Supply Chain Risk Assessment

Focusing on maritime transport to and from Iceland

Þórhallur Jóhannsson

Thesis of 30 ECTS credits
Master of Science in Engineering Management

June 2015

Supply Chain Risk Assessment

Focusing on maritime transport to and from Iceland

Þórhallur Jóhannsson

Thesis of 30 ECTS credits submitted to the School of Science and Engineering
at Reykjavík University in partial fulfillment
of the requirements for the degree of
Master of Science in Engineering Management

June 2015

Supervisor(s):

Páll Jensson, Supervisor
Professor, Reykjavík University, Iceland

Svana Helen Björnsdóttir, Co-Supervisor
PhD Student, Chairman of board at Stiki

Examiner:

Viktoría Jensdóttir, Examiner
M.Sc. Engineering at Síminn

Abstract

This thesis is intended to perform risk assessment of the supply chain focusing on maritime transports to and from Iceland. Companies that depend on secure and stable maritime transports need to be well informed and understand the risk of their supply chain disrupting. The assessment is performed by proposing research questions aimed at identifying key risk factors in the chain. Two techniques are selected that have different approach to identify risk factors. Firstly a so-called FMEA technique that approaches the assessment from bottom-up and secondly a so-called FTA technique that approaches the assessment from a top-down approach. The methodology of the techniques as well as the process of performing the techniques is described step by step in the thesis. The techniques provide in combination nine risk factors that are classified as key risk factors in addition to various other risk factors classified as less urgent.

Útdráttur

Þessari ritgerð er ætlað að framkvæma áhættumat á virðiskeðjunni með fókus á sjóflutninga til og frá Íslandi. Fyrirtæki sem reiða sig á örugga og stöðuga sjóflutninga verða að vera vel upplýst og skilja hver áhættan er á því að virðiskeðja þeirra gæti brotnað. Áhættumatið er framkvæmt með því að leggja fram rannsóknarspurningar sem beint er að því að finna lykil-áhættuþættina í keðjunni. Tvær aðferðir eru valdar sem hafa sitthvort nálgunina til að greina áhættuþættina. Annarsvegar svokölluð FMEA aðferð sem nálgast matið frá grunni og upp og hinsvegar svokölluð FTA aðferð sem nálgast matið frá toppi og niður. Aðferðafræði greininganna og ferlið við framkvæmd beggja greininganna er lýst skref fyrir skref í ritgerðinni. Greiningarnar fundu saman níu áhættuþætti sem eru flokkaðir sem lykil áhættuþættir til viðbótar við allmarga aðra sem eru flokkaðir sem minna áríðandi.

Supply Chain Risk Assessment

Focusing on maritime transport to and from Iceland

Þórhallur Jóhannsson

30 ECTS thesis submitted to the School of Science and Engineering
at Reykjavík University in partial fulfillment
of the requirements for the degree of
Master of Science in Engineering Management.

June 2015

Student:

_____

Þórhallur Jóhannsson

Supervisor(s):

_____

Páll Jensson

_____

Svana Helen Björnsdóttir

Examiner:

_____

Viktoría Jensdóttir

Contents

Abbreviations

FMEA	Failure Mode and Effects Analysis
FTA	Fault Tree Analysis
ISO	International Organization for Standardization
IEC	International Electrotechnical Commission
SCM	Supply Chain Management
SCRM	Supply Chain Risk Management
TEU	Twenty foot Equivalent Unit
PMI	Project management Institution
PMBOK	Project Management Bok of Knowledge
OED	Oxford English Dictionary
UNCTAD	United Nations Conference on Trade and Development
RPN	Risk Priority Number

List of figures

List of tables

1. Introduction

1.1 Background

In today's global environment where companies continuously try to expand their market coverage as well as distribute and seek cheaper production sites, it is imperative to be informed and have good knowledge about possible risk factors that can interrupt the business chain and what ways are possible to mitigate those factors.

Many companies that operate in Iceland are very dependent on secure and stable maritime transports, such as imports of raw materials or exports of finished goods to consumers. Those companies rely on that their goods will reach its destination undamaged and on time. These companies need to be well informed, understand and also be able to measure if possible the risk that their supply chain might disrupt because of the maritime transport link failing. The maritime transport link can fail because of incidents that may be called conventional such as; vessel capacity overload or mechanical breakdowns. But it can also fail because of more rare unforeseen incidents that can be called unconventional such as; labor crisis or perhaps more Icelandic specific as natural disasters.

Having a secure and stable maritime transport link requires investment of time and money in equipment and processes. Costs that eventually will need to be reflected in prices to end consumers. Having unstable and risky maritime transport link will also be costly in lost values or lost opportunities. Both situations will eventually result in higher production cost or less sales and lead to worse financial results.

Consequently selecting and performing thorough analysis with the right approach is very valuable. An effective approach that can detect the most of possible risk factors as well as support the creation of mitigation strategy in the fastest and cheapest way possible.

1.2 Supply chain management

The supply chain is the process of which a material, service, information or money flows through. It is a chain of separate links which can be maritime or air transport, as well as warehousing, assembly and distribution on land. Material can for example flow from supplier onwards to manufacturer onwards to a wholesaler and so on to an end consumer. The chain comes in all variations; it can be short or long process, simple or complex products, span one country or half the world. To demonstrate the complexity one can look at the assembly of the Boeing 787 airplane. Whereas parts are produced all over the world to be assembled in Everett USA and finally delivered to end buyers once completed.

