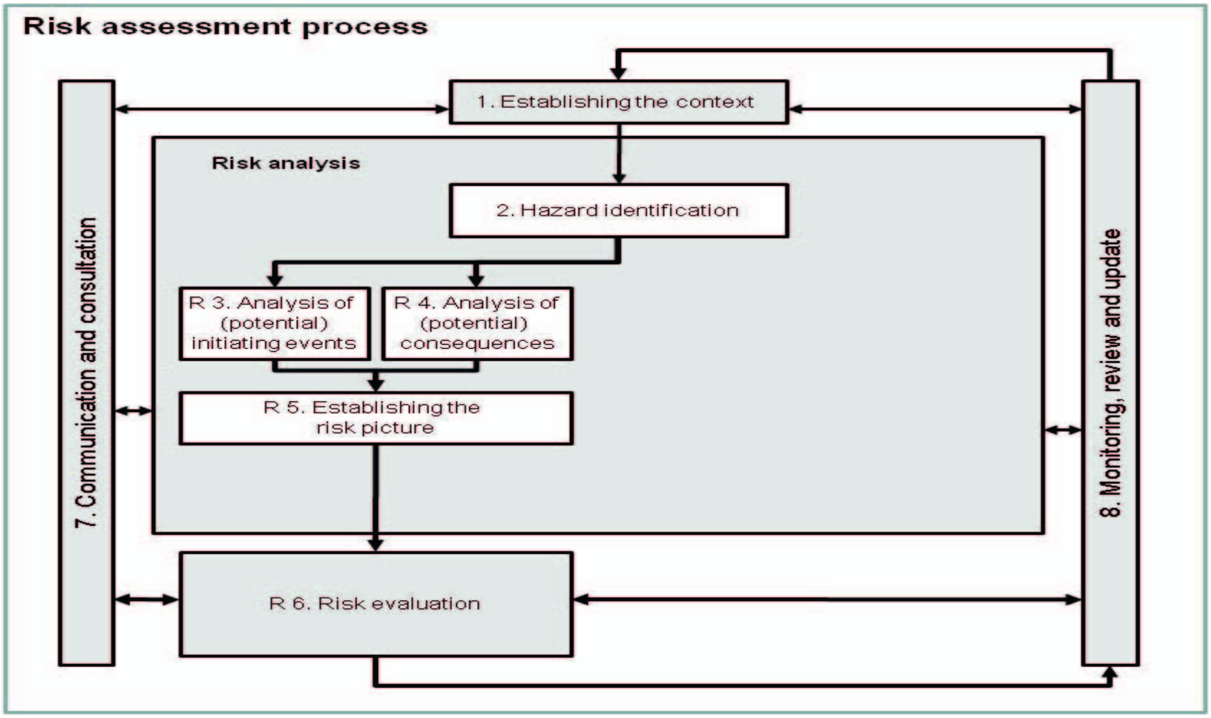

Risk assessment process
1. Establishing the context
Risk analysis
2. Hazard identification
R 3. Analysis of (potential) initiating events
R 4. Analysis of (potential) consequences
R 5. Establishing the risk picture
R 6. Risk evaluation
7. Communication and consultation
8. Monitoring, review and update

Figure 5: Steps required in a QRA culled from NORSOK Z-013 standard: Risk and Emergency Preparedness Assessment)

3.2.1.1 Hazard Identification:

To carry out an efficient hazard identification, which uncovers all the threats that a system will encounter the analyst has to understand the key term what is a hazard? A hazard is a potential source of harm and a hazardous event occurs when a hazard is realized. From this analogy a HAZID involves a systematic process where each activity to be carried out will be placed in a checklist and the likely hazards involved in these activities will be identified. The HAZID should be done in a thorough manner because and hazard that is not identified will arise in an incomplete risk picture thereby rendering the QRA as a decision support tool ineffective.

3.2.1.2 Risk Analysis

3.2.1.2.1 Analysis of initiating events:

This involves analyzing and identifying the potential causes of initiating events which can lead to a hazard and assessing the probability and frequency of occurrence without neglecting the uncertainty about this probability. And this can be done in a qualitative or quantitative manner, in the qualitative method the use causal analysis should display a good understanding of design, operation and maintenance and in cases of coarse and subjective analysis the experience basis by the expert should be adequate to reduce the level of uncertainty about this analysis.

Meanwhile in the quantitative case the initiating events will be identified based on the requirements set out for HAZID in 3.2.1.1. The initiating events that can lead to an ignited process leak can be determined by knowing the leak frequency of the process modules involved.

Leak frequency: This is simply the rate at which the gas will be released from the broken pipe. When establishing the risk picture standard models for determining the value of the leak frequency will be employed such as the following equation will be employed:

F(d)- f(D)dm +Frup (for d-1 mm to D) (HSE, 2012)

Where

F (d) =frequency (per year) of holes exceeding size d
f (D) = function representing the variation of leak frequency with D
D= equipment diameter (mm)
d=hole diameter (mm)
m=slope parameter
Frup = additional rupture frequency (per year)

The leak scenarios encountered in this assessment will be classified as full pressure leaks and zero pressure leaks

- **Full pressure leaks**: These are leaks that exit through the defined hole, beginning at the normal operating pressure, until controlled by emergency shutdown (ESD) and blowdown, with a probability of ESD/blowdown failure

- **Zero pressure leaks**: These are leaks where the pressure inside the leaking equipment is virtually zero (0.01 barg or less). This may be because the equipment has a normal operating pressure of zero, or because the equipment has been depressurized for maintenance. These leaks may typically be ones, which release small quantities of gas, short lasting oil spills, or liquid releases from atmospheric tanks.

3.2.1.2.2 Analysis of potential consequences

For this scenario of an ignited process leak the key parameters useful in modelling the consequences such as gas dispersion, ignition potential, fire model and explosion model will be determined using relevant models. This will be done based on the scale of the fire, where the consequences of the ignited gas release in the process area will be modelled taking into account loads.

- **Gas Dispersion**: This will take into account the boundary behavior of the gas when it leaks and how it is influenced by its thermodynamic properties (pressure, volume, temperature) and the ambient conditions (wind speed, terrain) in the process area. It is very difficult to model a gas release due to the number of variables acting upon the released gas. It is not accurate to base a gas dispersion model on gas densities alone. Even on a calm day, the average wind velocity is 3 m/sec. which is enough to displace gases even though the wind cannot be felt (Draeger, 2010). According to AristaTek, models such as PEAC and ALOHA can be used to determine this and then simulated using any suitable software such as FLACS, Draeger, and Cameo etc (AristaTek, 2015). For the purpose of this work FLACS will be used.

- **Ignition Potential**: Ignitions occur when hydrocarbon gas cloud expands and encounter an ignition source. The gas must be within its flammability limits in order to ignite. The closer the gas concentration is to its stoichiometric concentration the less energy will be required to ignite it. Models such as UKOOA, TDIIM, and MISOF will be useful in determining this. (Falck, 2014).

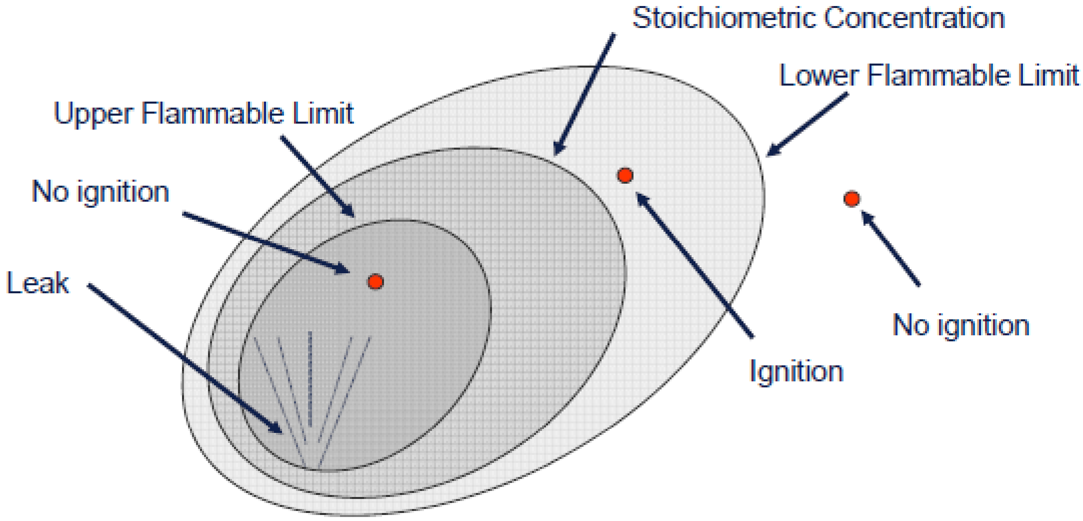


Figure 6: Showing how an ignition occurs culled from (Falck, 2014)

- **Fire modelling**: Here different fire scenarios are simulated using integral or CFD based models and results are evaluated using sensitivity or uncertainty analysis to determine the suitability of the model.
- **Explosion modelling**: The rapid increase in volume and release of energy in an extreme manner, usually with the generation of high temperatures and the release of gases will be modelled using CFD based models such as FLACS. The following activities will be carried out during this modelling:
  - Probabilistic explosion analysis
  - Blast propagation
  - Realistic case explosion analysis

- Explosion mitigation and layout optimization
- Dust explosion modelling

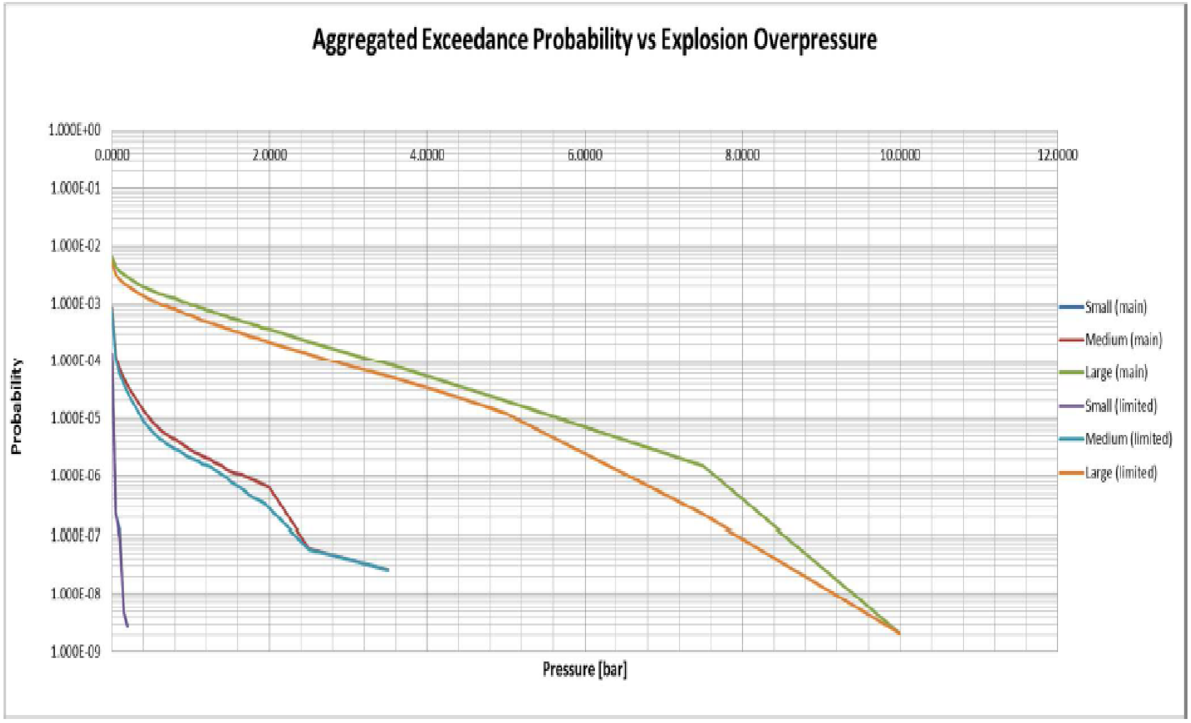


Figure 7: Graph showing the probability exceedance aggregates versus explosion overpressure culled from (Falck, 2014)

3.2.3 Establishing the risk picture

In order to establish a good risk picture, there should be a good understanding of the phenomena involved which is an ignited gas release in a process area by the analyst to present a relevant QRA to the decision makers that is clearly understandable, useful, and definite about what the risk is. This essentially involves a systematic reporting of the risk assessment process. With emphasis on this scenario key terms such as modelling of accident sequences and fatality calculations will be useful as appropriate guides in this assessment. Modelling of accident sequences: Methods such as BORA, TTS, OMT, FMECA, FTA and Bayesian belief networks will be useful in modelling the consequences of an initiating event, in this case an ignited process leak. The scale of the ignited fire and explosion will be modelled using computational fluid dynamics software’s with respect to the company requirements. For the purpose of the analysis, the scale of the fire will be differentiated as follows:

- Small

- Medium
- Large

For a small-scale fire, it is assumed the leak frequency will be considerably low and will be detected by detection system thereby reducing its ignition potential. The consequences will be relatively low with no harm to personnel.

