Faculty of Science and Technology

MASTER'S THESIS

Study program/ Specialization: Offshore Technology Risk Management	Spring semester, 2015 Open access
Writer: Amanj Sheikhi	(Writer's signature)

Faculty supervisor: Professor Eirik Bjorheim Abrahamsen

Thesis Title:

On How to Describe Security Risk?

Credits (ECTS): 30

Keywords: Risk Risk Analysis Risk Management Security Terrorism Decision-making Decision-making principles	Pages: 62 Stavanger, 19 June 2015

University of Stavanger

Master Thesis

Faculty of Science and Technology

Title: On How to Describe Security Risk?

Amanj Sheikhi

Stavanger, 19 June 2015

Abstract

The word terrorism is one of the most-used terms in a daily life of people in this century. Governments and organisations apply many different definitions to cope with their existing issue(s). Thus, the terrorism risk evaluation is one of the most important matters in today's life. Many contributors involve in this process worldwide, and each organization or government has its preferences and definition. In Norway, several parties involve in the risk assessment investigation, i.e. (Egeli, 2014). Thus, using a standard procedure for the risk evaluation in this area is of interest. For this reason, the two Standard are considered (*NS 5831*, 2014, *NS 5832*, 2014).

The issue is to compare the existing scholarly literature within the area of security risk assessment with the standard procedure for security risk assessment in Norway to find the possible weakness points. The thesis discussed the most significant weakness points of the Standard and concluded that the four top points need reviewing and changing. The weakness points are risk definition, risk picture, strategies to deal with the risk, and applying the reducing measures.

At the end, the risk analysis may end up with the various alternative of different types each has its value and, therefore, the analysis compares them to each other to find the most suitable result. Standard suggests to find the threat from different contributors include technical, organizational, and human resources. The various contributors have different values, for example, the value of statistical life, damage to the infrastructure, and damage to the environment have not the same values and comparing them is a controversial task. According to Abrahamsen et al. (2011) the only way is to transform all attributes into the one comparable value. They stress that these frameworks are tools to help the decision-maker having the most useful and reliable decision and hence, the tools should take carefully to avoid the mechanical and decision-making process. Furthermore, the ALARP and the cautionary principle applies for both safety and security sector in the risk assessment to balance the situation safely and financially. The thesis focuses on the security standard in Norway, and suggest other Standards and Regulations for further work in this area.

Keywords: Risk, Risk Analysis, Risk Management, Security, Terrorism, Decision-making, Decision-making principles

Acknowledgement

I am grateful for being graduated after a long period of essaying to be what I wanted to be. I am more cheerful than ever for making my master thesis done. The long distance I was through to do it did not seem easy at the beginning but the best person who could ever guide all over the way Professor Eirik Bjorheim Abrahamsen made it ongoing to the end. He did his best to give me plenty of ideas within my topic, gathering data and a lot of other perfect and genuine hints.

This remarkable ending of my studies at University of Stavanger and the whole life I had here in Stavanger made me braver than ever to maintain on competing with challenges I have faced or I may encounter in aspect of life. I hope to take as much advantage as I can by the means of knowledge to the rest of my life path.

University of Stavanger, 19 June 2015

_____

Amanj Sheikhi

Abbreviations

ALARP	As Low As Reasonably Practicable
BAT	Best Available Technology
BRTF	Better Regulation Task Force
CBA	Cost-benefit Analysis
E[NPV]	Expected Net Present Value
ETA	Event Tree Analysis
FAR	Fatal Accident Rate
FIZ	Fuzziness, Incompleteness and Randomness
FTA	Fault Tree Analysis
ICAF	Implied Cost of Averting a Statistical Fatality
IR	Individual Risk
MC	Monte Carlo Simulation
ME	Method of Moments
ML	Method of Maximum Likelihood
MTO	Man, Technology, and Organization
NPV	Net Present Value
PDF	Probability Density Function
PLL	Potential Loss of Life
PMF	Probability Mass Function
PRA	Probabilistic Risk Assessment
PST	Politiets sikkerhetstjeneste
TOR	Tolerability of Risk
VSL	Value of Statistical Life

The word Standard in this document refers to Norwegian standards for risk management and risk analysis (*NS 5831*, 2014, *NS 5832*, 2014), respectively.

Table of Contents

List of Figures, Table, and Examples

The following lists address all figures tables and examples in this document.

Figures:

Table:

Examples:

1 Introduction

1.1 Background

There exist several parties that involve in the risk assessment investigation in Norway, e.g. (Egeli, 2014). They are the most contributor in risk evaluation and each of which may have its procedure. It is of the great interest to know whether they use the precise definition of risk and its critical elements. Hence, the existing standard procedure shall be assessed to ensure that they are fruitful for the defined purposes and serve the society's interest. The Standard is the reference for any investigation within the prescribed area and, therefore, it is crucial to reflect the meaningful assessment procedure.

Furthermore, presenting risk picture may lead to different uncertain variables like in the terrorist risk assessment or the MTO (Man, Technology, and Organization) method for offshore safety assessment. Indeed, the impact of the terrorist attack is different for the society, economy and politic and, therefore, the result may show outcomes of various types. There exist different views on decision-making when facing the uncertainty that are mostly about applying the risk reducing measures in connection with an economy that is of interest.

1.2 Challenges

The challenge is to define the risk and to present the risk picture in a way that covers all areas of the risk. The key aspect of risk assessment when facing to complicated situations is uncertainty, so, the risk picture should highlight this aspect. Different approaches to risk highlight various aspects, therefore, finding the appropriate approach to risk assessment is of interest. The widely used approach is the probability-based risk assessment (PRA), and many works have been done worldwide within this area in the industries, ref (Bedford and Cooke, 2001; Vinnem, 2014). Aven et al. criticised this approach to risk analysis and mentioned that the PRA can not highlight uncertainty (Aven et al., 2014). Hence, for assessing the risk in the social security section or the offshore industries, the analyst faces to uncertain elements and enormous consequences. It is suggested to use the uncertainty-based risk assessment that involves modelling, knowledge evaluation and surprise assessment.

For the purpose of security risk assessment in Norway, two Standards reviewed which are (*NS 5831*, 2014, *NS 5832*, 2014). They apply to risk management and risk analysis respectively. The definitions and procedure for the assessment shall be reappraised to find any

possible vagueness in the definitions and the procedure. There are many examples that are not clear and do not give any message for further steps in these Standards. One example is about risk description according to (*NS 5832*, 2014). The Standard defines pure risk as the potential for loss and not the potential of profit. Another example is choosing strategies in proportion to the risk that may have wide implication in the society. One alternative strategy is to transfer risk to other. With these two examples, the author convinced that it is necessary to review the Standards in depth to find whether it is appropriate for the terrorist risk assessment. There are some weakness points either in the used approach or in the risk definitions that considered in this thesis.

The second part is also close to this area. It is about presenting a risk in a practical way to decision-makers that is useful to finalise the situation with the most suitable decision. Some economists may prefer traditional cost-benefit analysis to transfer all aspects to money while others challenge this model and prefer the multi-attribute analysis to avoid transferring non-market issues into money. Abrahamsen et al. argued that all uncertain variables of different types shall transfer to the unique value having consistent and transparent decision-making(Abrahamsen et al., 2011). Presenting the existing discussion in this area is of interest.

1.3 Scope and Limitation

The thesis reviews the Norwegian standard for the security risk assessment to answer the question; to how extent the Standard for the security risk analysis is fruitful? Moreover, the author presents the existing literature on decision-making and combine them to have a useful overview.

In some sources, threat mentioned as terrorist and sabotage for the security risk assessment, e.g.,(Guikema and Aven, 2010). In this thesis, we consider threat as the terrorist attack and do not mention sabotage because many of them are not group work for political reasons. In general, the sabotage is not as clever as a terrorist attack with an adaptable plan.

1.4 Content

The first part ofter the introduction contains review scholarly articles and books. In this part, security risk assessment presents alongside with two approaches to risk assessment to show the applicable area for each approach. Although the PRA has a wide application the weakness points of this process presented in the literature. The presentation clarifies to how

extent the uncertainty assessment is necessary. Furthermore, several tools are presented for the process of decision-making.

The third part reviews the Norwegian standard for security risk assessment. The Standard contains the requirement for evaluating the security risk. Hence, Standard shall contains clear definitions and straightforward procedure. Thus, §3 presents the Norwegian standard for security risk assessment, and §4 is the discussion about the Standard and decision-making. Conclusion and further work present in (§5).

2 Theory

2.1 Different Approaches to Risk Assessment

Reminding §2.2.3 in Willis approach the probability, and the expected values are considered to calculate the risk. This approach calls probability-based assessment (PRA), which has some weakness points. In this section, two different approaches to risk and the associated risk picture present according to the literature.

Risk analysis comprises of three main steps; planning, risk assessment, and risk treatment. Planning step aims to identify the problem, organising works and obtaining information. This step defines the possible measures and the acceptable level of risk. In the second step, analysts should determine the causes/threats, consequences, and the probability of occurrence. The last step is risk treatment that carries out to assess the measures, comparing all available alternatives, managerial review and decision making at the end. For short, The risk assessment involves identifying threats, analysing causes and consequences also defining the risk picture at the end (Aven, 2008). Defining the risk picture is the key point of different perspectives of risk that highlights various aspects of risk.

2.1.1 Probability-Based Risk Assessment (PRA)

Many different descriptions of risk are available from the traditional perception of the risk to the new perspective that applies for scientific reasons see, e.g.(Veland and Aven, 2013). Mostly, the risk introduced as probability and the expected value. In this sense, The risk defined as a triplet (s_i, p_i, x_i), ref (Kaplan and Garrick,1981 mentioned by Bedford and Cooke, 2001). In this risk picture, "s" is the scenario, "p" is the probability of occurrence, and "x" is the associated consequences. Thus, probability plays a significant role in this risk picture, and analysts pay the considerable attention to the probability calculation using any appropriate model(s). The risk have been described more widely as (A, C, P) in which A is an undesirable event, C is the consequences, and P is the probability describes in either relative frequency or subjective probability. In this approach, the analyst assigns the probability number for each unfavourable events (Aven, 2011). This risk picture defines the risk as the undesirable event, associated consequences and the likelihood of occurrence of both events and consequences.

The PRA relies on the probability and the expected values for undesirable outcomes. The approach aims to define the expected value of all possible causes and consequences in the

assessment. The PRA consist of six steps that present shortly in the following, ref (Aven et al., 2014).

- Identification of threat/hazard: it is the first step, consist of understanding the system application to find the proper condition of the system. There is a different contribution to safety and security assessment that introduced in (§2.2.2).
- Cause Analysis: this step is to identify the condition of changing from the standard situation to hazard/treat.
- Consequences Analysis: the possible effects of each threat/ hazard identify in this step. For each scenario of an accident/attack, the fault tree implement to identify the avoiding barriers and the paths leading to the initiating event. On the other side of the bow-tie diagram, the event tree is used to identify the mitigating obstacles and possible consequences, see Figure 2.1.
- Probabilistic Analysis: analysts determine the probability of occurrence for each scenario. In this step, analysts can find scenarios with significant consequences and high probability of occurrence. However, the modern approach shall consider the scenarios with low probability and enormous consequences.
- Risk Description: Based on cause and consequences analysis, analysts illustrate risk picture and risk matrix for each scenario. Risk matrix helps to identify the major scenarios. Some indicators use to describe the risk such as potential loss of life (PLL), fatal accident rate (FAR), and individual risk (IR).
- Risk Evaluation: in the last step predetermined criteria compares to the result of risk analysis and if necessary measures apply to reduce the risk to the tolerable level.

However, in the security risk analysis there is no clear sign of developing a problem. Hence, the analysis needs more reliable data from different sources together with expert judgement. It seems clever to use the word undesirable event instead of an initiating event in the security risk assessment because the associated consequences might be enormous and irrecoverable.

The most used probability interpretation in PRA is the frequentist probability. Frequentist probability of an event A defines as the fraction of time event A occurs if the experiment repeats (hypothetically), in a long run. If the considered test or operation occurs n times, and event A occur n_A times then, frequentist probability is defined as the limit of the ratio between n_A and n when n goes to infinity. This probability is considered to be converged on a

number in the long run under a particular condition, ref (Aven and Reniers, 2013). Hence, this probability defines as;

$$P_f(A) = \lim_{n\to\infty}\left(\frac{n_A}{n}\right)$$

Running the test or operation, for many times, result in some actual probability that describes the aleatory uncertainty in a quantitative way. However, the analysts cannot repeat the test for infinite times because the physical characteristics of the components degrade. Therefore, the circumstance does not meet the "similar condition" in reality. Thus, it is just a model to describe the real phenomena where the considered population is always finite. Assuming that the probability exists, and it is the same in all independent experiments, the frequentist probability can be applied. Nevertheless, it is utterly impossible to make a defect in the particular machine for many times, without changing characteristics of it as assumed but for practical reasons it is possible to adapt the frequentist probability. For more information on justification, see (Aven et al., 2014, p. 32).

In oil and gas industries the situation, for example, a defect in the system components, might be different from time to time. In this manner, analysts make a frequentist probability model for system components and hence, according to their reliability block diagram the likelihood of initial event calculates e.g. leakage[1]. Reminding §2.2.2, the probability of a terrorist attack or other issues within the security sector is subjective.In subjective probability, experts assign the probability of an attack based on the background knowledge and their judgement, more discussion at §2.1.2.

2.1.1.1 Probabilistic Models and Application to the Risk Analysis

Many statisticians apply the probability models to calculate the uncertainty involving in the experiments. The problem of implementing such models arise when considering the epistemic uncertainty. For example, the models like Markov chain has application in physics and mathematics because, mostly, the experiments in this area involve aleatory uncertainty regarding the observation. Indeed, a physical experiment involves a chain of successive events which applies to the availability and maintenance.

[1] The probability of defect in many critical components in industries especially for oil and gas is collected in the handbook so called "Offshore Reliability Data Handbook"(*OREDA*, 2002).