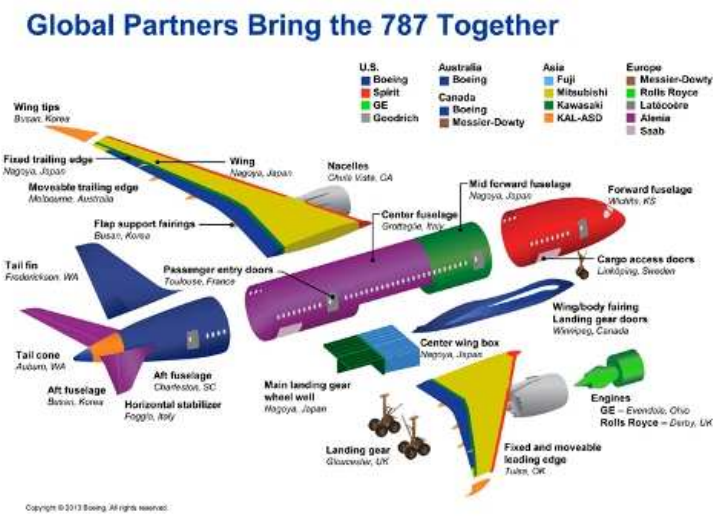


FIGURE 1: BOEING ASSEMBLE PARTS ORIGINATIONS

SOURCE: www.boeing.com

Managing these flows requires a strong oversight to coordinate and integrate both between and within companies that can for example be both manufacturers and wholesalers. An effective supply chain management minimizes costs of the process such as transport and inventories as well as securing timely deliveries. Important prerequisite to an effective supply chain management is to be well informed about risk factors and what mitigation strategies are available.

1.3 Maritime transport

Maritime transport is the largest mode of transport of cargo between continents and countries both by volume and value. In UNCTAD Review of Maritime Transport from 2014 it is estimated that around 80% of the world's trade is carried at some time by the international shipping companies. (UNCTAD, 2014). The fact that maritime transport is this significant is naturally based on historical roots but is upheld in current environment with cheaper prices compared to other modes such as air transport as well as it is a lot bigger and more flexible capacity compared to any other modes of transport. In Iceland all cargo to and from the country is transported with airfreight or maritime transport. According to Statistics Iceland imports plus exports to the country amounted to approximately 6,5 million tons in the year 2013. Of that approximately 50% was transported with container vessels through the port of Reykjavik according to their website. In addition containers including aluminum from the smelter Rio Tinto Alcan are exported through the port of Hafnarfjörður, making containerized cargo account for more than half of the imports and exports in Iceland.

The shipping industry comprises of companies operating various different types of vessels designed for different types of cargo, locations and sailing routes. Generally the industry can be split into four main categories by vessel design;

- Bulk vessels — Designed for transportation of raw cargo such as meal, grain, cement and coal.
- Container vessels — Designed to carry containers with wide range of cargo, such as general consuming goods, frozen fish or equipment. The size of the containers is measured in TEU.
- Tanker vessels — Designed for transportation of crude oil, chemicals and petroleum products.
- Specialized vessels — Designed specifically to carry other "difficult" cargo such as refrigerated cargo.

In Iceland the shipping industry comprises of few smaller companies that can offer transportation with specialized vessels or container vessels and two large companies, named

Eimskip and Samskip. The two large are relatively similar in size and operations and can offer transportation with vessels in all of the above mentioned categories except for the tanker vessels. Eimskip and Samskip combined service the majority of seaborne imports and exports in Iceland. Both offer scheduled sailing routes with containers vessels on weekly basis or more often and operate their main terminals in Reykjavik.

Eimskip operates seven container vessels servicing the Icelandic market which range from 700 to 1.457 TEUs in size each. These vessels sail to ports in Faroe Island, Scandinavia, UK and the mainland of Europe as well as the east coast of Canada and the United States. These seven vessels sail on three different sailing routes which range from 2-4 weeks each round trip, resulting in 2-3 departures every week from Reykjavik.

FIGURE 2: EIMSKIP SAILING ROUTES

SOURCE: www.eimskip.is

FIGURE 3: SAMSKIP SAILING ROUTES

SOURCE: www.samskip.is

Samskip operates three container vessels servicing the Icelandic market which range from 505 to 908 TEUs in size each. These vessels sail to ports in Faroe Island, Scandinavia, UK and the mainland of Europe. These three vessels sail on two different sailing routes which take 2 weeks each round trip, resulting in 1-2 departures every week from Reykjavik.

1.4 Research questions

As described here above companies which operate in Iceland and are dependent on secure and stable maritime transport face a challenge of identifying correctly and managing its risk

associated to disruption of their supply chain. To investigate the risk for these companies two research questions are proposed.

1. What are the key risk factors in Iceland that can interrupt or break the supply chain, focusing on maritime transport?
2. How can these risk factors be mitigated to avoid business interruptions?

The objective with this thesis is to answer these two questions with the main weight and attention to the first question. To answer the first one different risk assessment techniques will be reviewed and the most suitable ones selected and compared if necessary. This process will be performed in compliance with ISO standards on risk assessment. The second question is in effect an extension of the first one and is considered secondary in this thesis. To answer the second one ISO standards on risk management will be reviewed as well as looking for available examples and previous similar researches. Regarding the second question it is not the intention of this thesis to investigate current risk mitigation strategies in place at any company and their effectiveness but rather to generally understand what options are available and their applicability.