For a medium scale fire, it is assumed that the leak frequency is moderate and it will possess a significant ignition potential. In this case, the consequences can be loss of equipment, and injury to personnel.

Lastly, for a large fire or explosion there will be a considerably high leak frequency with a significantly high ignition potential. The consequences of this are as follows:

- Significant structural damage to the platform thereby compromising its structural integrity and in extreme cases such as Piper Alpha; loss of the platform
- Serious injury and fatalities in the case of explosion and fire breaking through barrier walls

Taking into account the explosion modelling classifications above consequence classifications for an ignited release resulting in fatalities (Medium and Large explosions) will be computed as follows.

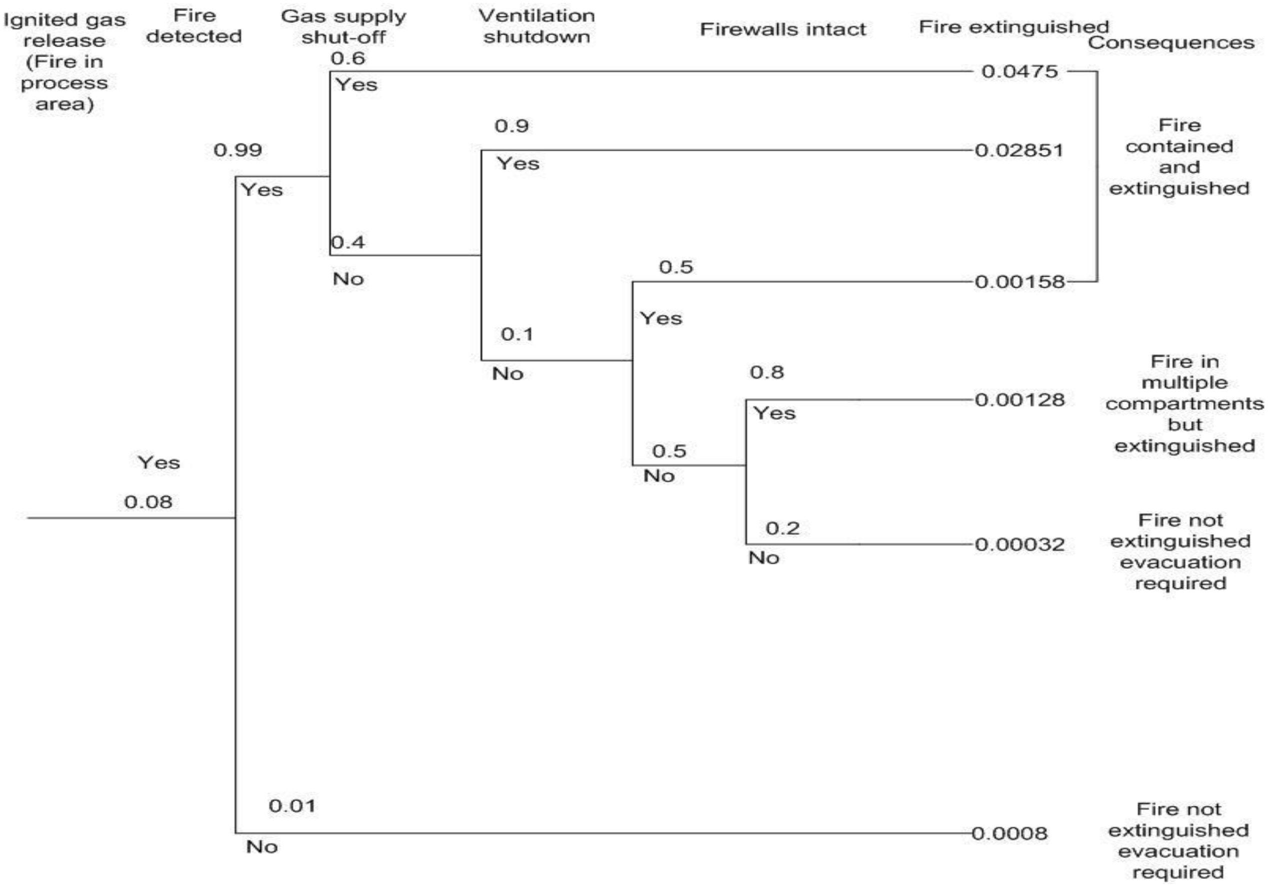

Ignited gas release (Fire in process area)
Fire detected
Gas supply shut-off
Ventilation shutdown
Firewalls intact
Fire extinguished
Consequences
0.6
Yes
0.0475
0.9
Yes
0.02851
0.99
Yes
Fire contained and extinguished
0.4
No
0.5
0.00158
Yes
0.1
No
0.8
Yes
0.00128
Fire in multiple compartments but extinguished
Yes
0.08
0.5
No
0.2
No
0.00032
Fire not extinguished evacuation required
0.01
No
0.0008
Fire not extinguished evacuation required

Figure 8 : Event Tree showing accident sequences and probabilistic consequences from an ignited hydrocarbon leak (Culled from QRA Methods and Techniques by Andreas Falck DNV GL)

- Fatality calculations (PLL): PLL is defined as the statistically expected number of lives lost (normally per year) as a result of accidental events. It is necessary to determine the fatal accident rate (FAR) which is the expected loss of lives per 10^8 hours of exposure. The relationship between FAR and PLL can be seen with the expression below:

$$FAR= [PLL/nt] 108$$

This analysis can be done by looking at different scenarios where parameter changes can result in an increase or decrease in consequences. Based on professional practice the analysis will be split in 2 stages

- Immediate: This will cover analysis of time dependent models and accounting for uncertainties related to heat resistance

- Escape and Evacuation: The key scenario that will be focused on here loss of escape routes due to explosion. In this scenario there will be a significant increase in the fatalities. This can further lead to escalation due to impairment of safety function and barriers; a good example of this is the Swiss cheese analogy where an alignment of the flaws between each barrier can result in event occurrence and escalation.

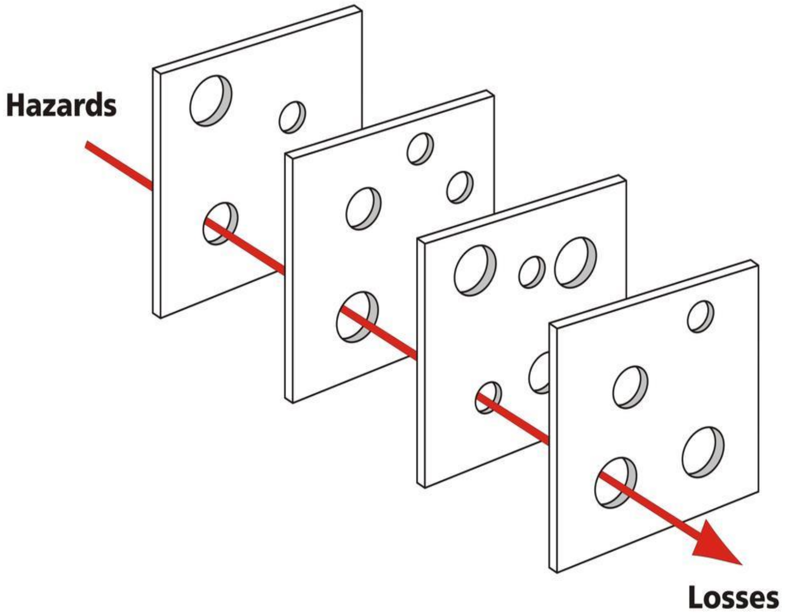


Figure 9: A Swiss Cheese Model showing alignment of barriers leading to event escalation (culled from David Mack,2015)

3.2B. Determination of Strength of Knowledge

3.2 Strength of Background Knowledge for QRA

The strength of background knowledge is important in any QRA. It is by evaluating this that we can ascertain the validity of assumptions and level of uncertainty in the QRA.

By itemizing each of the steps needed for a QRA based on the NORSOK Z-013 we can establish the strength of background knowledge by making use of a checklist/ranking of HIGH, MEDIUM AND LOW with respect to how much precision can be established with regards to the following issues:

- Validity of assumptions:
- Level of understanding of relevant phenomena
- Availability of data:
- Level of agreement/Consensus among experts

This evaluation of the strength of knowledge will cover the following areas in the QRA:

- Hazard identification
- Risk Analysis
    - Analysis of initiating events
    - Analysis of consequences
- Establishing the risk picture

3.2.1 Hazard Identification:

- Validity of assumptions: The event of an ignited gas leak is a well-known phenomenon, therefore the assumptions made in identifying the hazards will be well founded, in view of this basis a ranking of (**HIGH SoK**) is given here
- Level of understanding of relevant phenomena: There is thorough understanding of this phenomena by engineers and scientists, based on this a ranking of (**HIGH SoK**) is given here.
- Availability of data: There is a considerable amount of data with respect to events involving an ignited process leak although the frame conditions in each scenario may differ, based on this a ranking of **(MEDIUM SoK)** is given here
- Level of agreement/Consensus among experts: There is consensus among experts relating to hazards that can lead to an ignited process leak since it is a well understood phenomena, based on this a ranking of **(HIGH SoK)** is given here

3.2.2 Risk Analysis

- Validity of assumptions: There exists reliable models for predicting gas leak frequencies, ignition potential, fire modelling and explosion modelling. Therefore, assumptions made in determining the likely initiating events and consequences will be valid. Based on this a ranking of **(HIGH SoK)** is given here.
- Level of understanding of relevant phenomena: There is a thorough understanding of the phenomena and because of this carrying out an analysis to determine leak frequencies, gas dispersion rates would not pose a problem. Although, determining a fire and explosion model poses a challenge because various methods are used, based on this a ranking of (**MEDIUM SoK)** is given here.
- Availability of data: There is a lot of data available with respect to cause and consequence analysis regarding ignited process leaks although there exists some uncertainty about this data because of they are tied to probabilities. Based on this a ranking of **(MEDIUM SoK)** is given here.

- Level of agreement/Consensus among experts: There is some level of disagreement among experts on which methods are the best for fire and explosion modelling, based on this a ranking of **(MEDIUM SoK)** is assigned here.

3.2.3 Establishing the risk picture:

- Validity of assumptions: The assumptions made in modelling the accident sequences and PLL calculations will be dependent on the level of uncertainty with regard to this scenario. There exists some degree of uncertainty here and based on this a ranking of **(MEDIUM SoK)** is given here
- Level of understanding of relevant phenomena: There is although understanding of this scenario so establishing a risk picture with respect to accident sequences and Fatality calculations will pose no problems, based on this a ranking of **(HIGH SoK)** is given here
- Availability of data: There is a lot of data on failure modes from previous FMECA done in the past, although there exist some uncertainties about the reliability of this data, based on this a ranking of **(MEDIUM SoK)** is given here.
- Level of agreement/Consensus among experts: there is significant agreement among experts about the failure modes that will lead to an ignited process leaks so determining the accident sequences and the number of fatalities will not pose a problem, based on this a ranking of **(HIGH SoK)** is given here.