For the purpose of probabilistic modelling, analysts use known distributions with the expected values for parameters, ref (Bedford and Cooke, 2001). In this approach, the likelihood of each undesirable event models mathematically and, therefore, the distributions play the key role in the assessment. The probabilistic modelling and its calculation has a link to data and expert's consideration. However, some experts argued that focusing on the probability numbers and distribution camouflage the uncertainty regarding causes and consequences, ref (Abrahamsen et al., 2010). Some probabilistic models present in this section due to their application in the risk modelling together with their pros and cons to the risk assessment.

2.1.1.1.1 Markov Chain

Researchers have adapted Markov chain theory to solve numerous scientific problems like Paul Ehrenfest to solve some thermodynamic issues(Ghahramani, 2005). Thus, applying this method to solve another stochastic process might be possible. Markov analysis is the method of quantification. Nevertheless, the transition is an evolution in the system or degradation of a system components, as long as the change meet the circumstances Markov chain applies to solve the probability transition. According to Aven et al., the FTA can be used to calculate the transition parameters of Markov chain (Aven et al., 2007).

Markov analysis is a useful model in the context of availability and maintenance analysis. However, it is not easy to formulate realistic problems such as in offshore disaster or the terrorist attack. It is not well-suited to predict all possible failures and unforeseen. Additionally, it is not always easy to calculate the steady-state probability of the future events. On the other hand, the result from the model is just one probability number that does not contain useful information in practice. Furthermore, Markov analysis focuses on the rate of happening. Thus, it jumps from the start point to the probability numbers. The model focuses on the probability numbers and therefore uncertainty regarding causes and consequences are missed(Abrahamsen et al., 2010).

The second weakness point of the Markov analysis arises when considering the exponential distribution for continuous Markov chain. Although it takes into account the chronological order of events for continuous Markov chain the time between transitions is exponentially distributed while not all process in industries follows the exponential distributions. In the terrorist risk assessment, the steps does not depend on any known distributions and the continuously chains has no application to our purposes. The third point is absorbing state that does not present the status of the system and just shows the outcome of the

function. Also, the absorbing state does not depend on the type of failure or failure time. In a word, this state does not help to understand the system. The last but not the least point about the Markov process is the order of the steps. In the security risk assessment, the three factors play the same role according to Willis. It means threat, vulnerability, and consequences should cover the critical area and, therefore, they do not come one after another like in the Markov process. The Markov process is a stochastic process and like many other models focuses on the aleatory uncertainties. Markov chain can not reveal the epistemic uncertainty, i.e. (Ghahramani, 2005; Levin et al., 2009).

2.1.1.1.2 Monte Carlo Simulation

Monte Carlo simulation is a mathematical model to simulate the probability rate of the undesirable events. The simulator applies to consider the effect of uncertainty in risk assessment. This technique is well-defined in some part of science such as portfolio analysis, corporate finance, and reliability analysis. Additionally, the procedure applies as a numerical tool to solve the mathematical issues. For example, the simulation applies to calculate the integral in the Bayesian formula.

In the probabilistic risk assessment, (PRA) historical data and expert judgement are two fundamental key points to predict the future. The data and expert consideration lead to a stochastic model such as in Bayesian updating and Monte Carlo Simulation. Indeed, analysts estimate the future using some models, and the estimation is, of course, involve uncertainty. For example, in construction industries engineers try to estimate the time and cost of the project with previous data and experts opinion.

The result of the assessment is, therefore, a probability number and there is no further information about the event(s). The calculation can be a little bit accurate if we use the range of maximum and minimum value beside the average one. Shortly, Monte Carlo simulation (MC) allows to mix different distribution for differents elements of the analysis. The model can choose the data randomly from each defined parameter and calculates the outcome. Moreover, the simulator can repeat the process of choosing randomly and calculate the likelihood for many times. This section is conducted according to Raychaudhuri (2008)and Earl and Deem (2008).

Unlike the Markov process, the MC Simulation does not apply the sequence of events in a chain. The MC simulation takes all involved parameters into consideration, simultaneously. The model is based on the repeated random experiments when the result of statistical data is unknown. Another advantage of the model is to use the numerical rules instead of mathematical solution for the equations. However, choosing the appropriate scenario for the experiment is

not an easy task. Experts evaluate the scenarios and then rate them from the best scenario to the worst one. Another difficulty is to consider several scenarios in the simulation and the only way is to use a computer software such as; Oracle Crystal Ball and @RISK from Palisade.

Defining the parameters is the first step of applying MC simulation. In this stage, all necessary parameters define to use in the MC model. It seems this step is more judgemental according to the expert's opinion and similar previous conditions.

Assigning the appropriate distribution of each parameter is the next step. A distribution describes each parameter either discrete or a continuous one. For example, binomial and Poisson distribution are discrete, and normal, exponential, and Weibull are continuous distribution. The analysts try to fit existing historical data into a known distribution. This process is called fitting. Fitting means using numerical methods to fit the data into a probability distribution that is suitable. In fact, fitting is the calculation of the distribution parameter. Three methods mentioned in the literature for data fitting such as; Method of Maximum Likelihood (ML), Method of Moments (ME), and Nonlinear Optimization. According to Raychaudhuri (2008), Maximum Likelihood Estimation has the better answer than ME method however it is sometimes difficult to apply this model even with the computer.

The third step is to choose a variable for each parameter as random. The MC method helps to generate the sequence of numbers as random. Thus, the probability defines using all selected variable in the trails. Of course, choosing a number in each trail is uncertain but the complex process involves possible outcomes that may neglect in the model.

The trail repeats many times to calculate the probability. The most common method for generating random variable is (RV`s). For generating random variables from distribution, we can apply inverse transformation method. This method works with the inverse of probability density function (PDF) or the inverse of probability mass function (PMF).

Monte Carlo simulation considers all involving parameters of real system likewise time dependency and failure behaviour. Moreover, this method avoids error-prone tasks like a vast numbers of spreadsheets in FTA (Fault Tree Analysis) and ETA (Event Tree Analysis). However, the simulation time is almost high, for example; 100,000 trailers is done within 8 hours for a stratospheric balloon risk assessment(Aven et al., 2007). Mostly, the MC method considers the aleatory uncertainty associated with the data collection and mathematical model. However, the method neglects the epistemic uncertainty about the process.

In line with MC simulation and mainly for probability-based risk assessment finding the appropriate distribution is of the primary interest. Thus, analysts try to build the distribution,

according to the available data. The data mentioned above which is used to make a model can be either historical or a new observation. In this manner, different techniques presented to make the proper distribution, according to available data in the literature. For this reason, Method of Maximum Likelihood(ML), and the Method of Moments(ME) can be applied, e.g.,(Haimes, 2005; Raychaudhuri, 2008).

Haimes (2005) believes that the worst-case scenarios occur in the tails of the distributions. This author emphasised that analysts pay the considerable attention to the mean value of the distribution and keep less attention to the tails of the considered distribution. The tails of a distribution show the unforeseen with a lower probability of occurrence and severe consequences. Additionally, Aven (2010) stated that the variance make the difference between the mean value and the tails of the distribution.

Furthermore, focusing on the average value may lead to choosing the different distribution with different tails. For example, Normal and Uniform distributions have the same mean value while their tails are different and extreme events occur in this part of the assigned distribution. Shortly, choosing the appropriate distribution and careful attention to design the tails is the challenging part of the PRA (Haimes, 2005).

Monte Carlo simulation has the vast application in economic risk evaluation by considering the effect of various parameters. The model let the analysis to repeat the calculation for many times and consider different variables simultaneously. However, for the security risk reasons the variables are complex to define a distribution and future events are more ambiguous to predict with this simulation. In short it might be possible to combine the existing data from different sources with this model for very limited decisions but assessing the risk of terrorist attack is not the scope of this simulation.

2.1.1.1.3 Bayesian Inference

The formula came to open by Thomas Bayes in 1763 for the first time. The method is now one of the strongest approaches in the statistical inference. Professor Dennis V. Lindley, the most advocate of Bayesian updating, stated that the Bayesian inference has as equal rank as the equation of Einstein and fundamental rules of genetic (Lindley, 2013). It tells us how to update the likelihood of events with newly acquired information. Lindley relied on the inference as a complete tool to update uncertainty. In his view, any further parameter and function to value uncertainty is related to our understanding but is not necessary. The argument of Lindley is correct as long as the distribution and applied models reveal all aspects of risk. However, the unforeseen is a rare event with a very low probability of occurrence, e.g., (Taleb, 2010). The

unforeseen may not expose in the central area of the distribution, i.e. (Haimes, 2005). The posterior distribution for the sample of "n" observation is;

$$f(\theta \mid x_1, x_2, ..., x_n) = \frac{f(x_1, x_2, ..., x_n \mid \theta) f(\theta)}{\int f(x_1, x_2, ..., x_n \mid \theta) f(\theta) d\theta}$$

The prior distribution of the marginal density of parameter θ is $f(\theta) = \int f(x, \theta) dx$. Since the denominator in is at most one, the posterior distribution is almost equal to the multiplication of prior and the likelihood function.

$$f(\theta \mid x_1, x_2, ..., x_n) \propto f(x_1, x_2, ..., x_n \mid \theta) f(\theta)$$

According to Bedford and Cooke (2001)there is a shortage of disagreement among experts either in the way of carrying out the inference or principles to judge the quality of estimation techniques. Experts believe that using MLE instead of Bayesian updating is an easier way to update the uncertainty about the parameter. The foundation of this argument is a dependency of Bayesian inference to the prior distribution. Note that the maximum likelihood estimator (MLE) derives from the maximum likelihood principle.

$$L(\phi \mid x) = \prod_{i=1}^{n} f(x_i \mid \phi)$$

Recall however in case of extensive observation, the role of prior distribution gets weaker, and the posterior distribution tends to converge to mass distribution at the real value of the parameter. In a word, the posterior depends on the new data. In the same manner, MLE tends to converge to the actual value of the parameter and, therefore, the two estimators has a similar answer. Hence, in the light of the big amount of new observation it is better to use the simpler inference that is off course MLE. Note that in MLE approach, it is not necessary to make a prior distribution.

The major difference between Bayesian and MLE is to choose a particular prior to Bayesian updating. The prior distribution for Bayesian paradigm is subjective, and every individual has a unique choice of this issue. As long as the prior is not objective the analysts try to find it with consensus. Nevertheless which model applies to make the prior distribution, two popular way of doing this task is to use expert judgement and generic data.

Concerning the Bayesian updating, if the distribution has one parameter φ, Bayesian updating writes as $P(\phi \mid x) = p(x \mid \phi) p(\phi) / p(x)$. However, some distributions have two parameters and, therefore, for the parameter of interest φ and a nuisance parameter ψ the inference writes as $P(\phi, \psi \mid x) = p(x \mid \phi, \psi) p(\phi, \psi) / p(x)$. In line with the formula, Professor

Lindley mentioned two difficulties in applying the model. The first barrier is summation over the parameters when calculating prior distribution and eliminating a nuisance that analysts use numerical methods to solve the integration. The second challenge arises when constructing the prior distribution.

Besides two difficulties in applying the model, the inference has attracted three serious criticisms. First, the prior distribution $p(\phi)$ in unknown. Second, the posterior distribution is subjective probability while the experiments and phenomena are objective(Lindley, 2013). Another criticism levelled at the model is that the model is unable to reveal the Black Swan, ref (Aven, 2013a according to Taleb, 2010).

Lindley praised the Bayesian inference, and he answered the censure in his book. Although parameter φ is unknown, the analyst has some information about the parameter before doing the experiment. Fundamentally, scientists make a new test collecting new data say, x, according to their understanding about φ. The critics stated that it is challenging to assign a proper distribution for prior φ and Lindley suggested doing further research into a method of assessment that lead to a better estimation of distribution and parameter(s). Furthermore, he agreed on this point that science is objective, and the probability is, of course, subjective. The author argued that two persons with different prior knowledge about an experiment led to an agreement in case of sharing a new observation. In a word, as long as the amount of acquisition is enough to dominate in the model then the Bayesian rule update their belief to almost a similar agreement(Lindley, 2013).

Moreover, Lindley did not accept the Taleb's point of view and wrote a review that is further presented according to Aven (2013a). Lindley mentioned that the calculation of probability is enough for considering uncertainty. He assumed sequences of the independent trail with constant chances of success, assigning the uniform distribution for prior distribution over the interval of zero to one $[0,1]$ and stressed that there exist a fraction of swans that is black. Hence, the probability of the black swan (Failure in the experiment) almost appear and it is, therefore, not outside of the scope of the analysis. However, Aven mentioned two false assumptions in Lindley's argument. First, the observation of Black Swan among the large population of the swan is not correct because the concept of black swan referrers to surprise extreme events. Second, when assuming the interval probability of black swan the uncertainty about a white swan is neglected. If the analyst assigns the prior probability for the white swan and then observation shows "n" white which n is a large population. Therefore, with Bayesian updating the likelihood of black swan observation is so small. For short, the inevitable

framework hides the possibility of surprises. In conclusion, this model is not enough to predict the surprises and alongside with the model, assessment should take the uncertainty into the consideration.

2.1.1.1.4 FTA and ETA

Fault Tree Analysis (FTA) applies to quantify the probability of occurrence of the considered events. FTA and Event Tree Analysis (ETA) applying based on the fixed order of events and, therefore, they do not consider the interaction between system function and the undesirable events correctly. To deal with this limitation, analysts may apply a dynamic method such as dynamic event tree. Figure 2.1illustrates a simple bow-tie diagram with Fault Tree and Event Tree in a threat assessment.