1.5 Assumptions and limitations

This thesis focuses solely on maritime transports to and from Iceland and is limited to containerized cargo. As demonstrated here above, of the four categories of vessel types, container vessels carry the most of imported and exported cargo in Iceland. In addition it has the widest range of type of companies, from small companies with specific cargo and few shipments to large global companies such as aluminum smelters with regular shipments. Still this is quite small market with relatively few service providers of maritime transport operating terminals in few ports. In addition its users, the importers and specifically exporters, are also quite monotonous group. Main goods of exports are fish and aluminum and main goods of imports are daily consuming goods and equipment. This results in limited size of data and possibly repetitiousness.

1.6 Structure

The thesis first chapter is intended to introduce the problem, briefly familiarize the reader to the concept of supply chain management and specifically the link of maritime transport, as well as introducing the research questions and assumptions and limitations. The second chapter introduces literature review prior to writing of this thesis which includes definitions of risk with emphasis on the supply chain risk. The third chapter then introduces the selected research methods and the process of which how they are used herein, followed by its results in chapter four. Final chapters include discussions and conclusion with response to research questions.

2. Literature review

2.1 Preparations

In preparing for the writing of this thesis relevant areas of literature have been examined and selected literature summarized specifically here in subchapters. The process of the review was to start broadly on literature concerning the general concept of risk and work towards more specific literature that could assist in search for response to the research questions as well as examine what researches have already been performed on the subject. As the research questions are aimed at the supply chain, literature concerning supply chain risk and specifically risk in maritime transport are examined. In addition, in the quest, to increase the likelihoods that objectives of the research will be reached relevant standards on risk management and risk assessment are examined and how it can be utilized for the research.

2.2 Definition of risk

In the current ever-changing environment every person, group, process or company is continuously exposed to some uncertainties in its daily actions. These uncertainties can either be the consequence of internal factors such as poor decision making or incompetency to control situations or the consequence of external threats or reformed environment. The internal factors are very difficult to detect and measure as it is for example based on human elements such as confidence and state of mind. The external factors we can usually measure and give probabilities based on historical statistics, such as there is 20% change of rain tomorrow based on the weather conditions past few days. Whether these uncertainties do actualize and what effects, if any, it has on the receiver of the effects are different in each case.

In its paper from 1982 Kahneman and Tversky researched the variants of uncertainty and demonstrated that there are multiplicity of states and experiences of uncertainty that cannot be described by a single concept or dimension of probability. *"Our distinction between ignorance and external uncertainty is closely related to a more general distinction between internal and external attributions of experience. Color, size and texture, for example, are normally*

experienced as properties that belong to external objects, but pains, feelings and memories *are attributed to the experiencing subject rather than to the eliciting object"* (Kahneman & Tversky, 1982) In essence their research reveals that uncertainties are surely various, can be complex and cannot always be assigned a probabilistic values.

There are several official definitions of risk that have been published by acknowledged universities and organizations. That includes the Oxford English Dictionary which has its definition of risk being the following:

> *"(Exposure to) the possibility of loss, injury, or other adverse or unwelcome circumstance; a chance or situation involving such a possibility"* (OED, 1997)

The Project Management Institution has also issued its definition of risk being the following:

> "*Risk is an uncertain event or condition that, if it occurs, has an effect on at least one [project] objective"* (PMBOK, 2013)

A third one comes from the International Organization for Standardization, in its standard on risk management ISO31000 risk is defined as:

> *"…effect of uncertainty on objectives. …An effect is a deviation from the expected – positive and/or negative"* (ISO31000, 2009)

The above mentioned definitions of risk have all its uniqueness and differ somewhat but the common denominator here is that risk is defined as a consequence of an uncertain event that possibly actualizes and if it does than it will have some effects. The main difference is that OED defines the effects as being adverse, PMI does not state anything about results of the effects but ISO states that the effects can be both positive and/or negative. Following the common denominator it can be concluded that not all uncertainties are risks, only those uncertainties that if actualizes it will have some effects.

To present this quantitatively one can look to definitions introduced by Kaplan and Garrick in their article from 1981 where they define risk as involving both uncertainty and some kind of loss or damage. In essence they define risk as the answer to the following three questions;

1. *"What can go wrong?"*
2. *"How likely is it to go wrong?"*
3. *"If it does go wrong, what are the consequences?"* (Kaplan & Garrick, 1981)

The answer to the first question defines an uncertain event, denoted by S_i. The answer to the second question is the probability of that event actualizing, denoted by P_i. The answer to the third question is the consequence of the event actualizing, denoted by X_i. Formally we can therefor say that the risk, denote by R, is the following set of triplets:

$$R = \{S_i, P_i, X_i\}, where\ i = 1, 2, \dots, N$$

Furthermore Kaplan and Garrick make a distinction between risk and hazard. Whereas hazard is a real source of uncertain event but risk is the probability of an event actualizing with consequences. A simple example to portray the difference is the following: A wet floor can be a hazard, slipping and hurting yourself is the risk. In addition a separation of hazard and threat needs to be identified as a hazard is the source in harmless state and threat is the source in harmful state. This distinction between hazard and risk supports the assertion that risk can be managed, that is reduced, if the hazards are known and understood. Managing the risk means to reduce vulnerability to hazards in order to minimize or eliminate the consequences. Vulnerability can be viewed as an assessment of how well or poorly one is protected against an event.