3.3 Analysis of Results from QRA with GIRA Approach

So far, the scenario of an ignited hydrocarbon leak on an offshore process facility has been analyzed using a quantitative risk assessment as detailed by the governing standard in Norway the NORSOK Z-013. The strength of knowledge for this assessment was also determined, now the results from this QRA will be further assessed with the GIRA approach by making use of the guideline provided for using this strategy. This step by step assessment is shown below.

1. **Identification of the threat type:** By referring to the scenario of an ignited process leak, it can be seen that this threat is stochastic in nature. This is so because it exhibits the characteristic of a high degree of randomness which is common with stochastic threats. It is also assumed that this scenario occurs because of negligence and there is absence of any intent of sabotage.
2. **Carrying out a quantitative risk assessment:** The QRA has already been carried out. Refer to section 3.2
3. **Determination of game type:** The threat has been determined to be stochastic in nature by referring to step 1. From the guideline provided for the GIRA approach, it was stated that when a threat is stochastic the game type can either be sequential co-operative or simultaneous co-operative. For a sequential game, the players will take actions in turns while

for a simultaneous game the players take actions at the same time. In order to place this stochastic threat in a suitable game, it will be assumed that the process facility will be operational and producing. With this assumption this scenario of an ignited process leak will be considered as a simultaneous game where the players (process engineers, operators and the Facility owner) co-operate with each other to maximize gains and minimize losses.

4. **Analysis of player actions and utilities:** It is assumed that there are two players in this simultaneous co-operative game, the platform owners and the crew (engineers and technicians). It was assumed in step 1 that this scenario of an ignited process leak was caused by negligence. To reinforce this fact a study was carried out by Willy Røed and Jan Erik Vinnem to determine the root causes of leaks in offshore facilities (Vinnem, 2015). From their findings it was shown that most leaks resulted from human input during scheduled maintenance activities. From this analogy there are two causes for a leak in this scenario; human input and/or equipment failure. Also, historical data about hydrocarbon leaks on the Norwegian Continental Shelf in the appendix can be used to assess trends in the industry. The actions that can be taken by the crew (engineers and technicians) in this game are 'negligence' which will result in a leak or 'cautiousness' which will help reduce the likelihood of a leak occurring. For the Facility owner, it is assumed that they will act to safeguard their interests at all times. Although in some cases culpable negligence might be the case.
5. **Developing Mini-max solution strategies:** To come up with dominant strategies, actions taken by the crew members and facility owners to maximize their gains will be uncovered. For crew members a strategy of caution during schedule maintenance activities will be regarded as their dominant strategy because it is only by adopting this strategy that the likelihood of an ignited process leak caused by negligence (dominated strategy) can be eliminated. For the Facility owner their dominant strategy is an absence of an ignited process leak. Since it was assumed that the Facility owner will always act to safeguard their interests except in cases of culpable negligence then the dominant for both players in this game have been determined.
6. **Presentation of results from GIRA approach to final decision makers:** The findings from the analysis of this scenario of an ignited process leak will be presented to the decision makers, in this context the Facility owner. A good picture of the risk associated with this stochastic threat will be shown from the results of the QRA and its further analysis with the GIRA model.

CHAPTER FOUR: DISCUSSIONS

In chapter two of this thesis the basic concepts behind intelligent and stochastic threats were shown and the methods useful in analyzing them were identified. The unique methods for analyzing each one from a risk analysis perspective was also reviewed with the strengths and weaknesses of each method stated. And in chapter three the GIRA approach for analyzing both intelligent and stochastic threats was presented showing how it will make use of inputs from the QRA process.

This discussion is divided into two main sections covering stochastic threats and intelligent threats. The case studies that were mentioned in the previous chapter will serve as a useful guide for the discussion. Arguments will be presented to support the use of the GIRA approach, these arguments will also encompass the use of probability as a tool for evaluating risk by measuring uncertainties when assessing stochastic and intelligent threats.

4.1 Assessing Stochastic Threats: Current Practices and the Way Forward

In section 2 of this thesis about stochastic threats, it was established that stochastic threats are characterized as having a high degree of randomness i.e. there is an absence of a clear pattern or trend when trying to predict such threats. It should be clearly stated that although there is a high degree of randomness when treating such threats, it does not mean they cannot be predicted, rather it is just difficult to predict them because of the uncertainty involved. Drawing from the black swan metaphor, it should be stated that stochastic threats for example the COSL Innovator fatal accident is a good example of a black swan (known knowns) type. These risk threats are known but are deemed tolerable because of the probability of occurrence is judged to be low and because of this they are not believed to occur. For this type of black swans one will assign a low subjective probability of occurrence based on the background knowledge and the large uncertainties that exist about the phenomena.

The big question is; how can one assess such threats, given this high degree of randomness? When analyzing stochastic threats, the current practice involves carrying out a quantitative risk assessment where probability is used as a tool to assess patterns or trends and quantify risk given all this uncertainty. Should we rely on this approach? Is this approach infallible? These are critical questions that a risk analyst should have foremost on his mind when carrying out a quantitative risk assessment for stochastic threats. The answer to these questions lies in the manner in which probability is used, in most cases probability is used by analysts to assess trends and patterns so as to quantify risk. In the COSL Innovator study mentioned in chapter 2, there were critical mistakes made during the design stage of the platform due to negligence and failure to account for air gap and weight changes after its commissioning. There were disagreements among the stakeholders in this project regarding the air gap calculations and this absence of consensus was ignored by COSL who assigned a low probability for any deviations in the air gap calculations based on their background knowledge. The weight changes can also be taken as uncertainties that were not accounted for during the QRA in the design stage for this platform. The choice to present expected values to the final decision makers gave an incomplete picture of risk. This use of probability is strongly against the best practices for a quantitative risk assessment, rather probability should be used as a tool by an analyst to quantify uncertainties.

Why should this viewpoint be taken? Firstly, surprises do occur as can be seen in the fatal accident that occurred. When talking about surprise, it is a reference to the black swan metaphor. In this instance, the weight and air gap deviations were not new knowledge, but the likelihood of this event was considered low, hence why it was assigned a low probability due to background knowledge and data available. One can only account for these surprises by making use of probability to express uncertainty on the assessments carried out. It is common with numbers that you can always manipulate them to give whatever meaning you wish to infer; one should tread this path with caution so as not to present an incomplete risk picture.

When probabilities are assigned, this should be done based on the background knowledge of the assessor and the strength of knowledge should be stated. Also when trying to quantify uncertainties it is paramount for the kind of uncertainty involved to be determined be it epistemic (lack of significant background knowledge) or aleatory (uncertainty about the data). The COSL Innovator scenario poses an interesting view on these issues because there was presence of both epistemic and aleatory uncertainties. How then can we unearth these uncertainties? To unearth these uncertainties, the way forward is to address the knowledge gap or lag for epistemic uncertainties and for aleatory uncertainties, probability should be used to express uncertainty about the key quantities being measured in the assessments. Where probability is precise but observable quantities that are being measured are uncertain. (Aven & Renn, 2009).

It has been shown so far how best to use probability to express uncertainties in a QRA. However, this approach still has some limitations; so what is the way forward? The way forward for analysts dealing with stochastic threats is to acknowledge the limitations of the QRA and see beyond the probability numbers (assigned or frequentist), but rather assess the strength of knowledge upon which these probability numbers were given. The GIRA approach suggested provides a framework on how this can be done. By making further use of the results from the QRA, the risk assessment will be more robust and the game sequence presentation will enable the final decision makers to have a clearer picture of risk since they can see the strength of knowledge upon which each assumption was conditioned on.

Finally, after taking into account the recommendations on the way forward, how then should a decision maker (government agencies, organizations) decide when to act upon such disclosures from a quantitative risk assessment based on the GIRA approach to reduce risk? In general practice the ALARP (as low as reasonably practicable) principle is applied when such situations are encountered. A justification on how to apply this principle was provided by Terje Aven where he states that ALARP should be applied in complex situations with high degree of uncertainty where past experiences does not provide a reliable guidance concerning consequences of current actions. (Jones-Lee & Aven, 2011)

4.2 Assessing Intelligent Threats: Current Practices and the Way Forward

In the discourse on intelligent threats in chapter two it was shown that intelligent threats, such as terrorist attacks or sabotage involve a high level of adaptability by the adversary or medium through which these attacks are carried out. They are usually characterized by high uncertainty, ambiguity and complex motivations: These factors contribute to the difficulty in assessing them, in fact they are more difficult to assess when compared to stochastic threats because of the high degree of epistemic uncertainty based on the attacker or saboteur's motivation or future behavior (Guikema & Aven, 2010). Epistemic uncertainty is simply uncertainty about the knowledge on the part of the assessor. By making reference to the black swan metaphor intelligent threats are good examples of black swans and can be of the unknown knowns type i.e. it is unknown to the government protection agencies, but known by the adversaries, but it should be stated that not all intelligent threats are black swans.

How then can intelligent threats be uncovered? In practice a QRA is done with a vulnerability analysis included. In chapter two of this thesis, it was shown that when assessing intelligent threats methods such as game theory, probability risk analysis, semi-quantitative analysis and allocation of resource to protecting high value targets can be used with strong arguments supporting each approach. It must be said that there are significant shortcomings in each individual approach, because of the magnitude of uncertainty, complexity, ambiguity and motivations present when assessing intelligent threats. In order to effectively manage intelligent threats there is need to address the above mentioned issues.

The '*Energetic Bear*' cyber-terrorist attacks will provide a useful baseline to examine the effectiveness of each individual approach (game theory, probabilistic risk analysis, semi-quantitative approach and allocation of resources to protect high value targets) to countering intelligent threats.

Looking at the Game theory, from a terrorism risk analysis perspective the key assumption for the game theory is that each of the game scenarios are interdependent that is the outcome for any individual in the game depends on the choices of others in the game. Another key assumption in the game theory is that all the possible utilities and consequences of the outcomes of each choice must be derivable and usable within the game model. (Ezell et al., 2010). Looking at these assumptions and juxtaposing them with the outcome of the *'Energetic Bear'* cyber-attacks, it can be seen that these assumptions are valid only when the motivation of each player is known. How can the motivations of the perpetuator(s) be known? This can be done in practice through the use games of incomplete information which account for the multiple utilities a player possesses (Harsanyi, 1967, 1968a, 1968b). To be successful in predicting the motivations of a player in such a game it must be assumed that the players in this game are **rational** and **intelligent** enough to resolve and determine the consequence of their actions. (Binmore, 1990). There are limitations in these assumptions of **rationality** and **intelligence**, for instance the players might not be as logical and erudite as first assumed (e.g., they have misinterpreted the consequences of their actions). An argument given to support the rationality and intelligence assumption in game theory is that in terrorist attacks the perpetuator’s objective is to maximize his utilities (consequence or severity of attack) by following this analogy planning or defending against the most severe consequences of an attack is a good approach. However, there are some loop holes in this argument for example if a choice is made to protect a high value target and remove protection from a small value target an attacker might just decide to attack the small value target given that he can optimize his utility by doing this with less expense of resources (Ezell et al., 2010). Bier et al also agree with this viewpoint, although with some little differences. According to (Jun & Bier, 2007) to efficiently protect a target from a potential attack the defender must be able to predict how much effort an attacker will put into any attack not only the likelihood of the target of being attacked. A model to determine the probability of damage from an attack versus the attacker’s motivation and defender’s investment was also proposed by Zhuang &Bier. In this model the decision process of the defender and attacker were presented in a more simplified model where the following were analyzed:

- The technology available to both attacker and defender versus the amount of effort on the part of the attacker and the defensive investment on the part of the defender
- The valuation of the potential targets by the attacker and defender
- The utilities and disutilities available to the attacker and defender when considering severity of consequences
- The utilities and disutilities of attacker and defender with respect to attacker effort and defensive investment.