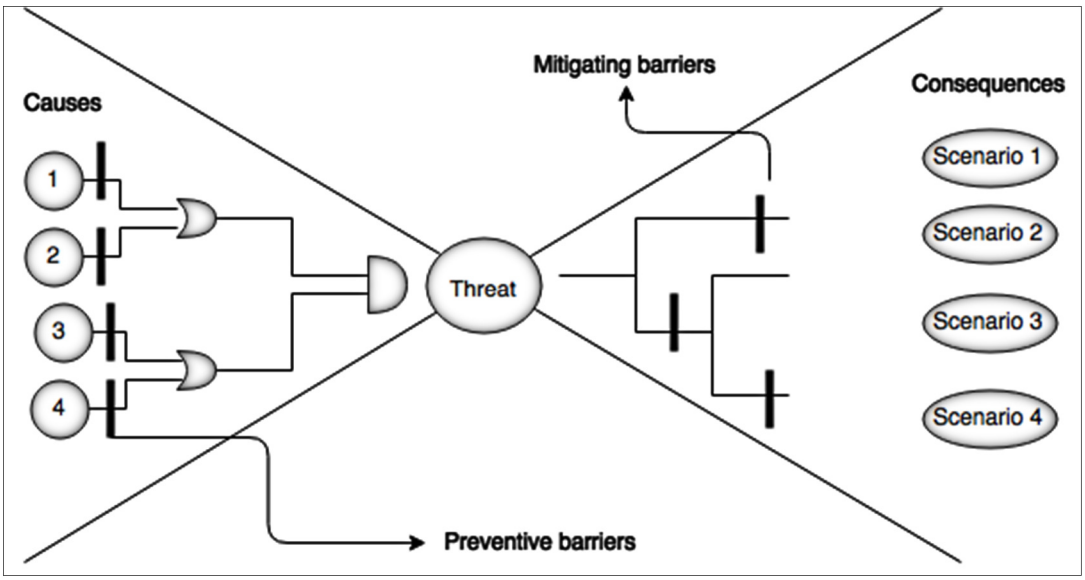

Figure 2.1: The bow-tie diagram with barriers, FTA, and ETA

FMECA cannot consider the redundancy of the system and FTA disregard the chronological order of events and ETA is time-consuming and error prone. FMEA, FTA, and Markov analysis need many assumptions. They are limited in dealing with the previous history of evolution. The memoryless feature of Markov chain let us forget the past and build the future upon the present values. However, for some reasons it is necessary to develop the model with all previous history of changing (Aven et al., 2007). Models are a mind-constructed algorithm that can cope with the existing ideas, and they are unable to predict beyond the designed framework.

2.1.2 Uncertainty-Based Risk Assessment

Aven stated that there is no guarantee that the probability numbers unfold all uncertainties involving in an experiment or phenomena, that is way the uncertainty should be an element of risk picture(Aven, 2010). Hence, it is necessary to introduce an integrated framework for the risk picture that can reveal all necessary factors. Abrahamsen et al. (2010) believed in the integrated framework for safety management as an event, associated consequences, and the uncertainty involving the process. Abrahamsen et al. stressed that probability is the measure of uncertainty, yet, the risk is neither probability nor the expected value. Using probability to describe risk camouflage the uncertainty involving in the events and consequences. Additionally, Aven et al. criticised the probabilistic approach to risk analysis and mentioned, the PRA does not consider background knowledge assessment and surprise evaluation (Aven et al., 2014).

Accordingly the risk picture in this approach can be (A, C, U, P, K) in which U represent uncertainty and K stands for the background knowledge. In this approach, analysts try to have a list of top-ten undesirable events with a low probability of occurrence and adverse effect. Besides, analysts assess the background knowledge to identify the most reliable data for the assessment, ref (Abrahamsen et al., 2010).

Accordingly, the probability interpretation refers to the subjective probability. Objective frequentist probability contains aleatory uncertainty about the experiments while, in subjective probability, the analyst describes the purely epistemic uncertainty about the future events based on the background knowledge.

This knowledge-based probability is a description of epistemic uncertainty, according to background knowledge of contributors. Thus, the probability of an event A given the background knowledge $P(A \mid K)$ is assigner's degree of belief for occurring the undesirable event “A” with background knowledge “K” of the assessor. Therefore, assessor embeds his/her degree of belief with a number. It is important to assess the background knowledge because the probability number depends on the assigner's belief, and any further investigation depends on the background knowledge. Consequently, the probability will change if the background knowledge slightly changes. With this point of view, the constructed model is different from time to time using new data and expert judgement.

Moreover, probability numbers should be interpreted in a way that can be understandable. This issue emphasised by Aven and Reniers (2013) that risk analysts should be

able to demonstrate the meaning of probability numbers. The paper mentioned above stated that probability should be meaningful in a way that helps managements and shareholders in decision-making.

The idea of interpretation for probability arises because people understand each phenomenon using comparing it to a known measure. For example, people compare the distance with the known standard calls meter, and they compare feelings about the weather with the known measures like degree Celsius or degree Fahrenheit. De Finetti (1930), judged the uncertainty regarding the occurrence of undesirable event equivalent with the uncertainty in gambling. On the other hand, Lindley (2013)interpreted the uncertainty associated with the undesirable event comparable with the uncertainty regarding an Urn Standard. Both interpretation model present bellow.

- **Interpretation regarding Betting**

Understanding and interpreting the reality depends on people's need and has a connection to the period of application. It seems that betting especially on horse racing was popular in the era of De Finetti; starting in the 20th century. This method presented by Aven and Reniers (2013) which rest on De Finetti(1930).

This approach is similar to the gambling situation. In this approach, Probability of occurrence for event A can be interpreted as the known procedure of gambling. The likelihood of event A compares the amount of money the assessor willing to put on the table if he/she would receive a single unit of payment if event A occurs, and nothing otherwise. Conversely, the assessor willing to pay the amount of $(1 - P(A))$ if he/she would receive a single unit of payment if the event "A" not occurs, and nothing otherwise.

- **Interpretation regarding an uncertainty standard**

This method developed by Professor Denis Lindley (2013).The assessor compares his/her degree of belief about the probability of occurrence of event A with a standard measure that is an urn. For example $P(A) = 0.1$ means that the assessor judge the uncertainty associated with the occurrence of event A with a standard experiment. The uncertainty is equivalent to the uncertainty regarding the occurrence of a standard event of drawing a particular ball from an urn containing ten balls. Also, the balls in the urn should be fair. Fairness means that (1) there is no any single difference between balls (2) choosing balls from the urn is in the proper way without cheating.

This measure helps to understand world's phenomena using urn experiment. If, for example, the probability number is so small then the number of corresponding balls in urn standard can be increased such that; the interpretation will be meaningful. Randomness[2]in drawing a fair ball is an equally important aspect of this interpretation.

It is possible to develop the argument to the more complex situation. For example, considering two undesirable events let's say "A" and "B" with a probability of occurrence, for instance $P(A) = 0.1, P(B) = 0.15$. Assuming an urn containing 100 balls in which 10 are red, and 15 are blue with all others in white. Then, the assessor can judge the uncertainty associated with the occurrence of both events, simultaneously. The event interprets as equivalent to the uncertainty regarding the occurrence of a standard event of drawing 25 coloured balls from this urn containing 100 balls.

Note that, although the Urn interpretation has a link to the classical probability of drawing a ball from an urn the subjective probability is different from the objective probability. In the Urn Standard, the assessor compares the uncertainty about the occurrence of a real event A, with the uncertainty about a mind-constructed event B regarding the Urn Standard. Drawing balls from an urn is a classical probability for a mind-constructed event not for the event A, and analysts use this probability to interpret the subjective probability.

2.1.2.1 Uncertainty

Three different approaches exist for understanding uncertainty. The most used approach divides uncertainty into the epistemic and aleatory types. Here, three different approaches present and the second one is the reference that applies to the upcoming sections of the thesis.

2.1.2.1.1 Ignorance and Variability

In this classification, uncertainty has two categories, ignorance and variability. Ignorance denotes the partial incertitude due to the limitation of the empirical study and further research; new information or using new techniques can reduce it. However, variability has an

[2] If there exist 'n' different elements for a particular sampling each in which has two choices, then there exist (2n) factors involved in the assessment, and that is so much to investigate. Moreover, assessor still in doubt about existing any other factors include in the experiment. Experiment should be out of any conflict, means no interaction. Samples choose randomly and check again to prove this to overcome this issue. " Random means that the withdrawal of the balls is not affected by anything"(Lindley, 2013, p. 47)

objective in reality that has no connection with new data or implementing new methods. The additional effort, in this case, can provide a better estimate, but the variability cannot be reduced(Ferson and Ginzburg, 1996).

2.1.2.1.2 Aleatory and Epistemic Uncertainty

Aleatory represent an unplanned situation that is more stochastic. Aleatory uncertainty relates to inherent variability that exists in the nature of phenomena, and it is irreducible. On the other hand, epistemic uncertainty refers to the lack of knowledge, and it is reducible. When analysts achieve to adequate information then, the probabilistic methods can be implemented to calculate the probability distribution. In contrast, information is very few and scattered for the condition of epistemic uncertainties to support objective probability. This condition results in subjective probability or interval specification in non-probabilistic methods.

In some situations, data involves both categories of uncertainty. It is possible to define the share for each of them in the total uncertainty, e.g. (Eldred et al., 2011; Sun et al., 2012)

2.1.2.1.3 Fuzziness, Incompleteness and Randomness

David Blockley (2013) classified uncertainty in three conceptually distinctive characteristics which calls FIZ (fuzziness, incompleteness and randomness). He believes that characterization of uncertainty into the two categories of epistemic and aleatory types is not clever enough to deal with the practical situations. Fuzziness is imprecision or vagueness of the definition. Let's consider this statement;

> "The risk related to riser/pipeline fire scenarios is small. Hence, the effect of protecting the escape routes from riser fires is small".

It is implicit either in the level of performance for escape routes and the intensity of the fire scenario. It sounds like epistemic to some extent, and it is reducible by increasing the information about fire scenario and level of performance for escape routes. Blockley according to Zadeh (1973) stated that since complexity increases in the system, the ability to make an accurate statement decreases until the precision and importance are mutually exclusive. For short, mathematic cannot model the fuzziness like in the theory of fuzzy sets.

Incompleteness refers to whatever the analysts do not know. It is a part of epistemic uncertainty, but it is neglected. The sum of all probabilities equal to one and everything in this interval drops in fussy sets and what analysts do not know is not assigned with classical

probability. Randomness defines as a lack of knowledge in the pattern. Therefore, it is aleatory uncertainty.

Assuming that $P(A)$ is the probability of occurrence of event A. These three types of uncertainty involve the calculation. The below-mentioned statement consists of both Fuzzy and incompleteness types of uncertainty.

> "The effect of protecting the escape routes from riser fires is small, but there exists some evidence to prove the importance of this improvement".

2.1.2.2 Black Swan

Black Swan refers to the surprise in the eyes of assessors. It means a dangerous situation might exist even if the analysts did not consider or understand that. In fact, the Black Swan concept says if there is no swan with black colour in the US it is possible to see many swans in black in other parts of the world (Taleb, 2010). The Black Swan concept is not new in the world, but it presented and popularised by Taleb in 2007 in the context of risk management. For example, it is mentioned by Blockley (2013, p. 31)that David Hume in 1739 doubted this statement "evidence from the past could be used as evidence for the future."

Taleb described the black swan with three features, ref (Aven, 2013b). First, it is outside of the normal expectations because nothing in the past can prove the possibility of an event in the future. Second, it has severe consequences. Third, after happening, it is easy to think about it, and it is explainable. Additionally, Aven divided the surprises into three categories (Aven, 2014a, p. 12).

- Unknown-unknown means these events and correspond probability are unknown for scientists. These events are difficult to include in assessments.
- Surprise events are in comparison with analyst's risk picture. These events do not appear in the risk picture as a result of risk assessment.
- Surprises with a very low probability of occurrence.

Aven mentioned that the first category is hard to predict. However, the second and third category of surprise events are known for assessors. The second one refers to events that the assessor do not believe in happening them. Those scenarios are beyond the investigation of the risk analyst team. It might be due to the complexity of scenarios. Besides, it is also possible to overestimate the strength of applied barriers. The third category indicates the events that has

mentioned in the investigations but neglected due to the low probability of occurrence. It can happen when the assessor does not verify the strength of the information.

To assess the surprises, Aven (2013) suggested an approach involving them in the risk assessment. The first step is, preparing all possible types of activities with low risk and address corresponding consequences and probability of occurrence. The second step is, reviewing all evidence of occurring these events. These two steps help to go insight the phenomena and predict the events that are possible to happen in the future. With this view, the MTO method can be the best approach for industries. The Standard(§3.4.1) suggested to find threats of different contributors include technical, organisational, and human resources. Similarly, for the purpose of the security risk assessment Abrahamsen et al. (2010)suggested the list of top-ten surprises for the safety section alongside with the probability-based approach. This method has, of course, application of the security section. The security police in Norway (PST) in the last report (NTV, 2014) summarised nine threats with the high impact in Norway and explained each in details.

2.1.2.3 Strength of Knowledge

In probability-based risk assessment, the procedure highlights the expected values and probability of occurrence. The risk defines with the expected value and certainly the probability calculation involves information, analysis, and expert judgements. The weakness point of the procedure is the used information and events beyond the scope of the analysis which mentioned as Black Swan in the previous section. The solution is to address the strength of the data. Aven (2013b) referred to that the strong knowledge the small level of uncertainty and suggested two methods of knowledge assessment.

- **Method 1 for assessing the strength of knowledge:**

In this method, direct grading and scoring are used to evaluate the strength of knowledge together with the probabilistic risk analysis. If following conditions exist, then the knowledge is inadequate.

- The assumption shows strong simplification
- Data are not available, or if any it is unreliable
- Experts do not have any agreement with modelling, assumption, and so on
- The mechanism of the phenomena is not well understood

In contrast, strong knowledge has these characteristics; availability of a reasonable assumption(s), reliable data, agreement among experts, and known mechanism for considered phenomena.