The content covered in this subchapter reveals that already there are challenges in simply defining what risk is, as there does not exists a single universal definition, as well as that it can be difficulty in assigning a probabilistic values to some uncertainties. Still there are similarities between the definitions and this research will work out from the definition of Kaplan and Garrick. In addition to challenge the problem of assigning probabilities, risk will be analyzed from different perspectives and results compared.

2.3 Supply chain risk

The study of supply chain risk is relatively young as a specific research area within the field of supply chain management. Even so ever increasing number of researches has been issued since the start of the 2000's in line with increased global activities and awareness to this field. This development is demonstrated in a research published in 2011 by Piyush, Gopal and Murali where they perform a review of 15 recognized journals on business and science and search for publications on the matter by searching for keywords on supply chain risk management. Their result can be seen in the below figure.

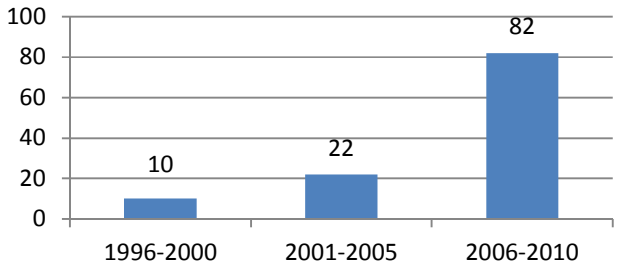


FIGURE 4: PUBLICATIONS ON SCRM IN GROUP OF FIVE YEARS

SOURCE: (Singhal, Agarwal, & Mittal, 2011)

Still it is interesting to discover that parallel to this increase in researches and academic awareness it seems that corporations are not all responding. In 2014 the Global Supply Chain Institute at the University of Tennessee conducted a research where a questionnaire was sent to 150 different supply chain executives. The findings of the research were among other the following: *"None of those surveyed use outside expertise in assessing risk for their supply chain"* and *"90% of corporations do not quantify risk when outsourcing a production"* (Dittmann, 2014) Similar results can be found in a research conducted by the multinational consulting company Accenture in the same year 2014. The research involved a web-based survey of 1.014 senior executives' at large global companies. The research revealed among other the following: *"…while a vast majority of executives believe supply chain risk management is a priority, only a small group of companies employ practices that enable them to generate a significant risk management ROI."* (Don't Play it Safe When it Comes to Supply Chain Risk Management, 2014) Despite many corporations lack of response to act on supply chain risk the above mentioned

researches do though confirm corporation's awareness and understanding that the issue to find the best way to analyze and manage supply chain risk is important and valuable.

As stated previously in this thesis supply chains come in all variations and can be very long and complex processes. That complexity results in vulnerability to various types of risks. As a response to this diversity and in the effort to better understand, identify and hopefully manage these risks many researches published in recent years propose a classification by risk sources. The simplest classification would be to split the risk sources between external and internal. The external risks then are those that arise from outer factors that can be difficult or impossible to manage such as new regulations, natural disasters or terrorism. The internal risks then on the other hand originate within the chain itself, either in specific connection points or in the links between them. Risks that should be somewhat or fully manageable, such as mechanical breakdowns or incorrect loading of a containers.

In its research published in 2003 by Jüttner, Peck and Christopher they propose a classification of supply chain risk sources into three groups. *"Environmental risk sources, network-related risk sources and organizational risk sources"* (Jüttner, Peck, & Christopher, 2003) further demonstrated in the below figure.

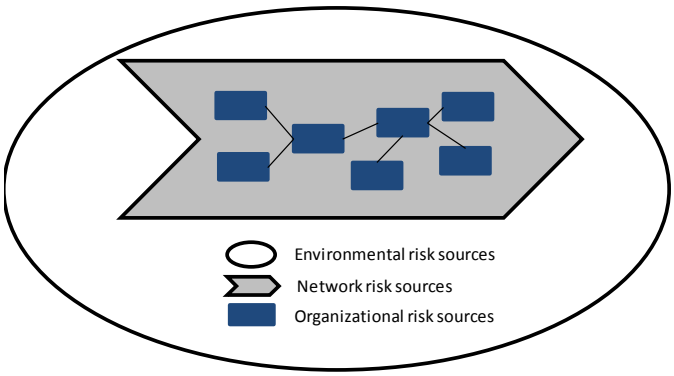


FIGURE 5: THREE CATEGORIES OF RISK SOURCES IN SUPPLY CHAINS

SOURCE: (Jüttner, Peck, & Christopher, 2003)

Furthermore Jüttner, Peck and Christopher explain the three classes as follows:

"Environmental risk sources comprise any uncertainties arising from the supply chain environment interaction. These may be the result of accidents (e.g. fire), socio-political actions (e.g. fuel protests or terrorist attacks) or acts of God (e.g. extreme weather or earthquakes).

Organizational risk sources lay within the boundaries of the supply chain parties and range from labor (e.g. strikes) or production uncertainties (e.g. machine failure) to IT system uncertainties.

Network-related risk sources as the third category arises from interactions between organizations within the supply chain." (Jüttner, Peck, & Christopher, 2003)

In another research by Cristopher and Peck published the year after in 2004 they propose a more detailed classification of supply chain risk in five sources of three groups.