The following assumptions were made in establishing this model

- □ The probability of damage of an intentional attack is zero when the defender investment is at infinity, therefore the attacker marginal returns will decrease. The same applies vice-versa
- The utility of the attacker is increasing with total damage while that of the defender is decreasing with total damage. This also implies that the total expected utility is the sum of expected utility of total damage and the disutility of attacker effort and defensive motivation given that the attacker and defender are risk seeking or risk neutral or risk averse
- The attacker and defender have prior knowledge on the rules of the game where the game can either be simultaneous or sequential in nature. (Jun & Bier, 2007)

Although this model presented some very interesting views on the use of an endogenous attacker its shortcomings lie in its assumptions. As stated by (Guikema & Aven, 2010), the assumption of rationality that is players (attacker and defender) choose actions to maximize their utilities is inaccurate because rationality is a normative model and not a descriptive model that will account for attackers and defender’s behavior. Individual might not act to maximize the subjective expected utility but can be spontaneous or act with honor both of which do not fit into the rationality decision making process (Hollis, 1991). This argument was further reinforced by Allais and Ellsberg in their paradoxes which shows deviations on a player’s choices from the predictions in the expected utility theory. (Allais, 1953; Ellsberg, 1961). Recent advances in game theory have succeeded in providing relevant strategies that can be applied for several situations of conflict and co-operation, it should be noted that even with this the theory still needs more development because in many cases the design of successful strategies by the players is more of an art rather than a science because of the normative nature of the game theory

The use of probability as a tool in QRA's for analyzing intelligent threats is very popular. A vulnerability analysis is further carried out alongside this QRA when assessing intelligent threats. There are two types of probability usually referred to during this analysis: frequentist and subjective. Frequentist probabilities express the fraction of times a given event occurs when this scenario is considered infinitely under the same conditions. Meanwhile, subjective probabilities are assigned probabilities where an assessor assigns a probability relative to his background knowledge and level of uncertainty about the occurrence of such an event. The use of frequentist probabilities to model intelligent threats is difficult because the conditions for each scenario differs, and considering the underlying principle in frequentist probabilities is for the scenario to be carried out infinitely which is not logically possible. It's similar to constructing the '*Energetic Bear'* cyberattacks infinitely under the same conditions. This is not possible because there will always be a slight change in strategy and approach by the adversary and the government. And also the resources (human life, explosive materials, and ammunitions) cannot be infinitely available. So this thought experiment is illogical. As a result of this, subjective probabilities are assigned when uncovering intelligent threats using probabilities to account for uncertainty about the QRA. (Aven, 2013) argues that because of the economic limitations a balance should be made to account for cautionary measures and protection cost: This can be done with the use of subjective probabilities to aid the decision making process, key to this approach is accounting for the background knowledge when deciding which targets to allocate more resources towards protecting. Where a target that the assessor has a strong background knowledge should be given more importance and measures to increase strength of background knowledge about attacker intents on other targets can be as a result of more robust intelligence gathering and modelling changes in attacker's effort due to defensive investment. The findings by (John Garrick et al., 2004) presents a different viewpoint on this issue, here an expert based approach is supported which is dependent on the knowledge of the experts carrying out the assessment. There are two arguments against this expert-based PRA approach presented by (Guikema & Aven, 2010) where they account for the difficulties in getting experts for problems that are classified and the inability of this approach to lead to a model that account for the strategic interactions between attackers and defenders. Rather the expert-based PRA approach develops a static view of attack probabilities representing the behavioral pattern of an attacker which is extremely difficult considering the infinite modelling scenarios of attacker and defender responses. In view of all this arguments, there is need to see beyond these assigned probabilities and note that probability is just a support tool for decision makers to account for uncertainties about the QRA.

The semi-quantitative approach makes use of probabilities and expected values to account for uncertainties. And risk can be presented quantitatively by probabilities and expected values, because of this there might be over simplification of the risk picture with respect to assumptions made: this can result in important factors being left out or not given significant weight when trying to quantify risk. This approach also accounts for vulnerability as is the common practice when analyzing intelligent threats. The aim of the vulnerability analysis is to evaluate the probability that a system function is reduced in reaction to a threat source and the expected consequences given a certain threat source. It is important to note all the probabilities assigned during this analysis are based on the assessor's background knowledge. And there exist some uncertainty about this knowledge, for example an assessor can say the likelihood of a cyber-attack of the same magnitude as the '*Energetic Bear*' is low given the non-occurrence of a similar attack from history and because of this a low probability is assigned. This viewpoint (background knowledge) can change once a QRA and vulnerability analysis is carried out because there might be new information available after the analysis that might strengthen or weaken the background knowledge. According to (Aven & Renn, 2009) all assigned probabilities are conditioned on the background knowledge that is available at the time we quantify our uncertainty. Therefore, assumptions are an important aspect of the information and knowledge, because they act as frame conditions for the scope of the analysis and the produced probabilities must be seen from the underlying frame conditions.

Some key arguments for the use of this semi quantitative model rather than other approaches such as the probability of frequency by Garrick are presented in (Aven, 2007). Most notably the probability of frequency approach by Garrick presents two levels of uncertainty rather than one level of uncertainty presented in the semi quantitative approach. This premise arises, because fictional probabilities are introduced in probability of frequency approach, which are just mental constructions and in no way represent what exists in the real world because infinite scenarios cannot be repeated or defined to make these fictional probabilities operational. A new element of uncertainty is introduced to account for the true frequency value, hence why we have two uncertainty levels in Garrick's approach, which reduces the strength of the risk analysis process. Despite how appealing this concept sounds, it puts emphasis on measuring fictional quantities rather than trying to quantify risk and this is a wrong viewpoint to take.

Although this method provides a comprehensive risk picture, it still has some disadvantages for instance it is still strongly dependent on expert assumptions and it neglects the strategic interactions that are exhibited between an adversary and a defender: although it should be stated that it incorporates more information and knowledge when carrying out the assessment which makes it more reliable than the probability risk analysis approach. (Guikema & Aven, 2010)

Lastly, there is the approach of allocating resources to protect the highest value targets. This approach involves setting aside resources (protection and emergency preparedness) given the severity of an attack should it occur? By applying this methodology, the assessor can eliminate the problem of having to specify probabilities for different attack scenarios and also avoid making assumptions that are prevalent in behavioral models such as game theory. The main standpoint taken in this approach is that the limitations of probability and decision rules are accepted, because they are too difficult to determine accurately, therefore regardless of the probability of an attack, resources are only allocated based on the severity of such an attack. In view of this, an assessor will assign more resources to be set aside to protecting assets that are considered by the defender to generate the most severity given a successful attack (G.E Apostolakis, 2005). One of the arguments given in support of this strategy is that if allocation of defensive investment is done in a cost effective optimal way, then it will lead to a "mini-max" solution where the capability of an attacker to carry out a successful attack is minimized while the ability of a defender to protect a target is maximized. Casting a glance at the game theory this leads to a zero-sum game i.e. games where the motivations and interests of the players are totally diverging such that one players gain is another player's loss and this "mini-max" stand-off poses a reasonable solution to this zero-sum game (Major, 2002). Despite the ability of this approach to ensure highest value targets are protected adequately, there are strong arguments against this approach when paying attention to its efficiency in allocating resources especially when there is a shortage of resources to protect all high value targets. One of such arguments is raised by (Guikema & Aven, 2010) where he acknowledges the efficacy of this approach in protecting the targets of highest value to the defender and its non-dependence on game theory, however this strategy can be result in a "sub-optimal" protection plan when resources are limited. The consequence of this strategy is that small value targets are left unprotected because of this biased allocation of resources. Also, this strategy does not take into account the dynamism that can be demonstrated in a strategic behavior between attacker and defender where they both value different things (economic, religious, life loss). For example, an attacker might value attacking a school rather than a government establishment, but based on this strategy it is assumed the attacker will go after the highest value target which in this case is the government establishment. This can lead to a very misleading assessment of terrorism risk with large consequences.

From the discourse on the individual approaches to tackling intelligent threats it can be seen that they all go about addressing the principal problems i.e. (uncertainty, ambiguity, complexity and motivations) associated with intelligent threats. It should be said that they are all noteworthy approaches and have unique ways of assessing intelligent threats. Are they standalone solutions to uncovering intelligent threats? The answer is no, because of the magnitude of uncertainty, ambiguity and complexity involved with intelligent threats no singular approach will be sufficient. As stated by Professor Yacov Haimes “the need for robustness and resilience on the part of the defender requires the use of multiple techniques for assessing terrorist actions as probabilities”. He reminds us that “no single model or methodology can effectively meet all the challenges of tracking terrorism (Haimes Y. Y). There are so many variables to monitor when assessing intelligent threats and the adversary keeps on adapting so it’s only by adopting a strategy of constant robustness and resilience on the part of the defender that intelligent threats can be handled effectively. What then is this strategy? The GIRA approach put forward in Chapter three of this thesis is such a strategy. This strategy involves the use of game theory principles and inputs from a QRA. By employing this strategy, a defender will have multiple *mini-max* solutions to choose from and hence improve the quality of the defense strategy that will be implemented. Also, a clearer picture of risk from an intelligent threat will be clearly seen since the results from the QRA process will be re-analyzed using the GIRA framework. However, this approach also has a shortfall which is the terrorism risk analysis might become cumbersome since two analyses are being carried out..

CHAPTER FIVE: CONCLUSIONS

Assessing risk from intelligent and stochastic threats can be a very demanding process, therefore there is need for efficient approaches to counter these threats and present a true risk picture. The various approaches that can be implemented to achieve this were shown with arguments for and against each approach These approaches are not new, per se rather they are further developments on existing approaches by researchers such as Prof. Aven, Prof. Haimes and Dr. Guikema with the aim of capturing and presenting a true risk picture to the final decision makers. A framework involving the use of game theory and a QRA termed (GIRA) has been proposed in this thesis as the most efficient method in uncovering and countering stochastic and intelligent threats.

For stochastic threats, there is need for the risk assessment to display the limitations of the QRA and see beyond the probability numbers (assigned or frequentist), but rather assess the strength of knowledge upon which these probability numbers were given. This can be achieved with the proposed GIRA approach which will show the multiple minimized losses and maximized benefits (mini-max) solutions available to a decision maker and the strength of knowledge behind each solution. This line of thought would have been useful to COSL and would have helped prevent the fatal accident that occurred. Also, to ensure robustness, a strategy of constant improvement must be embraced by decision makers in the Norwegian oil and gas industry. A guideline to justify investment on risk reducing measure can be arrived at by following the ALARP principle. Prof. Aven provides a guideline for this where he states that "ALARP should be applied in complex situations with high degree of uncertainty, where past experiences do not provide a reliable guidance concerning consequences of current actions". (Jones-Lee & Aven, 2011).

For intelligent threats, because of the high degree of uncertainty, ambiguity and complexity involved when assessing such threats, an integrated approach termed the GIRA approach is suggested. This underlying principles for this approach was shown in chapter three of this thesis. The reason for adopting this approach is that there are different assumptions when applying the individual methods available for assessing intelligent threats. By operating under these individual assumptions a true risk picture will not be captured. And this will influence the final decisions made by policy and decision makers negatively. Therefore, the aim of this GIRA integrated approach is for the true risk picture to be captured thus providing maximum benefits for decision makers as well as simplifying their decision making.