- **Method 2 for assessing the strength of knowledge:**

This method concentrates on identifying primary assumptions involved in the probabilistic analysis. Analysts use uncertainty factors for assumptions like the historical data to predict the future. Hence, uncertainty about assumptions should be clearly defined to understand the deviation of assumptions from established state. The scoring system shows the criticality of assumptions. If assumptions are strong, then corresponding deviation will be small, and then the uncertainty regarding the process is low.

2.2 Security Risk Assessment

2.2.1 Terror Definition

The word terrorism is one of the most-used terms in a daily life of people in this era. Newspapers and TV-news contain these terms or the similar expressions every day. Governments and organisations apply many different definitions to cope with their existing issue(s). There is no unique definition worldwide, and the term terrorism is more dynamic such that the world leaders nominate various groups in a different way over the time. Despite different political behaviour, terrorism definitions almost contain the same characteristics. PST (Politiets sikkerhetstjeneste) in Norway has this definition for terrorism:

> Terror activities are a serious crime, which often has a connection to the branches across the borders. Terrorist acts largely affect civil society, and the impact of terrorist acts go beyond the loss of lives and damage to property. It propagates through the fear and insecurity, ref ("Terrorisme | PST," 2014).

According to Matusitz (2013) most of the old definitions Involve three terms of (a)use of violence, (b) political objectives, and (c) propagating fear. The former terrorism propagated fear through using violence for political purpose(s). The goal was to attacks the particular target(s), and mainly secular groups used this method. However, the new terrorism behaviour indiscriminate objectives and attacks the large population. Mostly, it involves religious behaviour that deny other ways of life and try to propagate inflexible models of life. The old definition refers as classical terrorism while the modern and post-modern one aim to damage the population in high level, and also they use weapons. Moreover, post-modern terrorist use

extra powerful weapons such as chemicals and radioactive arms to suppress and eliminate their targets. The two features are, therefore, added to the definition. The first one is arbitrariness and indiscriminate targeting and the second one is to victimise civilians. It is crucial to have an integrated description to reflect all its aspects in the risk picture. Hence, the most used definition of terrorism presents here by Matusitz (2013, p. 4).

> Terrorism means creating fear by using violence for political or religious reasons.
> These intentional actions are mainly against civilians to reach a particular goal(s).
> Thus, terrorism is different from murder or the threats of the same level.

To clarify the effect of a terrorist attacks two example present below. The former example refers to as a classical terrorist attack (Terror in Sarajevo), and the latter one refers to as the modern terrorism (September 11th). These two short examples describe how the world will change after such undesirable events.

Example 2.1: Terror in Sarajevo

The assassination of Archduke Franz Ferdinand of Austria and his wife in Sarajevo on 28 June 1914 was the start point of the world war one that first was between Austria-Hungary and the Kingdom of Serbia. During four and a half year, many countries on both Entente side and central power side fought against each other. The Ottoman Empire helped Empire of Germany and Austria-Hungary(Cawood and McKinnon-Bell, 2002). The direct consequences of that war were about millions of fatalities, injuries and destroyed cities. The two significant consequence for the world war one were the revolution in Russia in October 1917 and Partitioning of the Ottoman Empire in 1920. Contributing the Ottoman Empire resulted in the creation of the new countries in the Middle East which causes many conflicts afterwards. The world war two was the indirect consequence of the world war one. Simply the terrorist plan by few people in Sarajevo resulted in the vast consequences in the history of the world.

Example 2.2: September 11th

The terrorist attack on September 11th, 2001 against World Trade Centre changes the history of the world. Many fatalities and injuries, collapsing famous stock markets worldwide, and the two wars in Afghanistan and Iraq were the direct consequences of the attack. Dropping economy in nearest and growth of radicalism in the Islamic countries and consequently in other areas are some of the indirect effects of that attack.

2.2.2 Safety and Security

There are several differences between the concepts of safety and security. Thus, security assessment and safety assessment highlight different elements of the analysis. For example, the sinking of the Sleipner A offshore platform (1991) was the safety failure, and the two case examples mentioned above were the security issues relating to the criminal plan of invaders. In line with these definitions Reniers and Audenaert (2014) aggregated many ideas about this two concepts that present here. The authors defined safety risk assessment as analysing probability and consequences while they defined security risk assessment by analysing target, vulnerability and consequences.

Table 2.1: The list of differences between safety and security

Safety	Security
Incident is undesirable and unplanned.	It is a man constructed plan.
It is the result of an individual or groups plan.	It is the result of human behaviour.
Seldom a malicious action, and mainly without any wishes for considered output.	Malicious action with wishes for the defined output.
Hazard is observable and tangible.	The threat is not observable and tangible.
The source is domestic.	The source is intentional.
There is no invader.	Caused by Invader.
Quantitative or qualitative probability of occurrence.	More qualitative approaches based on expert opinion. The probability of occurrence may be available in case of existing relevant information.
Risk is the nature of experiments and phenomena.	The threat is the nature of security-related risk with high degree of uncertainty.

This table ispired by (Egeli, 2014; Reniers and Audenaert, 2014).

The more precise definition of safety provided by (Aven, 2014b). Aven stressed that as long as events and consequences are unknown then we cannot mention high or low safety. Consequently, the term safety defines by reference to the acceptable risk. He adapted a graph that illustrated the safe situation within two risk approaches. In the probability-based risk assessment, the safe boundary is much smaller than the acceptable area of risk. In this approach, epistemic uncertainty involves the analysing procedure for both causes and consequences. Conversely, if analysts implement the uncertainty-based perspective then, the safe and

acceptable risk area coexist. Aven also believed that being in a safe area is a subjective judgement and, therefore, it defers from one institution to other. He believed that the probability is the measure of uncertainty, yet not all aspects of safety reflect in expected value and probability numbers. This issue presents widely in (§2.1).

In brief, there are three key differences between safety and security mentioned in(Guikema and Aven, 2010). First, terrorist risk adapt to the risk management program because it is a clever plan. The failure of the system may change due to the risk management program, but the initiating event does not alter. Second, there is no consensus among experts about using probability for the terrorist attack, e.g. (Aven, 2008) due to high uncertainty and The Black Swan(§2.1.2.2). Thus, calculating the probability of attack is difficult like in Willis approach (§2.2.3). Accordingly, a traditional cost-benefit analysis that revolve around comparing the likelihood of cost and benefit has not a real meaning. The third difference is the restriction to the loss of liberties. Thus, defining measures to reduce risk may interrupt the individual freedom.

2.2.3 Security Risk Description by Willis

Many researchers have been working on the concept of the terrorist risk assessment for decades. Each definition may highlight different aspects of the risk. However, the broadly used definition by the experts and analysts is the contribution of threats, vulnerabilities, and consequences(Willis and Rand Corporation, 2005)[3]. The Standard in Norway suggests almost the same contributors for the security risk assessment (§3). The three parameters present in the following paragraphs according to these authors. The probability of an attack defines as a particular threat and target with assigned consequences if a successful attack occurs. In this definition, risk involves threat, vulnerability, and consequences that his the intersection between the three defined factors, see Figure 2.2.

$$Risk = P(A) \times P(S \mid A) \times C = Threat \times Vu\ln erability \times Consequene$$

[3] RAND Corporation is a non-Profit organisation in US.

Figure 2.2: Security risk diagram

2.2.3.1 Threat

The first step in this definition is to define the threat. In the safety risk assessment initiating event defines as hazard while, in security risk analysis, it is preferred to define the initiating event as a threat. The threat definition is the most challenging part of this approach, and Aven mentioned "what you have not identified, you cannot deal with"(Aven, 2008, p. 39).

Human life and infrastructures such as; roads, tunnels, dams, and industries can be the target for a terrorist attacks. For example, the foundations that are not so far from the urban areas are more likely to be the goal for terrorist organisations. Another example can be a dam nearby an entirely populated region that is an excellent target for the terrorist attack. The threat is meaningful when both intent and capability exist in a person or in an organisation to offend a particular target in a given period. An attack involves weapons, transportation and delivery, target, and so on, and each target may have unique characteristics. Hence, analysts should consider all aspects of the possible targets in the risk assessment and decision-making. Here, the threat is measured as the probability of attacking a particular target in a defined way during the distinctive period.

Threat=P (occurring attack)

The terrorist attack on September 11th involved both intent and capability. Indeed, the Intent came from the radicalism behaviour toward life, and the capability was about the international branches with various experts in the scientific areas.

2.2.3.2 Vulnerability

The second parameter of this formulation is a vulnerability. In fact, not all existing targets are deemed to be equally vulnerable. A bridge in the long distance to the city is more vulnerable than the city's airport because of the security concentration surrounding the airport. The University in Kenia, which was the goal of a terrorist attack in April 2015, is more vulnerable than The White House in the US. Therefore the infrastructure or the sensitive destination should be accurately defined to have complete information about it. According to Haimes(2004) mentioned by Willis and Rand Corporation (2005) vulnerability is the inherent state of any system or infrastructure when an attack occurs by an enemy. Thus, vulnerability is defined as the probability of any possible damage to human being or assets for a particular attack in a defined way during the distinctive period.

The vulnerability is meaningful if and only if the attack yields to damage, nothing otherwise. For example, a glass showcase is vulnerable to the rubble whereas the concrete wall is entirely safe if hitting with the rubble or similar materials. Furthermore, a concrete wall is inherently stronger than a glass showcase. Hence, the formula does not involve the magnitude of an attack. Thus, the damage to the target should be considered in the formula.

$$\text{Vulnerability} = P(\text{Attack yield to damage} \mid \text{occurring attack})$$

2.2.3.3 Consequences

The third parameter is all possible consequences of the particular attack. It shows the quantity and the type of the potential loss and structural damages. In general, damage remarks as fatalities, injuries, economic or political issues and so forth. Thus, the consequence is almost always uncertain. Hence, many authors introduce some methods to build a distribution instead of just highlighting the expected value. In this context, Haimes (2005) tried to turn our attention to tails of the assigned distribution. He believed that the extreme events might happen in the tails of the distributions. However, some other believe in the qualitative assessment for considering possible unforeseen. They suggested uncertainty-based risk assessment instead of Probability-based assessment, e.g. (Aven, 2014a). Here, according to Willis and RAND the consequence defines as the expected magnitude of any possible damage to people and assets if a successful attack occurs in a defined way during the particular period.

$$\text{Consequence} = E(\text{damage} \mid \text{successful attack which leads to damage})$$

2.3 Decision-Making Frameworks

2.3.1 Cautionary Principle

The cautionary principle is one of the basic principles of safety management. The principle stated that, when facing to uncertainty, the standard and guidance principle is to be caution. For example, the Norwegian regulation stipulates to use the fireproof panels to protect the living quarters on an offshore installation. Although the probability of fire for the living quarter and exposed areas of the facility might be judged as low the consequences are high, and it may happen time to time. Although the principle applies broadly in the safety regulation, it is, of course, possible to implement this principle in the public sector for treating security issues, ref (Aven and Vinnem, 2007). Thus, being caution means to apply the minimum safety for the industries or, in a broader sense, applying the minimum security for the society regarding people, the environment, and assets.

In case of an uncertain situation of work in industries, the cautionary principle should be adopted for managing the risk. Some experts suggested vital considerations when applying the cautionary principle for safety management that some of them is useful to apply in the security sector. The requirements for the safety section presents according to (Aven and Abrahamsen, 2007; Aven and Vinnem, 2007) in the following;

- The robust design aims to resist the system to any deviation from the standard condition. For the security assessment, there is no clear condition like in the mechanical product line. Here, the aim is to adopt the procedure to find the possible threats, e.g. monitoring suspicious activities.
- Flexible design means to operate a new situation in case of any hazards. For the terrorist attack assessment, analysts shall review the existing procedure of security investigation to overcome the possible adaptive terrorist plan.
- Applying safety barriers and improving the capabilities of barriers. It is applicable for the security reasons.
- Quality control of the whole system time to time.
- Applying the precautionary principle which means implementing measure to reduce risk or stop carrying out the activity.
- The cautionary principle suggests applying the ALARP principle for the system safety. The principle can adapt for both safety and security section, see §2.3.6 and §4.3.

Reminding Example 2.2, after the September 11th event the cautionary principle led governments to intensify the cautionary actions at the airports. These rules are the minimum measures to avoid the attacks with low probability and severe consequences. In some countries, authorities judged to use insensible armed police in the planes that are the minimum requirement, according to political justification, adapting this fact that the terrorist plan can frequently change. Although the regulation may be costly for the society, the authorities take more caution than applying cost-benefit analysis, see §2.3.3.

2.3.2 Expected Utility Theory

The expected utility theory is a framework for decision-making under uncertainty. This theory states that the best safety alternative is the one with the highest expected utility. The utility is the degree of usefulness and, therefore, the principle seeking the profitability and usefulness for the investment in the future. At the point of decision-making no one knows, exactly, what would be useful in the future even what would be the result of the existing decision? Hence, the expectation is the idea of decision-maker according to the outcome of the analysis and predicting the future. Thus, the goal is to maximise the utility of the project. Some scientists believe that starting from the rational condition the expected utility can be useful as the decision criteria, ref (Aven and Vinnem, 2007). However, there is no justification for this rationale in the framework.