- *"Internal to the firm*
    - *Process*
    - *Control*
- *External to the firm but internal to the supply chain network*
    - *Demand*
    - *Supply*
- *External to the network*
    - *Environmental"* (Christopher & Peck, 2004)

Further demonstrated in the below figure:

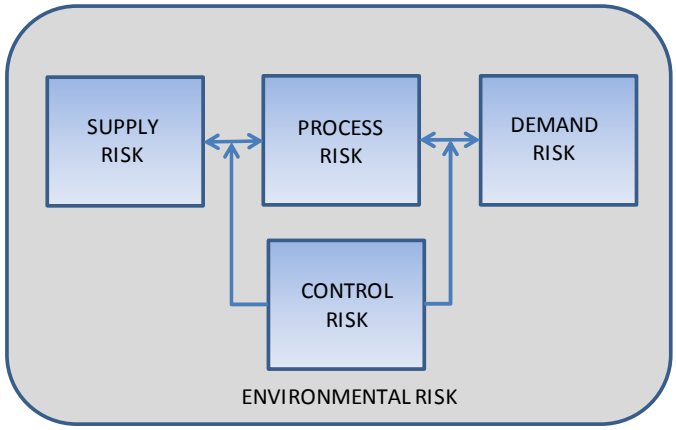


FIGURE 6: FIVE CATEGORIES OF RISK SOURCES IN SUPPLY CHAINS

SOURCE: (Christopher & Peck, 2004)

Main distinctions from previous definition published in 2003 are of two kinds. Firstly what was defined as network-related risk is replaced with definitions of supply and demand risk. Demand risk being the potential disturbance in downstream flow of product, service, cash or information in the supply chain and supply risk being potential disturbance in the opposite upstream flow. Secondly what was defined as organizational risk is replaced with definitions of process and control risk. Process risk being the risk of disruption in internal processes and control risk being the risk of misuse or inactivity of rules and systems that govern the processes.

In contrast to the classification approach on supply risk definition, it is interesting to review a research published in 2003 by Zsidisin where he proposes his definition of supply chain risk. In his research he performs a case study on seven pre-screened selected companies and investigates how they managed their supply risk. Firstly he examines how the companies currently define supply risk and discovers that majority of the companies do not have a formal definition. Secondly he goes through a series of data analysis and investigation on the company's management of supply chain processes. After reaching what is called saturation in the methodology used in his analysis he suggests the following definition of supply risk:

> *"Supply risk is defined as the probability of an incident associated with inbound supply from individual supplier failures or the supply market occurring, in which its outcomes*

result in the inability of the purchasing firm to meet customer demand or cause threats to customer life and safety" (Zsidisin, 2003)

From the literature reviewed in this subchapter it can be concluded that, as there is with the definition of general risk, there is also a challenge in identifying single universal definition of supply chain risk and it matters what approach is selected. This further supports the notion that analyzing risk from different perspectives can give better and more thorough results.

2.4 Maritime transport risk

As this research aims at the part of the supply chain that is maritime transport to and from Iceland it is necessary to review what has been published specifically on that subject. To the best knowledge of the author there are no researches that have been published so far on the subject in Iceland but there are several researches and papers that have been published abroad on maritime transport risk in general. In one such a paper published in 1998 the authors perform: *"…an analysis on the factors that are important determinants of maritime transportations risk."* (Psaraftis, Panagakos, Desypris, & Ventikos, 1998) In their analysis they create a database of accidents from 52 copies of Lloyd's Casualty Reports, which altogether contain more than 7.000 accidents. From their database they identify four main events that together account for more than 80% of the sources of marine accidents, which are:

- *Contact / collision*
- *Grounding*
- *Mechanical problem*
- *Hull problem*

Their analysis is limited to being quite facility oriented and high level, as it does not include further details on the real sources of events actualizing and causing accidents. Such as the real cause of a collision or what exactly the mechanical problem was. Still it provides interesting and valuable information on where to search for vulnerabilities.

In another report issued by UNCTAD in 2006 the approach to evaluating maritime transport security is examined. The paper identifies pitfalls in current approach and suggests an alternative analytical framework that reflects better the complex nature of global transport systems.

> *"It is difficult to assess and manage risk in a uniform manner when dealing with complex-system configurations presenting low probability risks and high potential impacts, such as maritime transport. The fragmented nature of existing security risk-assessment and management frameworks results in different sets of risk assessment and risk-based decision models."* (UNCTAD, 2006)

In essence the report is attempting to shift the subject of maritime transport security from the current focus on facility security to an extended framework of supply chain security. The alternative approach that is suggested is based on the three group classification proposed in 2003 by Jüttner, Peck and Christopher and described here in chapter 2.3.

> *"In the current maritime security regime, there is a strong emphasis on environmental and organizational risks and little focus on network-related vulnerabilities. These network-related risk sources are part of the network design and structure and their assessment is needed to avoid overlooking their capacity to absorb or amplify the impact of events from environmental or organizational risk sources."* (UNCTAD, 2006)

From this literature it can be concluded that whilst it is important to analyze risk factors of the facilities used in the maritime transport it is also necessary to analyze the overall risk factors in relation to the chain the transport belongs to.

2.5 International standards

There exist various standards on supply chain processes and maritime transport security as well as risk management in general. Perhaps most recognizable of all are the standards issued by the International Organization for Standardization referred to as ISO. Of all ISO standards there are two that should be mentioned specifically in relation to this report. First to mention is the ISO

31000:2009 standard on Risk Management - Principles and Guidelines. It is a comprehensive guideline on all risk management, from risk identification to risk analysis and risk evaluation. As well as risk treatment, risk monitoring and communication.