6.0 References

1. Allais, M. (1953). Le Comportement del'Homme Rationnel devant le Risque: Critique des Postulats et Axiomes del'Ecole Americaine.Econometrica1953;21(4): 503–46.
2. Aven, T. (2007). A unified framework for risk and vulnerability analysis covering both safety and security. Reliability Engineering & System Safety, 92(6), 745-754. doi:http://dx.doi.org/10.1016/j.ress.2006.03.008
3. Aven, T. (2013). Probabilities and background knowledge as a tool to reflect uncertainties in relation to intentional acts. Reliability Engineering & System Safety, 119, 229-234. doi:http://dx.doi.org/10.1016/j.ress.2013.06.044
4. Aven, T., & Renn, O. (2009). The Role of Quantitative Risk Assessments for Characterizing Risk and Uncertainty and Delineating Appropriate Risk Management Options, with Special Emphasis on Terrorism Risk. Risk Analysis, 29(4), 587-600. doi:10.1111/j.1539-6924.2008. 01175.x
5. Aven T, V. J. E. (2007). Risk Management, with Applications from the Offshore Oil and Gas Industry. London: Springer
6. Verlag, 2007.
7. Binmore, K. (1990). Essays on the Foundations of Game Theory. Basil Blackwell, 1990.
8. Ellsberg, D. (1961). Risk, ambiguity, and the savage axioms. The Quarterly Journal of Economics 1961;75(4):643–69.
9. Ezell, B. C., Bennett, S. P., Von Winterfeldt, D., Sokolowski, J., & Collins, A. J. (2010). Probabilistic Risk Analysis and Terrorism Risk. Risk Analysis, 30(4), 575-589. doi:10.1111/j.1539-6924.2010. 01401.x
10. Falck, A. (2014). QRA Methodology and Techniques.
11. Falck, A. (2014). Risk Analysis of a Hydrocarbon Event
12. Falck, A., Bain, B., & Rødsætre, L. K. (2009). LEAK FREQUENCY MODELLING FOR OFFSHORE QRA BASED ON THE HYDROCARBON RELEASE DATABASE.
13. G.E Apostolakis, D. M. L. (2005). A screening methodology for the identification and ranking of infrastructure vulnerabilities due to terrorism. Risk Analysis 2005;25(2):361–76.
14. Government: U. (2009). US Government: Deepwater Horizon Well Is Effectively Dead".
15. Guikema, S. D., & Aven, T. (2010). Assessing risk from intelligent attacks: A perspective on approaches. Reliability Engineering & System Safety, 95(5), 478-483. doi:http://dx.doi.org/10.1016/j.ress.2009.12.001
16. Haimes Y.Y, H. B. Adaptive two players hierarchical holographic modeling game for counterterrorism intelligence analysis.
17. Harsanyi, J. (1967). Games with incomplete information played by Bayesian players I. Management Science, 1967; 14(20):159–182.
18. Harsanyi, J. (1968a). Games with incomplete information played by Bayesian players II. Management Science, 1968a; 14(20):320–334.

19. Harsanyi, J. (1968b). Games with incomplete information played by Bayesian players III. Management Science, 1968b; 14(20):486-502.
20. Hollis, M. (1991). Honor among thieves in: Proceedings of the British Academy,1991.
21. HSE. (2012). Hydrocarbon Release Database (http://www.hse.gov.uk/offshore/hydrocarbon.htm).
22. IRGC. (2005). IRGC (International Risk Governance Council). Risk Governance—Towards an Integrative Approach. White Paper no 1, O. Renn with an Annex by Graham P. Geneva:
23. IRGC, 2005.
24. John Garrick, B., Hall, J. E., Kilger, M., McDonald, J. C., O'Toole, T., Probst, P. S., . . . Zebroski, E.
25. L. (2004). Confronting the risks of terrorism: making the right decisions. Reliability Engineering & System Safety, 86(2), 129-176. doi:http://dx.doi.org/10.1016/j.ress.2004.04.003
26. Jones-Lee, M., & Aven, T. (2011). ALARP - What does it really mean? Reliability Engineering and System Safety, 96(8), 877-882. doi:10.1016/j.ress.2011.02.006
27. Jun, Z., & Bier, V. M. (2007). Balancing Terrorism and Natural Disasters--Defensive Strategy with Endogenous Attacker Effort. Operations Research, 55(5), 976-991. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=27359004&scope=site
28. Klinke A, R. O. Klinke A, Renn O. A new approach to risk evaluation and management: Risk-based precaution-based and discourse based strategies. Risk Analysis, 2002; 22:1071-1094.
29. Major, J. A. (2002). Advanced techniques for modeling terrorism risk. Journal of Risk Finance 2002;4(1):15–24.
30. Maxwell, S. (October 6th 2014). Dragonflies, Crouching Yetis and Energetic Bears – the Hacking Organizations Targeting Oil and Gas.
31. Nalebuff., A. D. a. B. (2008). "Game Theory." The Concise Encyclopedia of Economics. Retrieved from http://www.econlib.org/library/Enc/GameTheory.html
32. NORSOK Standard Z-013 Edition 3. (October 2010). Risk and emergency preparedness assessment.
33. OGP. (2013). Safety Performance Indicators
34. PSA. (2014). TRENDS IN RISK LEVEL IN THE NORWEGIAN PETROLEUM ACTIVITY SUMMARY REPORT – TRENDS 2014 – NORWEGIAN CONTINENTAL SHELF PETROLEUM SAFETY AUTHORITY NORWAY.
35. PSA. (2015). Report following Investigation of Fatal Accident on COSL Innovator.
36. Renn O, G. P. IRGC (International Risk Governance Council). Risk Governance—Towards an Integrative Approach. White Paper no 1, O. Renn with an Annex by Graham P. Geneva:
37. Renn O, W. K. Renn O, Walker K. Lessons learned: A re-assessment of the IRGC framework on risk governance. Pp. 331–367 in Renn O, Walker K (eds). The IRGC Risk Governance Framework: Concepts and Practice. New York: Springer, 2008.

38. Vinnem, J. E. (1998). Evaluation of methodology for QRA in offshore operations. Reliability Engineering & System Safety, 61(1–2), 39-52. doi:http://dx.doi.org/10.1016/S0951-8320(97)00063-X
39. Vinnem, J. E. (2011). Evaluation of offshore emergency preparedness in view of rare accidents. Safety Science, 49(2), 178-191. doi:http://dx.doi.org/10.1016/j.ssci.2010.07.010
40. Vinnem, J. E. (2014). Offshore Risk Assessment: Principles, Modelling and Applications of QRA Studies: Vol 1 Springer Series in Reliability Engineering,
41. Vinnem, J. E. (2014). Offshore risk assessment: principles, modelling and applications of QRA studies: Vol. 2 (3rd ed. ed.). London: Springer.
42. Z-013, N. (October 2010).

APPENDIX

Development of Major Accident Risk to Offshore Personnel in the last 10 years

In this section, the causes of major accident risk on the Norwegian Continental Shelf and Worldwide offshore will be analyzed and a comparison of the trends will be drawn upon. In order to understand the premise for which to base this discussion, the key term 'major accident' has to be clearly understood. According to PSA in (PSA, 2014) "A major accident is an accident (i.e. entails a loss) where at least three to five people may be exposed or an accident caused by failure of one or more of the system's built-in safety and emergency preparedness barriers". In view of this definition the following defined hazard and accident conditions will be analyzed and compared in both scenarios:

- Hydrocarbon leak in a process area
- Loss of well control, blowout potential, well integrity
- Leak/Damage to risers, pipelines,
- Ships on collision courses, structural damage
- Helicopter incidents, Serious near-misses, Heli-deck factors, Air traffic management aspects, bird strikes

Data relating to exploration, production, drilling and other activities will be used as the reference point for the development of the major accident worldwide

It is important to state "the last major accident to result in fatalities on the NCS was in September 1997 in connection with the helicopter accident outside Brønnøysund" (PSA, 2014), because of this disparity, risk indicators will be used for the major accident risk on the Norwegian Continental Shelf and trends in fatalities will be used for major accidents worldwide.

Case 1: Norwegian Continental Shelf

Hydrocarbon leak in a process area

In Figure 10 below it can be seen the leaks exceeding 0.1 kg/s, standardized against the years for all production facilities on the Norwegian Continental Shelf (NCS). From this chart it can be seen how the number of leaks has reduced per facility annually in the Norwegian Continental Shelf and how in 2014 the leak level was lower than the predicted level. This shows an improvement in the measures taken to prevent Hydrocarbon leaks on the NCS

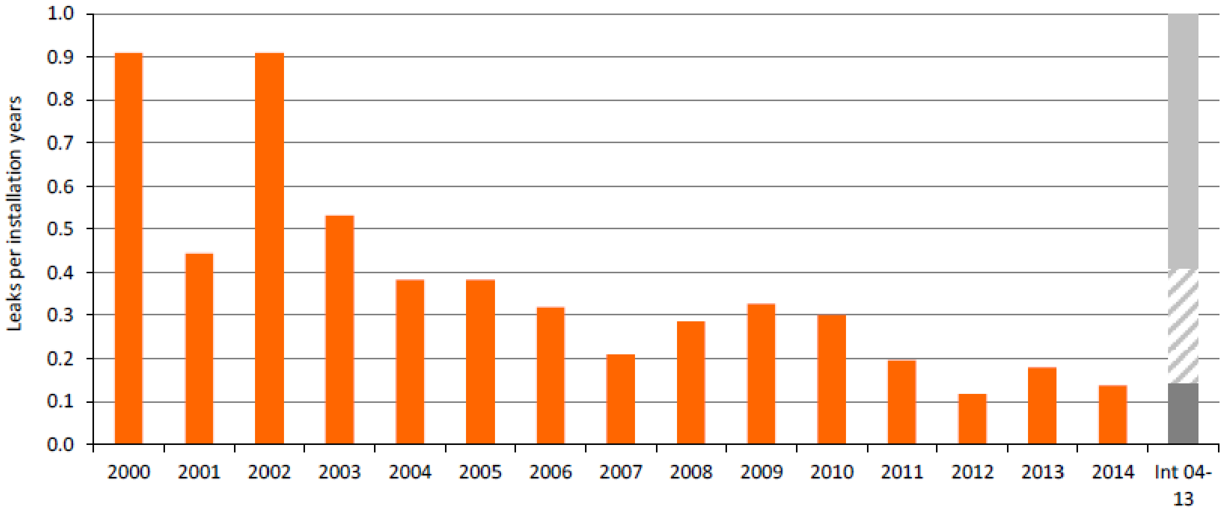


Figure 10: ***Trend, leaks, normalised against facility years, manned production facilities***

Loss of well control, blowout potential, well integrity

According to the PSA in (PSA, 2014) the Well Integrity Forum (WIF) established a pilot project for performance indicators (KPIs) for well integrity in 2007. This project was based on monitoring the performance of 1918 active wells on the Norwegian Continental Shelf and the WIF made use of the following categories to classify wells based on their barrier performance:

Red: One barrier failed and the other is degraded/not verified or with external leaks

Orange: One barrier failed and the other is intact, or a single failure could cause a leak to surroundings

Yellow: One barrier leaks within the acceptance criteria or the barrier has been degraded, the other is intact

Green: intact well, no or insignificant integrity aspects.

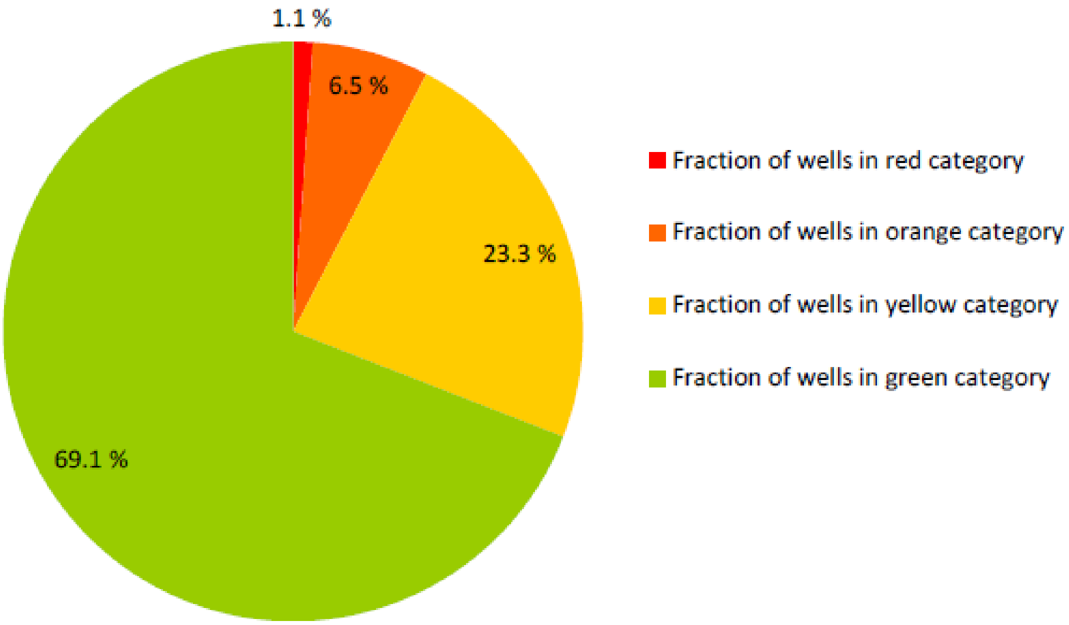


Figure 11: ***Well categories - red, orange, yellow and green, 2014***

The distribution of the wells according to their categories can be seen in the pie chart above. In this illustration it can be seen that 7.6 percent of the wells have low performance for two barriers (red +orange), 23.3 percent have low performance for two barriers but sufficient measures have been undertaken by the operating companies to balance this while 69.1 percent of the well pass the two barrier requirement.