The procedure consists of two parts. First, the utility defines for each calculated probability because the utility assignment has the same level of importance as the probability calculation. Second, the expected utility is capable of summation and so, the expectation is the sum of all utilities in the category. One method to assign the utility for different elements is to use the lottery approach, ref (Aven and Vinnem, 2007).In this method, the decision-maker assign the utility of one for the best scenario and the zero for the worst one. After that, they should assign the utility for all other outcomes in this interval. The decision-maker compares the best result with a chance of u=1 in one hand and, on the contrary, another outcome with the certain chance of u_i. Hence, the decision-maker assigns the utility for the outcomes when she/ he is indifferent between these two chances, u and u_i. The expected utility, thus, calculates as following:

$$E[Utility] = Eu(X) = \sum_{i=1}^{n} P_i \times u_i$$

Utility theory allows the decision-makers to reflect the like or dislike for a particular consequence by giving weight in comparison to the expected value. When decision-maker

dislike the negative outcome she/he gives more weight to the expected utility of the outcome than the expected value. From the viewpoint of the risk averse $Eu(x) < uE(x)$ while risk seeker gives more weight to the expected utility than the expected value $Eu(x) > uE(x)$. A neutral decision maker is indifferent between the utility, and the expectation, then she/he choose $Eu(x) = uE(x)$, ref (Abrahamsen and Aven, 2012). Aven and Vinnem (2007) according to the previous literature stated that the real situation are complicated, and every individual has an own preference for different outcomes. Further, the utility approach is not suitable for the group decision-making. Thus, it is not a fruitful method for group decision-making. Indeed, making a decision needs discussion and negotiation. Thus, mathematical optimization is not a complete tool for this reason. It is hard to assign the utility function for all outcomes and, in fact, there is no rational condition but individual preference in this model. For short, it might be suitable for starting the process but it is not the exact answer to make a decision.

2.3.3 Cost-Benefit Analysis (CBA)

This tool developed for evaluating the public policy issues by measuring the benefit and the cost of the project, comparing them with the value. The expected monetary value calculates through this formula $i - E[C(x)]$ in which i is the advantage of the investment for a particular alternative and $C(x)$ is the cost of x fatalities. Here, the decision-maker shall specify the value of the statistical life. When applying the model to a more complex situation of industries, analysts face to various elements and issues. For example, the framework considers the time value of money and the rate of return which is the proportion of the original investment. The value of all elements, both market and non-market goods, transfer into monetary.

The framework is to use the common scale value that should be a country's currency. Aven and Vinnem (2007) stressed that transferring goods into the monetary is an easy task because it depends on the society's tendency to pay for a particular product. However, transferring the non-market goods like human life and the environmental issues are more difficult.

Note that the method developed for the public policy issues and, therefore, it works with the cost of fatalities. Two approaches has suggested for determining the value of statistical life (VSL). The revealed approach aims to derive all values from actual choices. However, the questionnaire approach tends to investigate individual tendency toward risk. In this approach, decision-makers willing to pay under the different hypothetical situation, ref (Aven and Vinnem, 2007).

Additionally, in the private section, the stakeholders make an investment in the project during its lifetime. Thus, the value of time and discounting rate of the value is also considered. The goal is to compute the $E[NPV]$. In this formula, the time value of the invested money in its period involves the calculation by using the appropriate rate of return.

$$E[NPV] = \sum_{t=0}^{T} \frac{X_t}{(1+r_t)^t}$$

In the formula r_t is the expected rate of return at year t, considering the time value of the investment. The rate of return discount the cash flow X_t at year t. Since the cash flow in the future is uncertain, analysts should calculate the expectation of the cash flow $E(X_t)$ taking into account the uncertainty about future, i.e. (Aven and Flage, 2009).The method helps to improve $E[NPV]$ and ICAF(Implied Cost of Averting a Statistical Fatality) by involving risk and uncertainty in the formula.

$$E[NPV] = \sum_{t=0}^{T} \frac{E(X_t)}{(1+r_t)^t}$$

Note that, in this model the idea is to use the correct value for all attributes. Considering the cost of life may vary, depends on the different situation. Thus, another alternative is to present the result as the function of used assumption. It is the pragmatic view of the cost-benefit approach. This view allows to exclude some attributes that are difficult to transfer to value. Both traditional cost-benefit analysis and the pragmatic view provide decision support, and they are not a concrete recommendation, ref (Abrahamsen et al., 2011; Aven and Vinnem, 2007).

2.3.4 Cost-Effectiveness Analysis

Cost-effectiveness method is a framework aims to compare safety measures to support decision-making. The index of effectiveness uses instead of net value for each measure and the indices compare to each other to choose the most effective measure. The model take into account the decision maker's consideration regarding outcomes. A cost-effective measure has a characteristic as following, ref (Abrahamsen et al., 2011).

- The measure is effective but with less cost.
- The costly measure should be more beneficial to worth the added cost.
- The less efficient measure shall have less cost.
- The measure is cost saving with better or at least equal outcome to the safety or security.

The framework objective is to define the ratio of cost-effectiveness for each measure and compares all alternatives such that at least one of those criteria mentioned above exist. It is the ratio between the investment cost associated with safety measure and the total effect related to loss of lives if measure implemented. At the end, the ratio for the measure compares with the reference value. This method presents here according to (Abrahamsen et al., 2011).

- C_i denotes the investment cost associated with safety measure.
- Z_i denotes the total effect. This parameter relates to loss of lives if implementing the measure i.
- R denotes the reference value. This reference shows the tendency of the decision-maker to pay to gain one unit of effectiveness.

The effectiveness ratio defines as C_i/Z_i for each measure and when they compare to each other if $C_1/Z_1 < C_2/Z_2$, then the measure number 1 is more efficient. The decision maker's consideration involves in R and, therefore, the ratio compares to the reference value. The measure 1 is effective as long as the ratio is less than the reference value $C_1/Z_1 < R$. The weakness of the method is the uncertainty involving the calculation of the parameters.

2.3.5 Multi-Attribute Analysis

It is a decision support tool that analyse the consequences of various measures for the different attributes. This procedure does not transfer all attributes into a comparable unit and instead uses different ratios for different attributes. In the analysis, some elements may define by quantities while political issues and social considerations define qualitatively, ref (Abrahamsen et al., 2011; Aven and Vinnem, 2007).

2.3.6 ALARP Principle

The ALARP is one of the fundamental principles of risk assessment. The principle stated that the risk should be reduced to a level that is as low as reasonably practicable. The principle applied to different interpretation such as; “So Far as Is Reasonably Practicable” and” As Low as Reasonably Achievable”. However, The English court of appeal judged the principle as reasonably practicable in 1949. The court also stated owner handles the calculation regarding the risk. The owner place the risk on one scale while the involved sacrifice put on the other scale regardless of the cost of applying the measure, ref (Jones-Lee and Aven, 2011).

Reducing risk in practice imposes a cost on the society and, therefore, the principle applies in connection with the CBA (Cost Benefit Analysis). In line with CBA, ALARP principle stated that risk reducing measure should be taken to the level that cost of doing so is not "grossly disproportionate" or "disproportionate" to the benefit of the measure. The two definitions are slightly different, ref the discussion by Jones-Lee and Aven (2011). The difficulty of implementing measure is to compare cost and benefit and, here, CBA is a framework to examine the cost with the gained benefit. In the more practiced cases, the analysts refer to the existing procedure of safety practice but when facing the new situation, the effectiveness of the measure should be judged according to the associated cost. However, the benefit of applying the measure is not straightforward to compute.

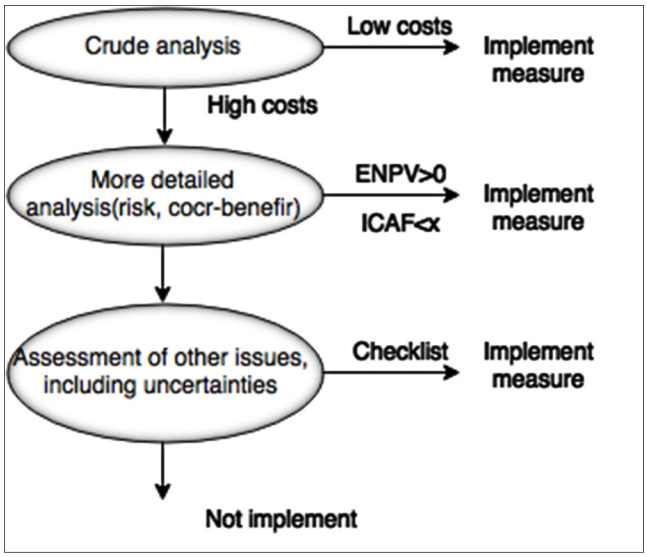

Figure 2.3: Procedure for implementing ALARP, ref (Aven and Vinnem, 2007)

Figure 2.3 illustrates the procedure of doing ALARP. The procedure requires that cost shall not be gross disproportionate to the benefit, means that cost should be lower than benefit. For this reason, the benefit shall be transferred to the monetary value that is, of course, problematic. Thus, the first step is to perform a qualitative analysis of the benefit and the risk reducing measure. If the cost is judged to be low then gross disproportion is not the case and if high the alternative approach is to calculate cost-effectiveness indices (§2.3.4) and $E[NPV]$. The framework suggests to imply the measure if $E[NPV]$ is positive or ICAF is smaller than a small number (some few millions), means that it is not gross disproportion. If none of those two conditions fulfilled, analysts assess the uncertainty and all other factors that have not considered

in previous steps. The checklist includes following points and if most of these points are met the gross disproportion is not appropriate, ref (Guikema and Aven, 2010):

- The uncertainty involving in the process and the effect of the applied measure of reducing uncertainty.
- The list involves the relation between the measure and manageability.
- The effect of applying measure on the robustness.
- The measure should involve the best available technology(BAT). It is to ensure that the used technology is up to date and not using the old systems.
- The unsolved problem(s) and possible conflicts between personal- safety and work environment area is defined.

The ALARP principle may interpret in line with the Tolerability of Risk (TOR). TOR has three levels that are “broadly acceptable”, “tolerable” and “unacceptable”. The tolerable area between two bonds shows the risk that can drop as low as reasonably practicable. In the safety risk assessment, it might be meaningful to compare ALARP with the cost-benefit analysis. However, when facing to the security assessment, the consequences may be enormous such that consideration of the cost of risk-reducing measures may not easy to calculate. In case of security assessment and related consequences, the cost of doing the security measure is more straightforward than confronting the risk, e.g. (Jones-Lee and Aven, 2011).

3 Security Risk Assessment Concerning the Norwegian Standard

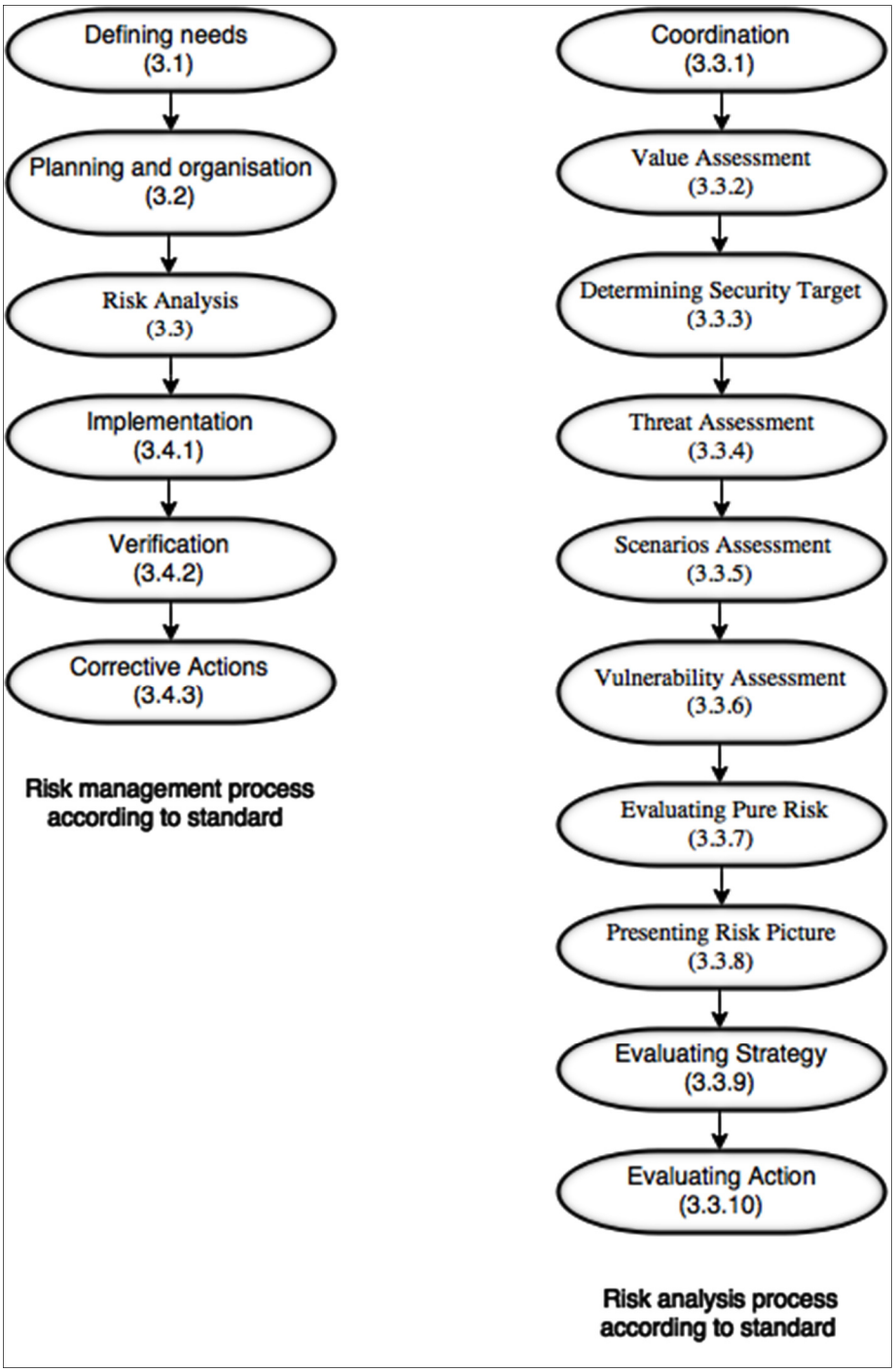

Figure 3.1: Security Risk Management(*NS 5832*, 2014)

The standard contains the requirement for doing the assessment in the particular area. Hence, Standard shall contains clear definitions and straightforward procedure. In the social section, the outcome of an undesirable event might be enormous involving vagueness and

lack of proper knowledge. Therefore, the definition of risk and the considered elements in the risk picture should highlight surprises (§2.1.2.2) and used data (§2.1.2.3).