> *"This International Standard provides principles and generic guidelines on risk management. This International Standard can be used by any public, private or community enterprise, association, group or individual. Therefore, this International Standard is not specific to any industry or sector"* (ISO31000, 2009)

In addition to be applicable to any type of industry it provides a common approach in risk management that can be used to deal with any types of risks, having negative or positive effects.

The second ISO standard to be mentioned is the ISO/EIC 31010:2009 that addresses specifically risk assessment. It is a supporting standard for ISO 31000 and it provides a range of techniques that can be applied in risk assessment as well as guidelines on selection and application.

> *"Risk assessment attempts to answer the following fundamental questions:*
>
> - *what can happen and why (by risk identification)?*
> - *what are the consequences?*
> - *what is the probability of their future occurrence?*
> - *are there any factors that mitigate the consequence of the risk or that reduce the probability of the risk?"* (ISO/IEC31010, 2009)

The standard splits risk assessment into three parts in sequence.

1. *"**Risk Identifications** is the process of finding, recognizing and recording risk*
2. ***Risk analysis** is about developing and understanding of the risk*
3. ***Risk evaluation** uses the understanding of risk obtained during risk analysis to make decisions about future actions"* (ISO/IEC31010, 2009)

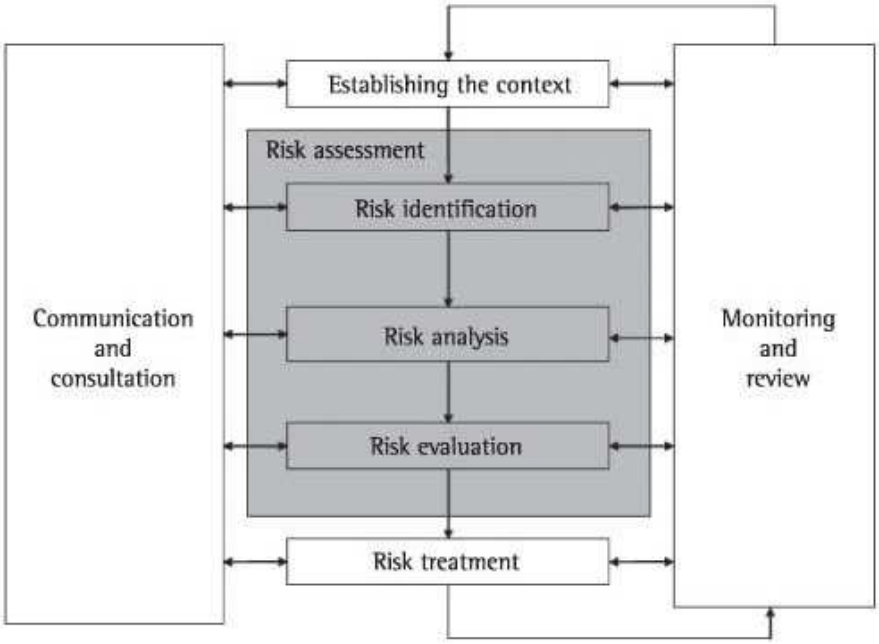


FIGURE 7: CONTRIBUTION OF RISK ASSESSMENT TO THE RISK MANAGEMENT PROCESS

SOURCE: (ISO/IEC31010, 2009)

In the effort to enhance accuracy and reliability of the process to find a response to the research questions the guidelines from these standards will be followed where applicable.

3. Research methods

3.1 Research approach

Following the literature review and definitions and conclusions made therein, the approach in this research will be to follow guidelines from aforementioned ISO standards, specifically the ISO/EIC 31010:2009 standard on risk assessment. Furthermore a mixture of qualitative and quantitative approach will be applied, with the main focus and effort to the qualitative part. The qualitative method will be conducted by observations into the operations at Eimskip and Samskip as well as interviewing experts at those companies that work in maritime transport, related operations and security management. The intention is to gather insight into supply chain processes and specifically maritime transport, identify possible hazards in these processes and rank them. The quantitative approach will be conducted parallel and/or following the qualitative approach, where it will be tempted to estimate probabilities and assign numerical values to identified risk factors. The quantitative approach will be conducted by interviews and questions to workers in maritime transport, related operations and security management.

To perform the risk assessment the ISO/EIC 31010:2009 standard suggests various proven techniques that can be utilized. For this research two separate techniques that have different perspective on the supply chain process have been chosen called Failure Mode and Effects Analysis and Fault Tree Analysis. How the techniques are utilized in this research and why it was selected is supported in the following chapters.

3.2 Failure Mode and Effects Analysis

3.2.1 Brief history

Failure Mode and Effects Analysis referred to as FMEA is a technique that was developed in the late 1940s by engineers in the US armed forces. The objective was to classify failures according to their impact on mission safety. Later it was adopted and refined in the Apollo space program to mitigate risk in processes were small sample sizes were affecting risk analysis. From there on the application of the technique gained momentum as manufacturing companies such as Ford

Motor Company adopted the method. Following further popularity the method is currently extensively used in variety of industries such as design, manufacturing and services.

3.2.2 Reasoning for selection

From the list of techniques suggested by the ISO/EIC 31010:2009 standard, FMEA is one of few which is categorized and strongly applicable for risk identification, analysis and evaluation. In a research published in 2013 by Curkovic, Scannell and Wagner the authors investigate how and if companies are applying FMEA for their supply chain risk management.