Figure 12 below shows the development of how the wells in the top 3 categories has increased from 24percent to 31 percent.

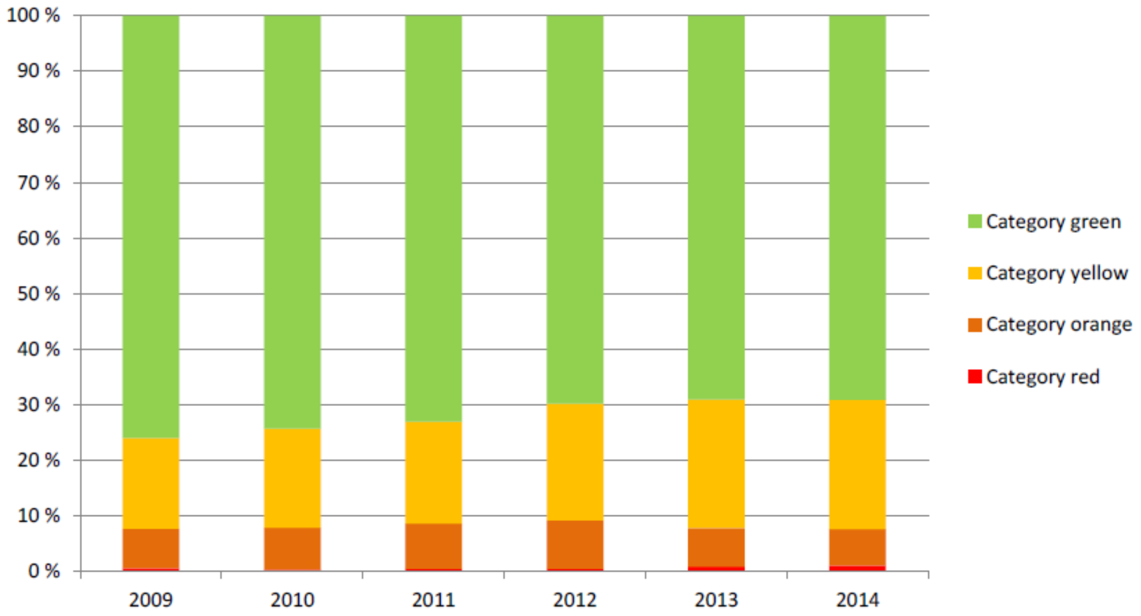


Figure 12: ***Development in well categories, 2009-2014***

4.1.3 Leak/Damage to risers, pipelines

The chart below shows the most severe cases of damage to riser and pipelines from 2000 till 2014. It should be noted all these incidents occurred in the safe zone. There were no leaks from facilities and pipelines in 2014 on the Norwegian Continental Shelf.

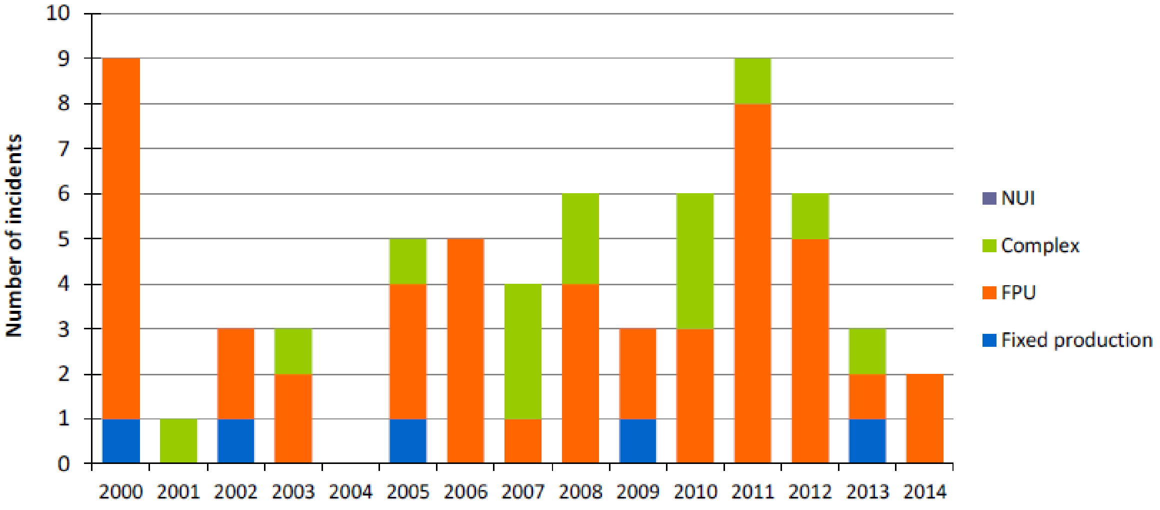


Figure 13: ***Number of incidents involving serious damage to risers & pipelines within the safety zone, 2000-2014***

Ships on Collision courses, structural damage

According to the PSA, the occurrence of ships on collision courses has reduced drastically on the Norwegian Continental Shelf, although there was a spike of vessel collision between 1999 and 2000 with 15 incidents occurring in both years. However, this number too has decreased to about 2-3 occurrences annually. Example of such scenarios include: Blue Protector collision with Oseberg Øst in 2014,

There were seven structural incidents in 2014 but none of them were serious. The chart below shows the trend in structural and maritime incidents on the Norwegian Continental Shelf (NCS)

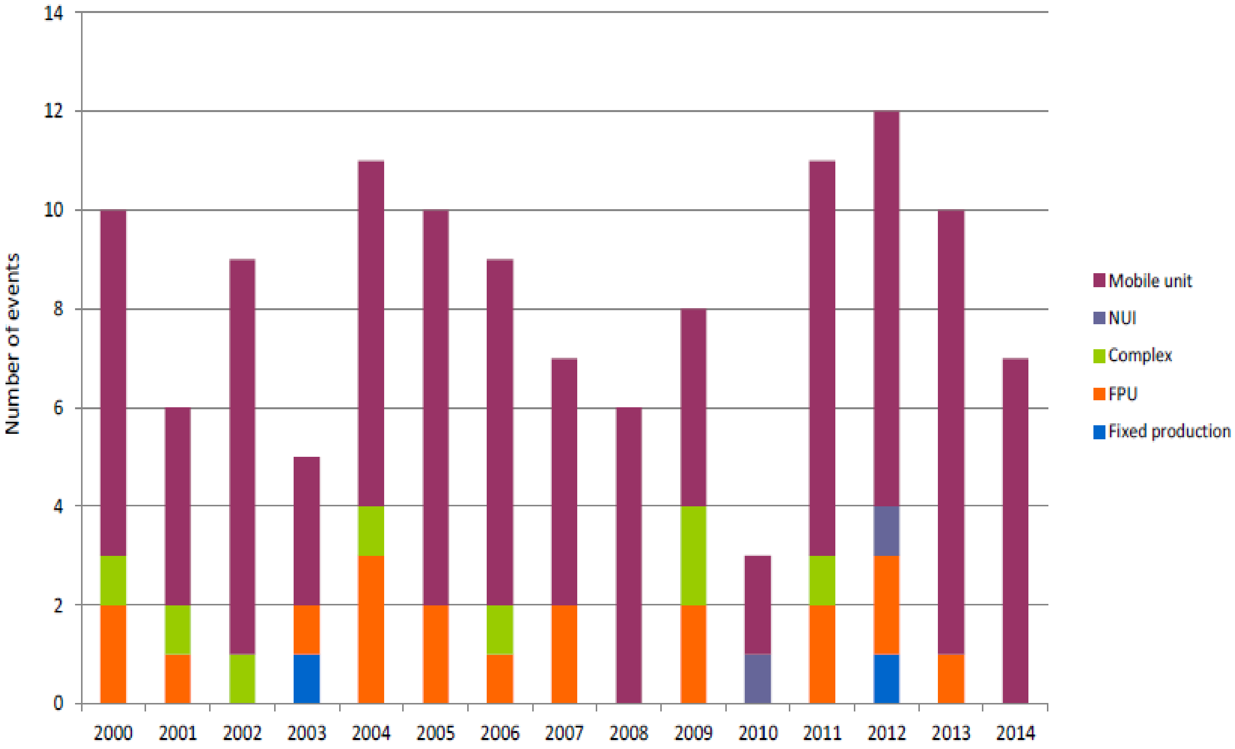


Figure 14: ***Number of serious incidents and incidents involving damage to structures and maritime systems***

Heli-deck factors and Air traffic management aspects

From the chart below (Figure 15) there has been a reduction in the occurrence of Heli-deck related incidents, although there was a little spike in 2010 compared with 2009.

In Figure 11 there was an increase in air traffic management incidents from 2013 until 2014 although there was a huge decline between 2011 and 2012. This is credited to the projects being developed to improve air traffic management on the Norwegian Continental Shelf

Lastly, there was a huge increase in the occurrence of bird strikes between 2013 and 2014, although it was decreasing between 2009 and 2013.