In this section, we outline and assess the plausibility of the Norwegian standards for civil protection against intentionally undesirable actions. For this purpose, we can review the standards number NS 5831 for risk management and standard number NS 5832 for risk analysis. The used terminology in these two Standards presents in NS 5830 which does not mention here. The weakness points of the process discuss in §4.2. Here the steps are illustrated in Figure 3.1according to *NS 5832* (2014).

Risk management is a process to make suitable decisions based on identified risks. The objective is to achieve an acceptable degree of risk. All steps have a connection to the decision-maker. The process results in establishing a report to decision-makers and stakeholders. The final document consists of risk picture concerning the defined security assessment with all assumptions and evaluation procedures. Hence, analysts can review the case in the future and re-evaluate the analysis to make a new decision or adding extra measures.

The first step of the process is to define different elements of risk management. Norwegian Standard (*NS 5831,* 2014)considers various steps of doing the assessment for the purpose of security risk management.

3.1 Defining Needs

The first thing before managing risk is to define the need(s). It means to describe either existing or the predicted future problem(s). It is the judgement of experts that predict the future's need, according to their experience. In line with this Standard, the risk has two parallel aspects; evaluating potential gain and possible loss. The Standard mentioned that when assessing actions and accepting risk, positive points are also appropriate to evaluate. The Standard mentions some examples of the potential gain such as increasing profit and marked share. On the other hand, the potential loss is damage to values, lack of fair access, and loss of reputation(*NS 5831*, 2014).

The Standard considered four strategies to manage pure risk. The first strategy is to stay away from any process or action that causes relevant risk. The second strategy is to transfer risk to others. The third strategy is to accept the risk. The last one is about implementing measures to reduce or eliminate the risk. Standard put attention on the positive points in the risk management which has a link to risk. The five elements of the risk management present in the following according to the Standards (Figure 3.1).

3.2 Planning

It is a part of the management system for all facilities. The risk management may involve different analysis for various purposes at different levels. The aim of this step is to make a clear plan and to document all necessary activities in the particular area of investigation. Additionally, all responsibilities identify for involving parties. The Standard also stated that the complexity of the analysis, available time and information, and consideration managerial influence the scope of the analysis. Furthermore, the analysis should involve unintentional actions that may lead to the disaster. Shortly, in this step the goal of the risk analysis defines clearly to use in the next steps.

3.3 Risk Analysis

Here the security risk analysis defines as risk assessment and evaluation of strategies and measures. The Standard defined the scope of risk management on the type of existing and future challenges. The risk analysis affects the risk-reducing actions and strategies, ref *NS 5832* (2014). The analysis discusses different solutions with different costs for the considered problem that shall result in defining the risk picture at the end of the assessment.

The analysis identifies the problems, break down all factors and assess all strategies and necessary measures. This structure includes reducing measures and gives them priorities to deal with the identified risk. This part is somehow conducts with the planning phase. It means the structure of the analysis constructs in the planning stage. Furthermore, Standard stressed that analysts should evaluate and complete the previous steps of the process. In each phase, new knowledge may be revealed such that it is necessary to reassess the previous phases. Moreover, Standard stipulated the documentation and connection between process and decision-maker in all steps. In fact, it is appropriate to turn the attention back to the previous phases and reassess the past steps to reveal the missed points and possibly misleading paths.

In line with the Standard, the implementation of the analysis should connect to decision-makers. The stakeholders and policy makers put their attention on the process and define the vital points for problem definition, analysis, and judgement. It is similar to decision-making model under uncertainty by (Aven, 2008) which all phases has a connection to decision-makers and stakeholders (Figure 3.2). Furthermore, according to the Standard the analyst team shall document all steps of the process. The process may include resources,

methods, and evaluations. The documentation let the analysts review and continue the process in the future.

There exist a section so-called "critical thinking" in the standard. The critical thinking emphasised that analysts should apply a systematic and standard way to collect and evaluate the different type of data. Using standard ways of data collection allows to ensure the validity[4]and the reliability[5]of existing data. Indeed, the advice motivates us to refresh our understanding of the risk picture and the new framework for the assessment.

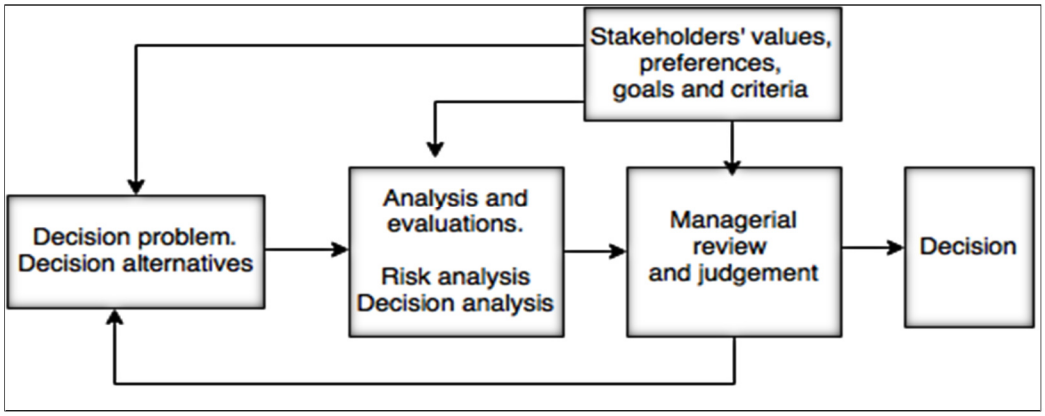

Figure 3.2: Decision-making under uncertainty by (Aven, 2008, p. 10)

3.3.1 Coordinating

This step more focuses on the scope clarification and resource allocation. The risk analyst group shall document the further resource requirements if there is a particular need for more economic resources. In fact, the Standard focuses on paperwork and restates that analysts shall document all assumptions, sources of information and participation. However, it is not the scope of this thesis. In line with the numerical value and assumptions, it is necessary to clarify the dependency between them. The process shall inform decision-maker that to how extent the numerical values depend on the assumptions and hence, how changing the assumption will affect the predictions. Aven (2008) suggested the sensitivity analysis for this reason.

[4] Validity means being relevant in connection to the highlighted problem, ref (*NS 5832*, 2014).

[5] Reliability means data comes from credible sources, ref (*NS 5832*, 2014).

3.3.2 Value Assessment

The assessment of risk consists of several steps that result in risk picture at the end. The process starts with value assessment. According to the Standard it is the entity that handles identification, evaluation and ranking the assets and resources. Moreover, the expected future asset may be reviewed and evaluated in the assessment. Identifying the values (such as people and assets) is the basis for further investigation and put a priority on all risky sources. Standard takes many dimensions into consideration such as; environment, the economy, reputation and freedom of speech and suppose that the analyst team apply the qualitative assessment of the process. Indeed, value assessment consists of different perspectives like individuals, organisations, national and international aspects.

3.3.3 Determining the Security Target

After value determination, managers and stakeholders determine the goals. This step has a link to decision-makers in which they determine the acceptable condition before and after any possible undesirable events. They shall describe the main points before and after an undesirable event.

3.3.4 Assessing Threat

The third step is threat assessment. This step identifies all possible actors using public information, data from the security police, and agencies. Moreover, the expert judgement can be a reliable source of finding and identifying any possible threats. Further, the threat may be from different categories such as groups or individuals. The Standard considers two main purposes for the threat assessment in the context of security. The first goal is to identify the actors. By this point, all possible actors Including individuals or groups of attackers identify by the analysis team. In this context, expert opinion is the best source of this investigation. The second purpose is early notification of any possible threats so that emergency preparedness may implement to withstand a potential attack. When undesirable events happen, the system should be ready to deal with the situation with minimum loss in values.

3.3.5 Evaluation and Choosing Scenarios

Based on defined values and threat assessment, scenarios are prepared. The scenarios are the source for further evaluation, and they describe how threats affect the targets. Standard mentioned the negative effects on the target because according to that the impact of the positive

point should also evaluate in the sense that they may help to improve the situations. Furthermore, the number of considered scenarios should be sufficient. The scenarios help the managers and analysts to have a clear understanding of the situation and also the discerption should not be complex.

In this phase, bow-tie diagram is the easiest and the most approachable way to illustrate the scenarios. For each scenario, a bow-tie diagram (Figure 2.1) illustrates the undesirable events and all preventive and mitigation barriers on the left and right side of the diagram. On the left side of the diagram, FTA analysis starts with the threats and end up with the undesirable event. In front of the bow-tie diagram, the vulnerability defines the targets and barriers.

3.3.6 Assessing Vulnerabilities

According to defined scenarios and what is unfolding in value assessment and threat assessment the entity evaluate the vulnerability of the targets. Evaluation of barriers and assessing the resistant of the system is the scope of vulnerability assessment. Analysts shall assess to what extent the existing barriers defend against an undesirable attack. Everything depends on the scenarios and all factors within the area of technology, organization and human resources should be involved in the process.

3.3.7 Evaluating Pure Risk

For each scenario, risk assessment describes the value, threat, and vulnerability which conclude with a level of risk for each scenario. The collected information of three parameters uses to describe the pure risk for each scenario. The Standard defines the pure risk as the potential for loss and not for profit.

For each evaluation, uncertainty shall be described. The Standard gives due attention to the assessment of uncertainty in the scenarios. Acceptance of this advice would be more practical even if the uncertainty involves in the risk picture. This issue will further discuss in (§4.2).

3.3.8 Presenting the Risk Picture

In this approach, threat, vulnerability, and values visualise the risk. These factors presented in §2.2.3, and the aim of risk picture is to explain all possible events and consequences. The risk picture illustrates an overview of risk to the decision-maker and the purpose of this is to provide the best possible basis for further security risk management.

Additionally, Standard emphasised that a comprehensive approach to risk should also highlight the potential gain.

3.3.9 Evaluating Strategy

In this step, decision-maker defines the integrated framework to deal with risk. According to the strategy that is chosen to handle the risk the assessment shall include a description of the different options and consequences. Note that Standard uses four different strategies for handling pure risk. These strategies are to avoid risk, to transfer risk, accept the risk or reduce risks. Based on relevant framework one or more strategies shall define to manage the risk. Here different entities may choose different strategies that construct the overall approach. Strategies are different in different sections, and the overall approach should take all targets into consideration. Hence, decision-maker may choose the combination of strategies, and finally they make a decision on the basis of these considerations.

Removing or reducing the risk on one hand and accepting the risk, on the contrary, depends on the existing situation. Hence, decision-maker considers all relevant factors as the potential for the gain in the final decision.

3.3.10 Evaluating Action

The analysis may address various possibilities and consequences. The decision-maker shall choose individual measure or group of measures to withstand the severe outcomes of different threats. Choosing measure is in relation to strategies to manage risk and technological, organisational, and human resources are relevant to select the proper measure(s). Of course, the cost of doing the measures and the effect of measures shall be considered.

The decision-maker shall define what is acceptable? Standard suggests accepting the risk in case the condition, benefits gain, or cost of implementing measure(s) dictate. The decision-maker shall determine the choice of measure.

3.4 Risk Treatment

The risk analysis shall end up with the risk picture. By now, we have the proper elements to deal with the possible future situations. After choosing involved factors in the risk picture and also choosing the appropriate strategy to address the risk it is time to apply necessary actions. The assessment deals with the possibilities and consequences of choosing or declining of these measures. It mentioned before, measures to prevent or reduce the risk depends on the

technology, organisation, and human values. Standard underlined the cost-effective analysis and assessing the effect of the measures about security goals.

Standard gives the order to reassess the security goals after choosing strategies and actions and also assessing associated consequences. It means a decision-maker shall decide on the acceptable security risk. With this view, the conditions, frameworks, expected gains, and cost might dictate to accept the high-security risk.

3.4.1 Implementation

As we have seen, after the analysis phase has been done process goes to the management part. This step is to implement the objective of the measure. It means how and when the measure should be taken in the sense that reduces or eliminate the risk. In the previous phase, the strategy and measure decided and in this step analysts set the timetable for necessary action(s). The analysts make the instruction for all actions comprises of technical and organizational measures or human resources.

The aim of this step is to coordinate the relation between measures and all other factors and hence, it is necessary to have the plan to implement all measures. Later, in the verification phase the timetable, measures and other factors are used.

3.4.2 Verification of the Process

Another important step of the process is the verification phase. The analysis shall evaluate whether the implementation of the measure(s) helps to achieve the goals. Here, analysts define the subjected area for verification. Also, the verification step should assess the conditions and make sure they remain constant during the analysis. In this step, analysts plan measurements, targets, and. The Standard mentioned that the verification implement in an acceptable way. Therefore, analysts should implement some accepted way according to the scientific literature, i.e., (Dedianous and Fievez, 2006).

3.4.3 Corrective Actions

After verification step if some circumstances failure to meet the defined requirements, measures should be implemented. If verification reveals any deviation from demand, then corrective action choose to apply. If decision-maker recognize the deviation as small and acceptable then, other strategies might be selected like staying away from risk or transferring it to other parts. If decision-makers decide to apply any corrective measure, the application should be planned such that the goal, the detail work and the deadline to finish the process is defined.

4 Discussion

4.1 Is Willis Approach Fruitful, Concerning Uncertainty?

The advantages of the formula presented in detail by (Willis and Rand Corporation, 2005). The authors mentioned three advantages for this method. First, it is beneficial for comparing risk across the different targets. Second, the method gives the explicit mapping between risk and management strategies and finally, the method helps to improve preparedness against risk and decrease the effects of damage. The only mentioned challenge through the approach is to find and to understand the source of uncertainties.