> *"Analyzing the risk associated with SCM is a relatively new subject, and little has been done to assist managers with this process. But one thing is certain, documenting and analyzing risk must be an essential part of continuous improvement… Most managers supported a modified version of the tool that could be used to help evaluate the risk of SCM decisions. For several of the firms in this study, FMEA is a well-documented and proven technique commonly used to evaluate the risk for failures in product and process designs."* (Curkovic, Scannell, & Wagner, 2013)

Their research revealed that there are limited numbers of companies that are applying FMEA for SCRM is but those that do indicated that it provided a substantial benefits if used properly and consistently. But most importantly FMEA generally suits well to identify risk factors that are internal to the firm or the process, in this instance the maritime transport process. Risk factors as were defined by Cristopher and Peck, the process risk and the control risk.

3.2.3 Methodology

Essentially FMEA is a systematic bottom-up approach whereas potential failures of a product, process or design are identified, analyzed and documented in a worksheet. Each identified potential failures are also assigned values as to the likelihoods of occurrence, degree of severity and detectability. By multiplication of these values a so called risk priority number is obtained.

Furthermore the effects of these failures on performance and safety are evaluated and appropriate actions decided to eliminate or minimize the effects.

FMEA has been developed to be utilized in various industries and sectors, in his book published in 2003 Stamatis presents four classes of FMEA, system, design, process and service.

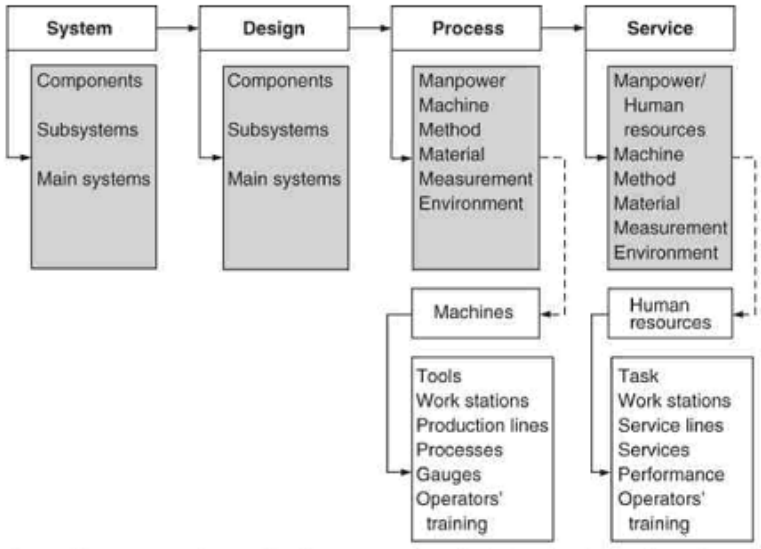


FIGURE 8: TYPES OF FMEAS

SOURCE: (Stamatis, 2003)

In this research the task to respond to the research questions will be approached by utilizing the definition of the service FMEA. In his book Stamatis also further defines among other outputs and benefits of the service FMEA which will assist with utilization of this approach.

There is not a single correct method for executing an FMEA as there can be slight differences that need to be adjusted for, such as in the environment or availability of resources, in each case. Many versions have been described by users and some companies and institutions have even defined standardized procedures. This thesis guides from standards issued by the US Department of Defense that can be summarized in the following ten steps.

Step 1: Identify components and associated functions.

The first step of an FMEA is to identify all of the components to be evaluated. This may include all of the parts that constitute to the process or, if the focus is only part of a process, the components that make up that part. The functions(s) of each part are briefly described.

Step 2: Identify failure modes.

The potential failure mode(s) for each part are identified. Failure modes can for example be complete failures, partial failures and failures over time, etc. It is important to consider that a component may have one or more failures.

Step 3: Identify effects of the failure modes.

For each failure mode identified, the consequences or effects on the component, product or process are listed. These effects are best described as seen through the eyes of the owner of the transported goods.

Step 4: Determine severity of the failure mode.

The severity rating indicates how significant of an impact the effect is for the owner of the transported goods. Severity can range from unnoticed effects to critical effects. Depending on the FMEA method employed, severity is usually given either a numeric rating or a coded rating and can be modified to the project. Here a scale of 1-10 ratings has been defined as follows.

Rating	Degree of severity
1	Unnoticed effects
2	Relatively low effects
3	Low effects
4	Noticeable effects
5	Relatively moderate effects
6	Moderate effects
7	Relatively high effects
8	High effects
9	Significant effects
10	Critical effects

TABLE 1: FMEA SEVERITY RANKING

Step 5: Identify causes of the failure mode.

For each failure mode its causes are identified. These causes can be of all sorts and can for example vary from human errors such as lack of knowledge to a component malfunction that result in process disruption.

Step 6: Determine probability of occurrence.

The probability of occurrence can be determined from historical data or estimated from known probabilities of similar events. If this information is not available a subjective rating is made based on the experience and knowledge of the experts working in the field. Here a scale of 1-10 has been defined as follows.

Rating	Likelihood of occurrence	Probability
1	Remote likelihood of failure	1 in 1.000.000
2	Low likelihood of failure	1 in 300.000
3	Infrequent failure	1 in 25.000
4	Occasional failure	1 in 2.000
5	Relatively moderate failure rate	1 in 500
6	Moderate failure rate	1 in 100
7	Relatively high failure rate	1 in 20
8	High failure rate	1 in 8
9	Almost certain failure rate	1 in 3
10	Certain failure rate	1 in 1

TABLE 2: FMEA OCCURRENCE RANKING

Step 7: Identify controls.