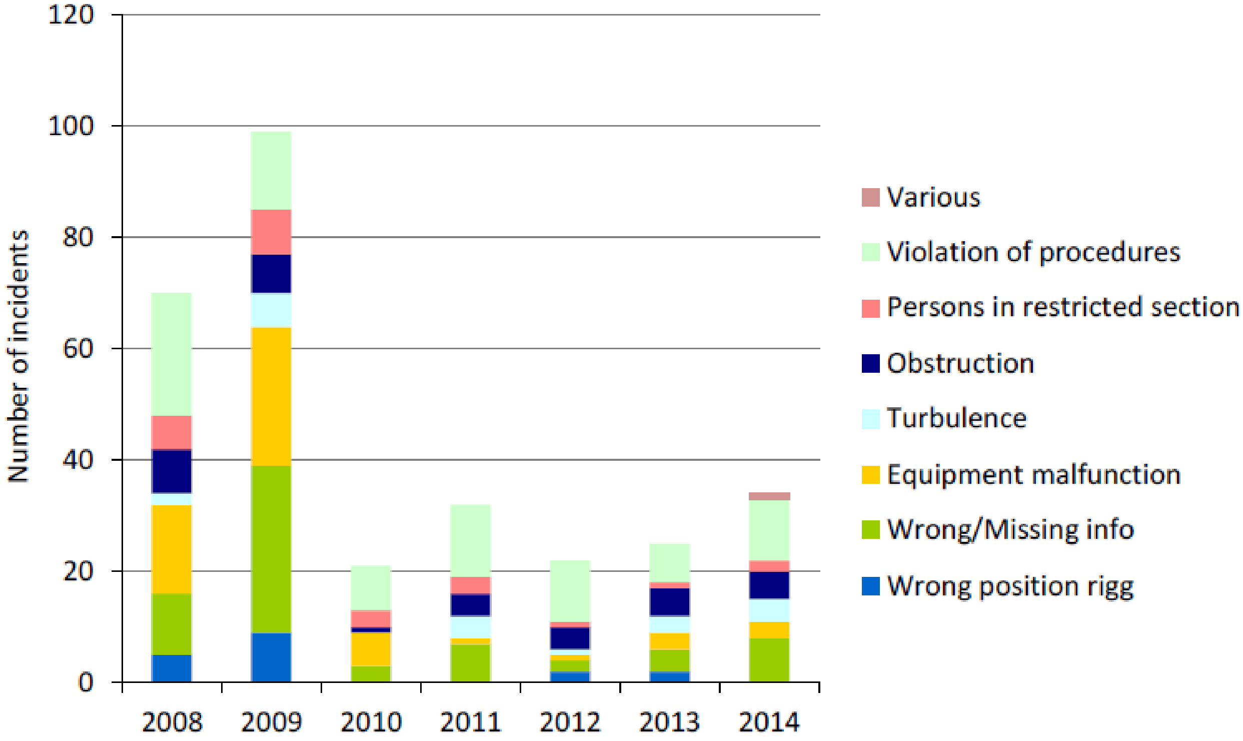


Figure 15: ***Helideck factors, 2008–2014***

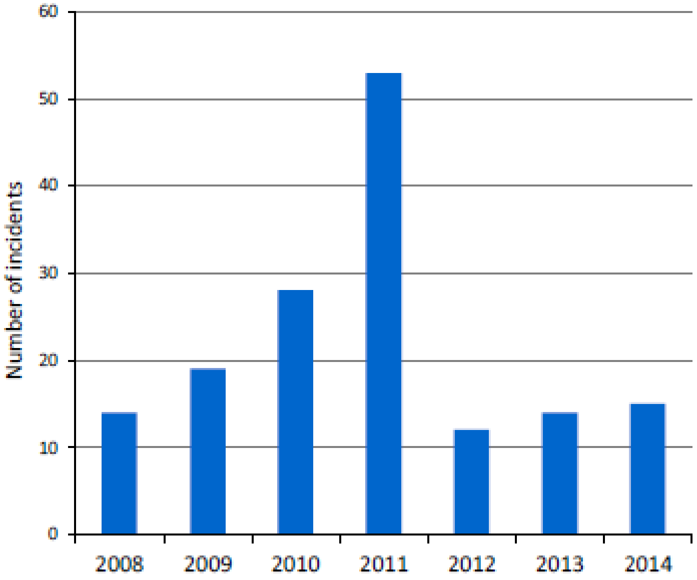


Figure 16: ***Air Traffic Management aspects, 2008–2014***

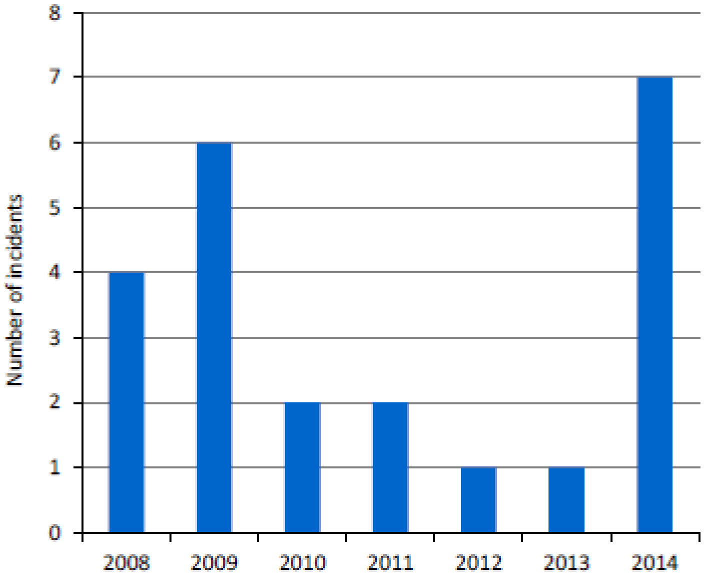


Figure 17: ***Bird strikes, 2008–2014***

A summary of the total risk indicators for facilities on the NCs can be seen in Figure 18 below

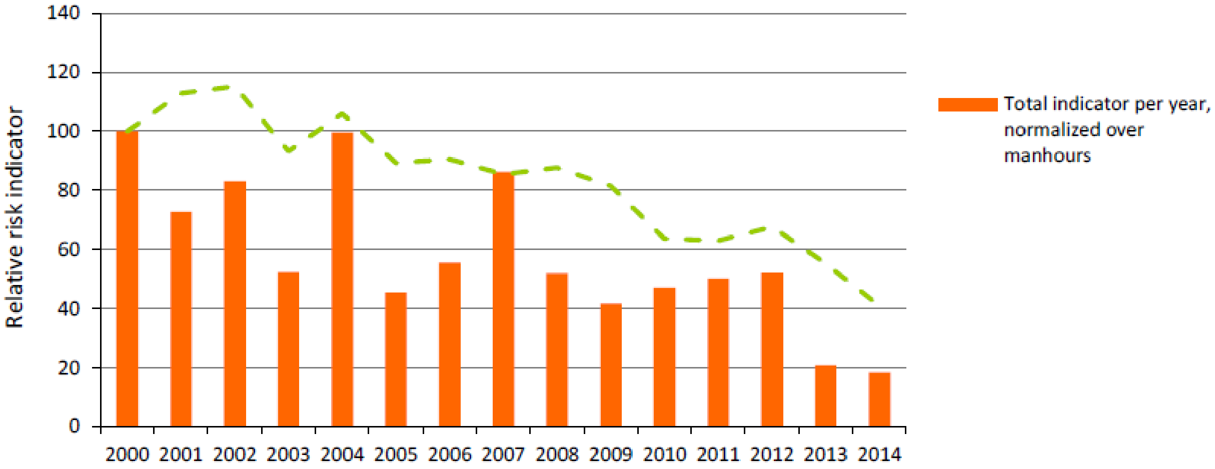


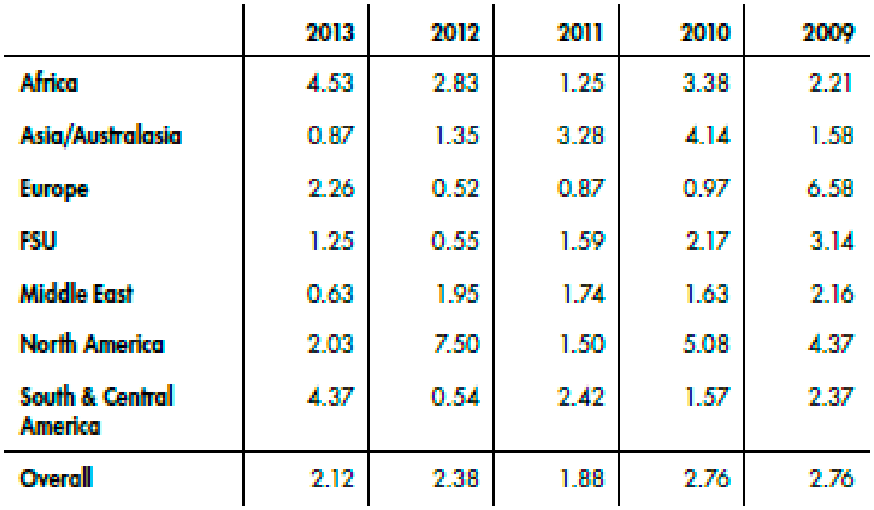
Figure 18: ***Total indicator, production facilities, normalised against working hours, annual values and three-year rolling average***

Case 2: Worldwide Offshore

Fatal accident rate (FAR) and Total recordable injury rate (TRIR) will be used as a reference in order to determine the development of major accidents globally. This section will present FAR and TRIR data obtained from International Oil and Gas Producers database. These data will be classified by function and by region.

According to IOGP in (OGP, 2013) FAR is the number of fatalities per 100 million hours worked. Also, Total Recordable Injury Rate is defined as the number of injuries (fatalities+ lost work day cases + restricted work day cases+ medical treatment cases) per 100million hours worked FAR values will be used as the basis to show the trends and development offshore globally with respect to major accident risk. FAR values from key functional areas such as exploration, drilling, production will be emphasized. These data were sourced from IOGP 2013 who got key input from partner companies and contractors in the industry.

Fatal Accident Rate FAR and Total Recordable Injury Rate (TRIR) Trends by Region



	2013	2012	2011	2010	2009
Africa	4.53	2.83	1.25	3.38	2.21
Asia/Australasia	0.87	1.35	3.28	4.14	1.58
Europe	2.26	0.52	0.87	0.97	6.58
FSU	1.25	0.55	1.59	2.17	3.14
Middle East	0.63	1.95	1.74	1.63	2.16
North America	2.03	7.50	1.50	5.08	4.37
South & Central America	4.37	0.54	2.42	1.57	2.37
Overall	2.12	2.38	1.88	2.76	2.76

Table 1: Fatal Accident Rate by region culled from OGP Safety Performance Indicators 2013

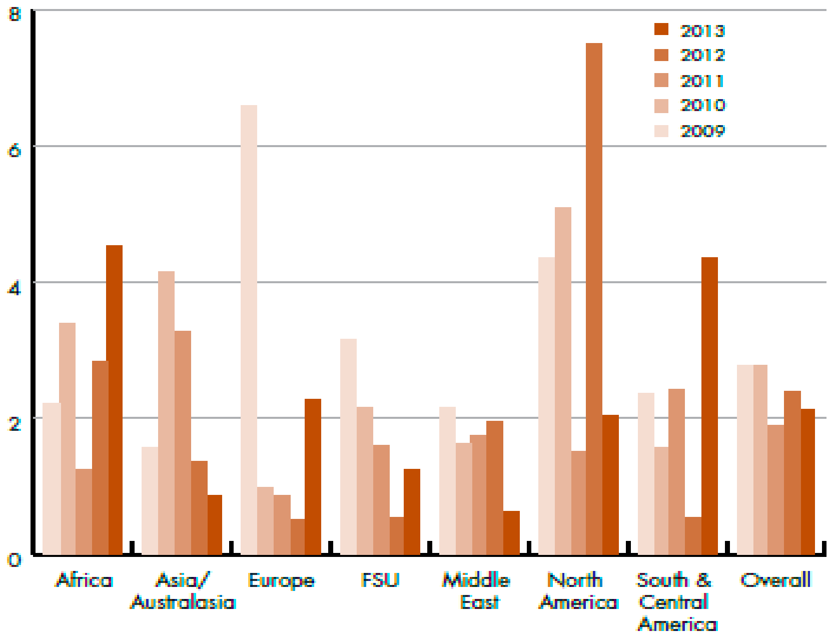
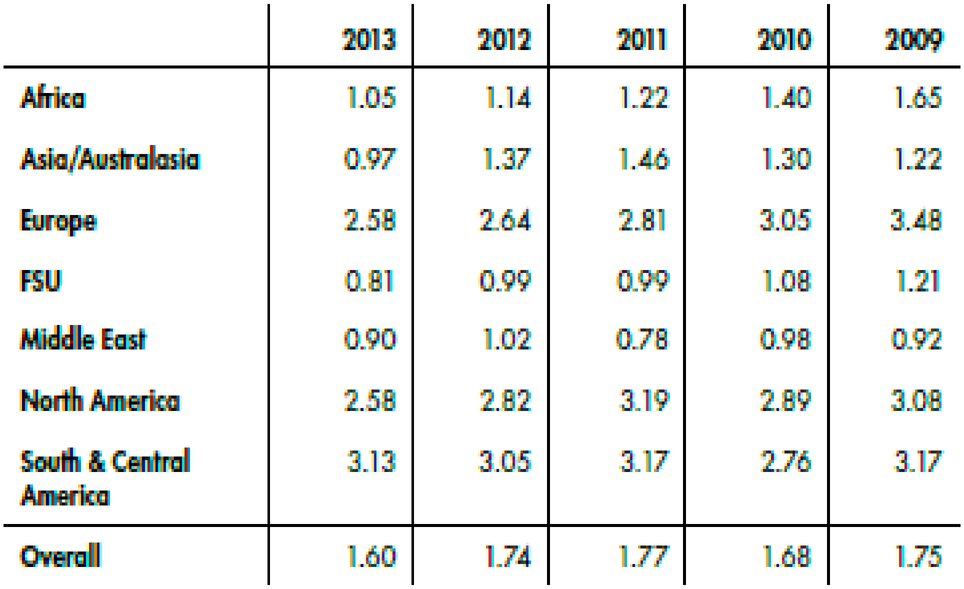


Figure 19: Chart Showing Fatal accident Rate trends for the last 5 years by region culled from OGP Safety Performance Indicators 2013

From the chart above it can be seen that there has been a huge drop in fatalities in the Middle East, North America experienced a spike majorly because of the Macondo accident. Meanwhile, the FAR values for the European zone decreased immensely between 2009 and 2012, although there was a huge spike in 2013. In Africa and South America there has been an increase in the FAR value between 2009 and 2013 while the Former Soviet Union and Asia saw decreases in their FAR values. In conclusion, the FAR globally has reduced a bit from 2, 76 in 2009 to 2.12 in 2013.