Willis and Rand recognized two sources of uncertainties in the context of terrorist risk. The former one is errors in the parameter estimation, and the later one is about evaluating different consequences(Willis and Rand Corporation, 2005). In this method, all three parameters represented by numbers. Moreover, different consequences compare together using numbers. The sources for uncertain numbers mentioned as:

1. Terrorist goals, motivation, and capabilities are uncertain sources for threats
2. Damage assessment as the uncertain source for consequences

It seems the formula is good prepared and considers enough factors, but there exist another sound in terms of the risk assessment concept that does not believe so much in such probability numbers. The definition of three factors may be useful and complicated enough, and it applies widely in practice, but still the formula cannot reveal the uncertainty about the causes and consequences of the phenomena. Despite the positive point that mentioned by Willis, Aven (2008)criticised this definition on two important points. First, the expected value misleads the surprise events with low probability and huge consequences. Second, Willis considered the true probability for the analysis that is not meaningful. The likelihood of the security risk depends on assumptions and suppositions and, therefore, it is a subjective probability. Shortly, there is no true probability for the undesirable event in the security section. The third weakness point of this approach is the uncertainty assessment. Even though Willis mentioned the uncertainty involving in calculating three elements, this view does not reflect the uncertainty as one of the main element of the risk picture.

Calculating $P(A)$means quantification of all existing information. To perform this, intent and motivation of the attackers and their abilities to movement and adapt to the defenders plan present as a probability number(Ezell et al., 2010). All three parameters of terrorist risk are

conditional on the existing knowledge $P(A \mid k)$. With another word, all probabilities are subjective based on the information and expert judgment. Thus, the assigned probability is reliable for the present situation. Thus, changing the defensive program or further intelligence from various sources make changes in the likelihood of the threat, and it is, therefore, necessary to assess again (Ezell et al., 2010). In case of enormous consequences like in the terrorist attack, it does not matter the probability of occurrence is x or y (Aven, 2008).

The significant challenge to defeat the terrorist attack is that the terrorism is an enemy armed with information and has the capacity of analysing all possibilities and limitation (Ezell et al., 2010). The terrorist can adapt the considered plan with all applied barriers and deterrent programs. Hence, to establish the preventive program in a long-term and protective plans to defeat and thwart the attacks we need to use all possible models. Ezell et al.(2010) mentioned that applying a single method is not reasonable to deal with this kind of challenges.

The second weakness point of the Willis approach to security risk assessment is to use he expected value. The expected value is the average result of doing the experiment in the long run. In §2.2.3 consequences of a terrorist attack formulated as the expected value of the damage. According to Aven (2010), Daniel Bernoulli(1738) challenged this idea for the first time. He stressed that the utility of any item is more important than the price of that. Aven mentioned that the consequences of the terrorist attack could be extremely high in both national and international levels. Hence, the expected value cannot predict such an unforeseen. Also uncertainty according to such an extreme consequences is high, and the existing knowledge does not help us to predict what would be the next disaster and its associated consequences. In the security risk assessment, expert judgement has more weight than the background knowledge.

Aven (2010)based on “Russian roulette game” and the following laws stressed that the expected value may be the successful prediction, if (1) several independent experiments within the similar range of value exist, (2) under the law of large number, (3) applying the central limit theorem. Here, the existing background knowledge about the projects plays the significant role

Willis and Rand Corporation (2005) made an assessment of resource allocation based on the potential of a terrorist attack in different regions in the US. They used the expected values for the terrorist risk that is similar to an investment in various independent projects within a similar range of value. Conversely, to assess the potential for individuals it is not reasonable to use the expected values.

Shortly, for the repeated experiments like gambling and availability of a system the expected value can lead to a good result. Conversely, the decision regarding any possible counterterrorism effort cannot be made according to the expected value or any distribution of attack because of the extreme national and international consequences (Aven, 2010).

4.2 To How Extent Considered Norwegian Standard Is Fruitful?

Standard defines pure risk as potential for loss and not for profit, see §3.3.7. The pure risk defines in the literature as an insurable risk that has a known probability of loss, ref (Moles and Terry, 1996). Additionally, the Standard defines risk as not the potential for profit that does not make sense when assessing the security risk. The authors mentioned above defines the known probability of loss which, tacitly, means to apply either classical or the frequentist probability, see §2.1.1.

The classical interpretation of probability cannot apply for scientific reasons because, in the real life, the outcomes for the events are not equally likely to occur, and some of them promote by others. Hence, the application of this interpretation is limited to stochastic experiments such as gambling and sampling. On the other hand, Frequentist probability does not refer to outcomes that are equally likely to occur, but it reflects the repeating experiments in a long run. For practical reasons, repeating the experiments is impossible, for example, we hope that September 11^{th} not to occur again. The disasters are unique with many barriers each of which has a different probability of failure and thus, it is not possible to repeat the disasters. Practical situations cannot be repeated for many times then to understand the probability of occurrence for a complex system it is necessary to adapt a subjective probability that refers to the background knowledge. Subjective probability implements when considering the background knowledge and uncertainty. In fact, in objective probability events are uncertain while subjective probability considers the uncertainty both in future events and applied background knowledge. For risk assessment purposes, it is more meaningful to use the Lindley's interpretation of subjective probability which refers to Urn standard, ref (Aven et al., 2014).

Aven (2012) collected all risk definitions in nine categories which the first one involves the potential for loss. This definition has a connection to probability and expected value. The probability is the measure of uncertainty but not as exactly as it is and, therefore, the only way is to apply the subjective probability as mentioned before. The expected value is the centre of gravity of the assigned distribution that involves many assumptions and limitation. Hence, the risk should not be limited to expected values and probabilistic modelling.

It seems unconventional approach to security risk when standard pays its attention to positive points such as increasing profit and marked share. In the area of security risk assessment how analysts can convince the decision-maker to have such a fortune? How the threats or, in general, an attack can affect the economy in the positive way? Although the Standards have the integrated view on the defined problems counting the fortunes is not a suitable framework for the security risk assessment. Indeed, analysts should take the negative points into consideration such as loss of life and damage to the infrastructures and so on.

Standard stressed that analysis should use the new way of thinking so-called "critical thinking" and it is about the new way of data collection. The Standard do not close the process with introducing a particular model for analysing the data. Hence, It will be beneficial if analysts apply the knowledge assessment and surprise assessment alongside the probability analysis Aven (2013a). Another good point to pay attention in this regard is Deference to expertise that is about answering all questions in the new situations with relevant experts. This pillar is about getting help from experts in risk management team(Aven and Krohn, 2014).

Standard defines risk as a threat, vulnerability, and values. On the other hand, Willis and other researchers define risk as a threat, vulnerability, and consequences. As mentioned before, defining these elements is not an easy task, and it is not meaningful to represent these factors as a single number. Willis believes in uncertainty in assigning the numbers, but he did not use any systematic approach for treating the uncertainty.

Fortunately, the Norwegian standard does not mention to allocate the factors with the probability numbers. The Standard suggested the qualitative assessment. It means to assess the risk both in qualitative and quantitative ways. Although the procedure put more emphasis on the connection between decision-maker and analyst group determining the appropriate values for the risk assessment is a difficult step.

Having considered values, it is also necessary to look at the associated consequences for each scenario. On the other hand, consequences are the possible failure for the defined values. Hence, it is conventional to replace the values in the risk picture with the consequences. This view gives more details about the failures and losses.

Besides, the Standard considers factors in a qualitative way, and Willis picture assigns a probability number for the risk. Accordingly, we can combine the two approach with a slight change in the definition. Thus, risk defines as a threat, vulnerability, consequences, and the probability of occurrence. Here, the remaining issue is the uncertainty associated with the background knowledge and future undesirable events.

Some experts believe the probability-based risk assessment (PRA) has poor risk picture and unable to predict surprises, e.g. (Aven et al., 2014; Bedford and Cooke, 2001). Probabilistic risk analysis involves uncertainty and model(s) cannot reveal all aspects of the risk. An equally significant aspect of the assessment is to rate the background knowledge. Thus, alongside the probabilistic assessment it is crucial to rate the background knowledge(Aven, 2013b) and to make the top-ten list of all undesirable events(Abrahamsen et al., 2010).

In uncertainty-based risk, assessment alongside with the PRA risk picture involves uncertainty and assessing background knowledge. Hence, safety risk defines as;
(A, C, C*, U, P, K). In the description, C is the associated consequences and C* is a prediction of the real possible outcomes. U is uncertainty about the initial event and consequences. P is the probability of occurrence and K is the background knowledge, ref (Abrahamsen et al., 2010). Hence, it is possible to apply a similar description for the security risk assessment.

The probability is the measure of uncertainty, and the uncertainty assessment involves the background evaluation. Therefore, the security risk assessment may describe as a threat, vulnerability, consequences, and uncertainty. In more simple form-like what mentioned by Abrahamsen et al.(2010)for safety risk analysis- the consequences comes from threat and depends on the vulnerability of the target. Hence, the risk has two main sides, consequences and uncertainty.

One of the considered strategies to treat the risk is to transfer it to other. It has not a clear definition about how to apply this strategy in practice. Transferring the risk has no connection to scientific literature about treating or reducing the risk. This part need to review and consider the better choices of strategies.

4.3 Discussion on the Integrated Framework for Decision-Making

The risk analysis may end up with causes, consequences and different tools to evaluate the risk. Alongside, analyst team evaluate the security measures in case the result of the analysis shows the severe consequences, see§2.3 and §3.3.10. The result is meaningful when comparing to the criteria and thus, the first point is the responsible party to define the criteria. The criteria define by either authority or private sections.

- **Who is responsible for defining the criteria?**

For the security assessment, the Standard (§3.4.2) emphasise that the decision-maker should define and verify the criteria for the evaluation. In the Security section, analyst team has the close connection with the authority.

In Norwegian petroleum sector, the licensees have the full responsibility for establishing and doing all activities, according to the rules. The authority has, thus, the supervisory role to ensure that working environment and safety criteria meet the regulation. It means the operator defines the acceptable level of safety in the petroleum sector in Norway. This regulation challenged by Abrahamsen and Aven (2012). The discussion provided using the expected utility theory, see §2.3.2. Assume, the operator defines the criteria and thus, invests money to reduce the risk of loss. The money invested in the self-protected area decrease the possessions of the operator and if the accident happens the extra money losses. The optimal situation is the point where the utility benefit equals the utility of decreasing the wealth. The utility benefit refers to as declining the probability of loss and increasing fortune for reducing losses.

The analysis by these authors shows that if the level defines the likelihood of being in a bad state, the operator should invest more money to satisfy the optimal investment point. The investment should be higher when protecting the society because the activity has an external effect on the society and it costs more money. When modelling this extra money, the investment should be even more, and it is not the preferred choice for the operators. The operator can define the higher utility level to spend less money on the self-protection. Accordingly, the authority should define the risk criteria as a part of the risk management program, ref (Abrahamsen and Aven, 2012).

- **Decision-making with outcomes of different types**

The second point in decision-making raises when there exist different alternatives and different tools to evaluate them in case of risk-reducing measures. The investment has no direct relation to the level of safety. It means, for example, investing double money does not make the project safe or secure as twice. Hence, it is the responsibility of the decision-maker to choose the best alternative that balance the level of safety with the investment. The acceptable level of risk and the amount of money to invest in the project are not mutually exclusive items. These two problems, of course, has one answer because both has a link to the value. Hence, the standard procedure is necessary to use these tools in the black box.

What are the characteristics of an excellent framework for decision-making? They are many regulations by authorities in the whole world. The issue is to find if a regulation is effective or not? Five principles are defined to examine the frameworks about their efficiency. Accordingly, the regulation is right when meets five principles. The principles also work when considering frameworks for decision-making. It is to ensure that the best framework for comparing outcomes is chosen according to the known and accepted principle of sound decision-making. Thus, the Better Regulation Task Force (BRTF) defined the five principles of good regulation as proportionality; accountability; consistency; transparency; and necessity, ref (Boyfield, 2006). These five principles present shortly in the following:

- **Proportionality**: Just in case of necessary situation authority shall defines the regulation, and the solution should be appropriate to the risk, cost should be reduced. This principle is to make sure the regulations are suited to deal with the situation.
- **Accountability**: Regulators shall be published in public, and they should have clear criteria for the judgement. They are accessible, fair and have an appeal process.
- **Consistency:** The rules should be linked together and be compatible with each other. They should take other rules into account. Regulation should be predictable.
  The consistent framework means to adopt a similar approach for similar situations.
- **Transparency:** The regulation should be open, simple and communicate to all involved parties.
- **Targeting:** The regulations should be focused on the considered issue and minimise the side effect.

Thus, a sound framework for decision-making should involve these five principles. The transparency and consistency are more important in the case of evaluating the decision-making procedure. Abrahamsen et al. (2011) examined some frameworks of decision making such as cost-benefit analysis and multi-attribute analysis. These authors concluded that a framework is neither transparent nor consistent if all attributes of different types do not transform to the one comparable unit that might be country's monetary value. The paper presents in the following, shortly, ref (Abrahamsen et al., 2011).

The procedure is applying the framework to compare all alternatives of different types to choose the suitable one for decision-making. In a cost-benefit analysis (§2.3.3), all outcomes transform to money, for example, the value of the statistical life or the damage to the environment. The weakness points of CBA mentioned before, in particular, transforming outcomes to money might be controversial. Thus, pragmatic view on CBA applies which does

not necessarily transform all attributes into money but a comparable unit. This assessment can be reviewed and judged again by others at any time. The decision is open to assess again and has rational links to the elements. The pragmatic approach to cost-benefit analysis is consistent and transparent when comparing outcomes of different types.

However, in multi-attribute analysis outcomes of different types do not transform to one value and decision-maker subjectively weights the money and safety. This analysis is not open to assess again because evaluating procedure is different from one person to another. Besides, there is no link to other elements in this framework and due to disutility between elements some situation promotes to some other situation.

Finally, Abrahamsen et al. (2011) assessed the cost-effectiveness analysis. In this procedure, the expected cost for non-commercial outcomes calculates by multiplication of decision-makers valuation of the outcome to the amount of that material. For example, the decision-makers valuation of hydrocarbon released to the see in tonnes multiplies by the released amount of hydrocarbon in a ton. In this procedure, the decision makers valuation is the subjective procedure and in situations with the various non-commercial materials the decision is neither consistent nor transparent. The analysis is sensitive to the valuation of different attributes.

- **Cautionary Principle and ALARP**

Standard (§3.3.10) suggests to apply measure in connection to profit and cost and, therefore, the cost-benefit analysis, or other economic analysis may apply. There is a discussion about applying ALARP and take the cautionary principle into consideration. Aven and Abrahamsen (2007) made a calculation and compared CBA and cautionary principle on the safety basis. The procedure is to assign a value of statistical life and apply the cost-benefit analysis for both situations of implementing and not implementing the reducing measure. The key point of the analysis is to assign the value of statistical life and to calculate the frequency of the failure. The cost-benefit analysis does not have the clear message for decision-making because the mathematical model may show the gross disproportionate due to some assumption and limitation. However, with small changes in the basic assumptions the result might be entirely different and accept to implement the measure.

In case of a threat in the public sector, the assumptions are rather sensitive to change and, therefore, the result of CBA shall take the sensitivity and uncertainty into account. Aven and Abrahamsen (2007) stressed that portfolio theory and corporate risk point of view proved the reasonability of using VSL but being caution means to use greater values for the statistical

life. Additionally, using discount rate and using certainty equivalent for cash flow does not consider uncertainty as it should be and hence, the analysis shall consider uncertainty outside of the CBA framework.

The nature of the security is different from the safety, ref §2.2.2. Thus, applying ALARP in security assessment needs take into account the adaptive nature of attack, quantitative conditional cost-benefit analysis and any possible limitation for personal liberties. The ALARP procedure (ref §2.3.6) is, therefore, shall be revised to meet these three key points as following, ref (Guikema and Aven, 2010).

1. The first step is to assess the benefit, and effect of the risk reducing measure, qualitatively. Since the attack can be adapt with the risk management program the potential risk to others is also important to evaluate. The procedure may consist of the loss of personal liberties due to applying the measure. If the cost of doing the measure is not high and the risk is not significant, then the measure applies, and the gross disproportion is not the point.
2. In case of large cost in the first step, analysts can perform cost-benefit analysis quantitatively. The $E[NPV \mid attack]$ and $ICAF \mid attack$ shall be calculated which both of them are conditional based on occurring attack. If the expectation for net present value is high or ICAF is small, also the probability of attack is not negligible then gross disproportion does not prove and measure should be taken.
3. If the circumstances in step two do not meet the criteria the next step is to perform an uncertainty assessment. The analysis prepares checklist of all possible uncertain elements and potential risk that have not included before, and if the checklist has high score then the measure shall be taken.
4. This step involves political consideration, and the decision-maker shall judge whether the risk reducing measure is gross disproportion to the benefit.

5 Conclusion

Two different perspectives apply for risk assessment worldwide in either industries or security sectors. The thesis presented PRA and uncertainty-based perspective to risk assessment. PRA, of course, involves background knowledge and expert's opinion but has no systematic procedure to evaluate them in the process and, therefore, this approach has a poor risk picture regarding uncertainty and data assessment. On the other hand, the terrorist attack is an adaptive plan against targets such as people, economy and infrastructure. Hence, dealing with this issue needs more complex and dynamic approach to risk assessment. Thus, uncertainty-based assessment is an alternative way to reveal all possible future events, particularly, in the security sector.

The next issue was to compare the existing scholarly literature within the area of risk assessment with the standard procedure for security risk assessment in Norway to find the possible weakness points. The thesis discussed the most significant weakness points of the Standard and concluded that the four top points need reviewing and changing. The weakness points are risk definition, risk picture, strategies, and the reducing measures. The risk definition consists of exact and known probability of a threat, and this implies to frequentist probability and the expected value that have challenged by many researchers, ref §4.2. Risk picture excludes uncertainty and the background knowledge as the main contributors of the risk picture. This weakness point avoids the decision-maker to have a clear overview of the future events and give incomplete information for further investigation. When considering the strategy to deal with the different level of risk, one of those four alternatives is to transfer risk to other, which has no justification according to existing literature. The last but not the least point is to apply the measure in connection with cost. The Standard suggests accepting the risk in case the condition, benefits gain, or cost of implementing measure(s) dictate. Here, the cautionary principle should apply and, at the same time, ALARP helps to find the balance situation, see §4.3.

When risk analysis evaluates different alternative for reducing the risk, the outcomes may have various types. Standard suggests to find the threat from various contributors include technical, organizational, and human resources. The various contributors have different values, for example, the value of statistical life, damage to the infrastructure, and damage to the environment have their values. Here, different frameworks exist to compare all alternatives, and each has various applications. Abrahamsen et al. (2011) argued the applied framework

should be consistent and transparent and conclude that the only way to have a procedure with these two principle is to transform all attributes into the comparable value and suggested pragmatic view on cost-benefit analsis. Moreover, they stressed that these frameworks are tools to help the decision-maker having the most useful and reliable decision and, therefore, the tools should take carefully to avoid the mechanical and decision-making process. Additionally, ALARP analysis should be a part of decision-making to balance the situation.

The thesis limited its attention to security risk Standard in Norway (*NS 5831*, 2014, *NS 5832*, 2014), but there exist other Standards which contribute to the security risk assessment. It is necessary to review all existing standard frameworks to find and correct possible weakness points. In §4.3 five principles of good decision-making presented but according to Abrahamsen et al. (2011) just transparency and consistency examined for the decision-making framework. The procedure can be reviewed for other principles to have the most suitable framework for decision-making.

References

Abrahamsen, E.B., Asche, F., Aven, T., 2011. To what extent should all the attributes be transformed to one comparable unit when evaluating safety measures? Bus. Rev. Camb. 19(1), 70–76.

Abrahamsen, E.B., Aven, T., 2012. Why risk acceptance criteria need to be defined by the authorities and not the industry? Reliab. Eng. Syst. Saf. 105, 47–50. doi:10.1016/j.ress.2011.11.004

Abrahamsen, E.B., Aven, T., Iversen, R.S., 2010. Integrated framework for safety management and uncertainty management. Proc. Inst. Mech. Eng. Part O: Journal of Risk and Reliab. 224, 97–103.

Aven, T., 2014a. Risk, surprises and black swans: fundamental ideas and concepts in risk assessment and risk management. Routledge, Abingdon, Oxon ; New York, NY.

Aven, T., 2014b. What is safety science? Saf. Sci. 67, 15–20. doi:10.1016/j.ssci.2013.07.026

Aven, T., 2013a. On the meaning of a black swan in a risk context. Saf. Sci. 57, 44–51. doi:10.1016/j.ssci.2013.01.016

Aven, T., 2013b. Practical implications of the new risk perspectives. Reliab. Eng. Syst. Saf. 115, 136–145. doi:10.1016/j.ress.2013.02.020

Aven, T., 2012. The risk concept—historical and recent development trends. Reliab. Eng. Syst. Saf. 99, 33–44. doi:10.1016/j.ress.2011.11.006

Aven, T., 2011. A risk concept applicable for both probabilistic and non-probabilistic perspectives. Saf. Sci. 49, 1080–1086. doi:10.1016/j.ssci.2011.04.017

Aven, T., 2010. Misconceptions of risk. Wiley, Chichester, West Sussex, U.K.

Aven, T., 2008. Risk analysis: assessing uncertainties beyond expected values and probabilities. Wiley, Chichester, England ; Hoboken, NJ.

Aven, T., Abrahamsen, E., 2007. On the use of cost-benefit analysis in ALARP processes. Int. J. Perform. Eng. 3, 345.

Aven, T., Flage, R., 2009. Use of decision criteria based on expected values to support decision-making in a production assurance and safety setting. Reliab. Eng. Syst. Saf. 94, 1491–1498. doi:10.1016/j.ress.2009.02.007

Aven, T., Krohn, B.S., 2014. A new perspective on how to understand, assess and manage risk and the unforeseen. Reliab. Eng. Syst. Saf. 121, 1–10. doi:10.1016/j.ress.2013.07.005

Aven, T., Reniers, G., 2013. How to define and interpret a probability in a risk and safety setting. Saf. Sci. 51, 223–231. doi:10.1016/j.ssci.2012.06.005

Aven, T., Vinnem, J.E., 2007. Risk management with applications from the offshore petroleum industry, Springer series in reliability engineering. Springer, London.

Aven, T., Vinnem, J.E., ESREL, European Safety and Reliability Association (Eds.), 2007. Risk, reliability and societal safety: proceedings of the European Safety and Reliability Conference 2007 (ESREL 2007), Stavanger, Norway, 25 - 27 June 2007, Balkema - proceedings and monographs in engineering, water and earth sciences. Taylor & Francis/Balkema, London.

Aven, T., Zio, E., Baraldi, P., Flage, R., 2014. Uncertainty in risk assessment: the representation and treatment of uncertainties by probabilistic and non-probabilistic methods. John Wiley & Sons Inc, Hoboken, NJ.

Bedford, T., Cooke, R.M., 2001. Probabilistic risk analysis: foundations and methods. Cambridge University Press, Cambridge, UK ; New York, NY, USA.

Blockley, D., 2013. Analysing uncertainties: Towards comparing Bayesian and interval probabilities'. Mech. Syst. Signal Process. 37, 30–42. doi:10.1016/j.ymssp.2012.05.007

Boyfield, K., 2006. Editorial: Better Regulation without the State. Econ. Affairs. 26, 2–8.

Cawood, I.J., McKinnon-Bell, D., 2002. The First World War. Routledge.
Dedianous, V., Fievez, C., 2006. ARAMIS project: A more explicit demonstration of risk control through the use of bow–tie diagrams and the evaluation of safety barrier performance. J. Hazard. Mater. 130, 220–233. doi:10.1016/j.jhazmat.2005.07.010
Earl, D.J., Deem, M.W., 2008. Monte Carlo simulations, in: Molecular Modelling of Proteins. Springer, pp. 25–36.
Egeli, A., 2014. Analysemetodikk i forbindelse med terrorisme: Bruk eller ikke bruk av sannsynlighet. University of Stavanger, Norway. Unpublished. Master Thesis.
Eldred, M.S., Swiler, L.P., Tang, G., 2011. Mixed aleatory-epistemic uncertainty quantification with stochastic expansions and optimization-based interval estimation. Reliab. Eng. Syst. Saf. 96, 1092–1113. doi:10.1016/j.ress.2010.11.010
Ezell, B.C., Bennett, S.P., von Winterfeldt, D., Sokolowski, J., Collins, A.J., 2010. Probabilistic Risk Analysis and Terrorism Risk. Risk Anal. 30, 575–589. doi:10.1111/j.1539-6924.2010.01401.x
Ferson, S., Ginzburg, L.R., 1996. Different methods are needed to propagate ignorance and variability. Reliab. Eng. Syst. Saf. 54, 133–144.
Ghahramani, S., 2005. Fundamentals of probability with stochastic processes, 3rd ed. ed. Pearson/Prentice Hall, Upper Saddle River, N.J.
Guikema, S.D., Aven, T., 2010. Is ALARP applicable to the management of terrorist risks? Reliab. Eng. Syst. Saf. 95, 823–827. doi:10.1016/j.ress.2010.03.007
Haimes, Y.Y., 2005. Risk Modeling, Assessment, and Management. John Wiley & Sons, Hoboken, NJ, USA.
Jones-Lee, M., Aven, T., 2011. ALARP—what does it really mean? Reliab. Eng. Syst. Saf. 96, 877–882. doi:10.1016/j.ress.2011.02.006
Levin, D.A., Peres, Y., Wilmer, E.L., 2009. Markov chains and mixing times. American Mathematical Soc.
Lindley, D.V., 2013. Understanding uncertainty, revised edition. John Wiley & Sons, Inc, Hoboken, New Jersey.
Matusitz, J.A., 2013. Terrorism and communication: a critical introduction. SAGE, Thousand Oaks.
Moles, P., Terry, N., 1996. Handbook of international financial terms. Oxford University Press, Oxford, England; New York.
NS 5831, 2014., Samfunnssikkerhet, beskyttelse mot tilsiktede uønskede handlinger. Krav til sikringsrisikostyring. Standard Norge.
NS 5832, 2014., Samfunnssikkerhet, beskyttelse mot tilsiktede uønskede handlinger. Krav til sikringsrisikoanalyse. Standard Norge.
NTV, 2014. Annual Threat Assessment. Norwegian Police Security Service, Norway.
OREDA: offshore reliability data handbook, 2002. . OREDA Participants : Distributed by Det Norske Veritas, Høvik, Norway.
Raychaudhuri, S., 2008. Introduction to Monte Carlo simulation, in: Simulation Conference, 2008. WSC 2008. Winter. IEEE, pp. 91–100.
Reniers, G.L.L., Audenaert, A., 2014. Preparing for major terrorist attacks against chemical clusters: Intelligently planning protection measures w.r.t. domino effects. Process Saf. Environ. Prot. 92, 583–589. doi:10.1016/j.psep.2013.04.002
Sun, S., Fu, G., Djordjević, S., Khu, S.-T., 2012. Separating aleatory and epistemic uncertainties: Probabilistic sewer flooding evaluation using probability box. J. Hydrol. 420-421, 360–372. doi:10.1016/j.jhydrol.2011.12.027
Taleb, N.N., 2010. The impact of the highly improbable, revised edition. Penguin Books Ltd, London.

Terrorisme | PST [WWW Document], 2014. URL http://www.pst.no/trusler/terrorisme/ (accessed 6.3.15).

Veland, H., Aven, T., 2013. Risk communication in the light of different risk perspectives. Reliab. Eng. Syst. Saf. 110, 34–40. doi: 10.1016/j.ress.2012.09.007

Vinnem, J.E., 2014. Offshore risk assessment: principles, modelling and applications of QRA studies. vol. 1&2, 3. ed. ed. Springer, London.

Willis, H.H., Rand Corporation (Eds.), 2005. Estimating terrorism risk. RAND, Santa Monica, CA.