	2013	2012	2011	2010	2009
Africa	1.05	1.14	1.22	1.40	1.65
Asia/Australasia	0.97	1.37	1.46	1.30	1.22
Europe	2.58	2.64	2.81	3.05	3.48
FSU	0.81	0.99	0.99	1.08	1.21
Middle East	0.90	1.02	0.78	0.98	0.92
North America	2.58	2.82	3.19	2.89	3.08
South & Central America	3.13	3.05	3.17	2.76	3.17
Overall	1.60	1.74	1.77	1.68	1.75

Table 2: Total Recordable Injury Rate by Region culled from OGP Safety Performance Indicators 2013

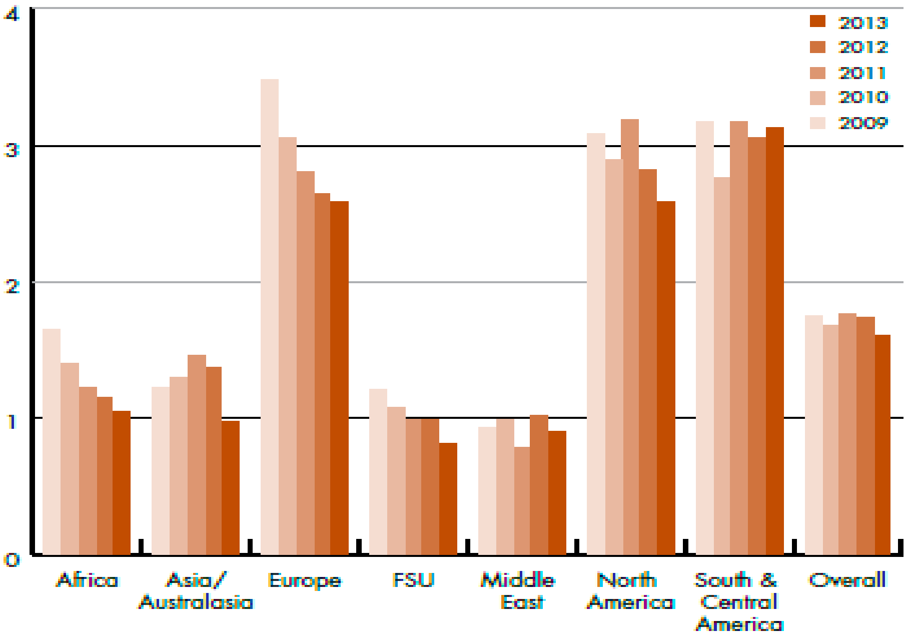
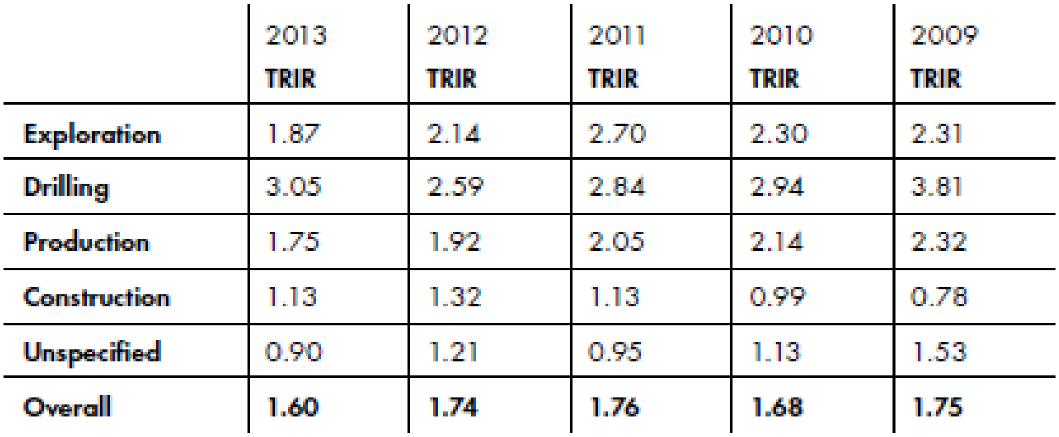


Figure 20: Chart showing the trends in Total Recordable Injury Rate from 2009-2013 culled from OGP Safety Performance Indicators 2013

From the Figure 20, it can be seen that the Total Recordable Injury rate was significantly high in Europe, North America and South America. There was a slight reduction in TRIR values for these 3 regions although they were not as significant as those experienced by Africa, Asia, Former Soviet Union and the Middle East, overall there was a slight reduction in the total recordable injury rate from 1.70 to 1.60.

Fatal Accident Rate FAR and Total Recordable Injury Rate (TRIR) Trends by Function



	2013	2012	2011	2010	2009
	TRIR	**TRIR**	**TRIR**	**TRIR**	**TRIR**
Exploration	1.87	2.14	2.70	2.30	2.31
Drilling	3.05	2.59	2.84	2.94	3.81
Production	1.75	1.92	2.05	2.14	2.32
Construction	1.13	1.32	1.13	0.99	0.78
Unspecified	0.90	1.21	0.95	1.13	1.53
Overall	**1.60**	**1.74**	**1.76**	**1.68**	**1.75**

Table 3: Total Recordable Injury Rate by Function from 2009-2013 culled from OGP Safety Performance Indicators 2013

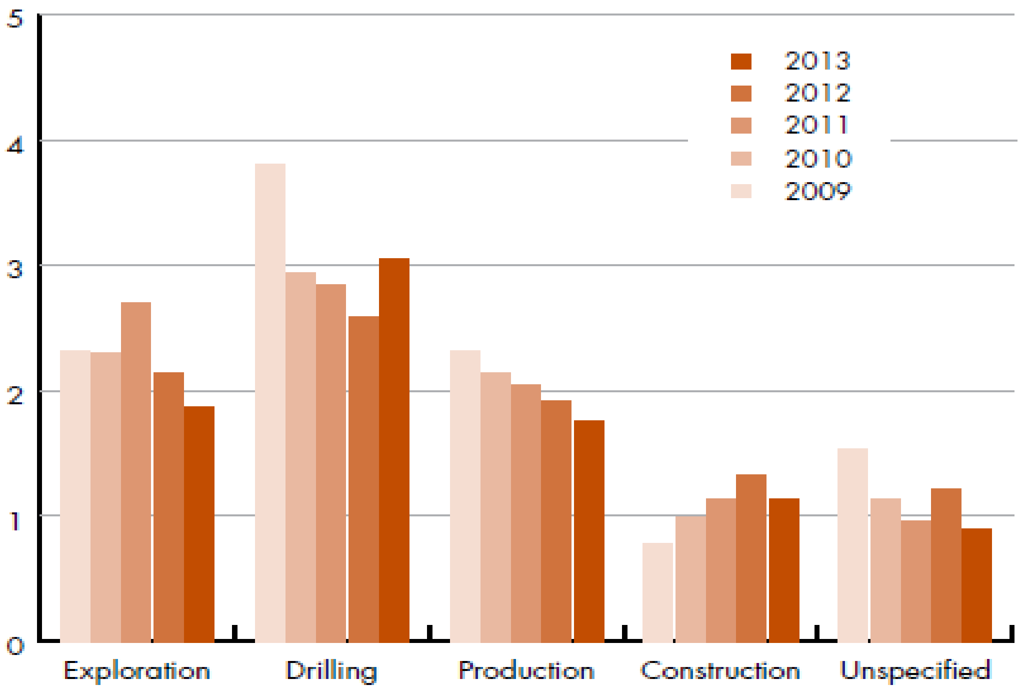


Figure 21: Chart showing Total Recordable Injury Rate by Function from 2009-2013 culled from OGP Safety Performance Indicators 2013

In the Figure 21 it can be seen there has been a stable reduction in the total recordable injury rate in exploration and production. However, there has been a spike in TRIR for construction and drilling, overall the total recordable injury rate has reduced from 1.75 to 1.60 between 2009 and 2013

.

Comparison between Accident Risk on the Norwegian Continental Shelf to Worldwide Offshore

According to PSA, the last major accident to occur in Norway to involve fatalities was a helicopter incident in 1997. However, there have been a couple of fatal accidents occurring worldwide as was shown in the FAR and TRIR data. One of such occurrences that offers a common incident is the case of helicopter accidents on the United Kingdom Continental Shelf. This comparison is good since it is also similar to the helideck, air traffic management indicator that was discussed earlier.

Apart from the helicopter incident on the Norwegian Continental Shelf in 1997, there have been no reported fatalities, meanwhile on the UKCS there have been 5 helicopter accidents in the last 5 years where 2 of them were fatal. In 2012, there were two emergency landings on the sea in the UK sector, and one controlled emergency landing on a facility in the Norwegian sector (PSA, 2014).

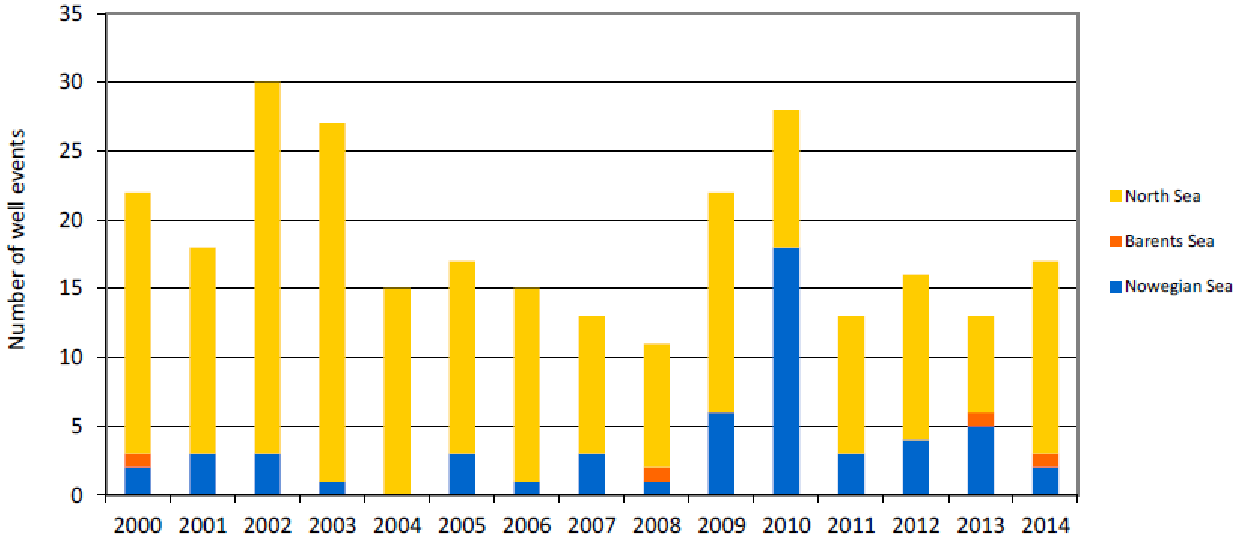


Figure 22: ***Distribution of well control incidents by areas, 2000-2014***