Controls that are currently in place that either prevent or detect the cause of the failure mode need to be identified. Preventative controls can either eliminate the failure mode or reduce its rate of occurrence.

Step 8: Determine effectiveness of current controls.

The effectiveness of the controls in place needs to be determined to estimate its usefulness to avoid failures. Control effectiveness ratings can be customized similar as for the severity and the occurrence ranking. Here a scale of 1-10 has been defined as follows.

Rating	Ability to detect	% detectability
1	Certain detectability	95 – 100
2	Almost certain detectability	90 – 94
3	High detectability	80 – 89
4	Relatively high detectability	70 – 79
5	Moderate detectability	60 – 69
6	Relatively moderate detectability	50 – 59
7	Occasional detectability	35 – 49
8	Infrequent detectability	20 – 34
9	Low detectability	0 – 19
10	No detectability	0

TABLE 3: FMEA DETECTABILITY RANKING

Step 9: Calculate risk priority number.

The risk priority number is a multiplication of the severity ranking, the occurrence ranking and the detectability ranking. It can be used to prioritize failure modes for actions.

Step 10: Determine actions to reduce risk of failure mode.

The final step is to decide on actions taken to reduce risk of failures and assign responsibility for completion. Some failures will require immediate action while others can be scheduled with later targeted completion dates. Alternatively some failure modes may not receive any attention or be scheduled to be reviewed again at a later date. After decided actions have been completed the severity, occurrence and detectability rankings should be re-evaluated in order to estimate effectiveness of the actions.

While conducting the FMEA steps, results for each step shall be documented in a FMEA worksheet. The worksheet can be generated in excel or other spreadsheet software.

Rating Before Action									
Item Identification	Function/Process	Potential failure mode	Potential effects of failure	Severity Rating (S)	Potential causes of failure	Occurence rating (O)	Current process controls	Detection rating (D)	Risk priority number (RPN=S*O*D)
What are the items in relevance	What is the process	What can go wrong ?	What is the impact if failure mode happens	A rating corresponding to the seriousness of an effect of a potential failure mode. (scale: 1-10. see ranking table)	What causes the failure mode to happen?	A rating corresponding to the rate a failure mode can occur, before any additional process controls are applied. (scale: 1-10. see ranking table)	What are the existing controls or procedures to detect and prevent failure modes	A rating corresponding to the likelihood that current controls will detect the potential failure mode before it happens. (scale: 1-10. see ranking table)	For a given potential failure mode, how bad the outcome is multiplied by how likely it would actually happen multiplied by what things are in place today to prevent or notice it before it happens

TABLE 4: FMEA WORKSHEET ANALYSIS TEMPLATE

Action Plan				Revised Rating			
Recommended actions	Responsibility and target date	Actions taken	Implementation closure date	S	O	D	RPN
What actions can be taken to reduce occurence or improve detection	Who is responsible for the actions taken	What actions are taken?	When have actions been implemented fully?	Severity rating revised	Occurence rating revised	Detectoin rating revised	RPN number revised

TABLE 5: FMEA WORKSHEET ACTION PLAN TEMPLATE

3.3 Fault Tree Analysis

3.3.1 Brief history

Fault Tree analysis referred to as FTA is a technique that was developed in the 1960s by Bell Telephone Laboratories for the US Air forces. The objective was to evaluate safety of the Minuteman lunch control system. Shortly later it was adopted by Boeing Aircraft Company and expanded to a significant system safety and reliability tool. Following Boeings expanded use it was adopted by other hazardous industries such as the nuclear power and chemical industries. Currently its usability has also expanded into various other industries and it is widely used in system safety and reliability engineering.

3.3.2 Reasoning for selection

Comparing FTA with FMEA reveals the contrast of the two as FTA is a top-down approach. It starts from a definition of an undesired top event followed by identification of possible next level causes of that event and so on to next level until the root causes are identified. Consequently FTA suits very well with FMEA to provide different perspective on the product or process being assessed for risk. This suitability has been pointed out and utilized before.

> *"The FTA always supplements the FMEA and not the other way around. In general, its application may be in a system or subsystem environment with a focus on identifying the root factors that could cause a failure and their interdependent relationships."* (Stamatis, 2003)

Another reference to mention is a paper published in 2014 by Khaiyum and Kumaraswamy where they present an integration of FMEA and FTA to analyze different causes of failures.

> *"The integrated FTA/FMEA approach ensures to be effective risk identification and reduction which can be applied on simple to complex applications. Further, this approach results in generation of risk priority values based on which mitigation plans can be formulated. The approach thus reduces human effort and yields efficiency in achieving higher reliability during system development process."* (Khaiyum & Kumaraswamy, 2014)

In addition FTA suits well to identify the remaining risk factors as defined by Cristopher and Peck, which are the external factors, demand risk and the supply risk and especially the environmental risk.

3.3.3 Methodology

In essence FTA is a technique where factors and causes that can contribute to a specific undesired top event actualizing are identified and organized in a logical manner and represented graphically in a diagram. In the diagram the undesired top event is represented as the top of a tree of logic. Below that event is a logic gate that can be "OR" or "AND" gates, meaning that underlying events below those gates can be independent causes or dependent

causes for the undesired top event actualizing. This is continued downwards the tree, where levels of gates and events exchange until root causes have been identified. Below picture demonstrates an example of how a tree is constructed combined of events and gates, graphic symbols further described in Appendix 1.

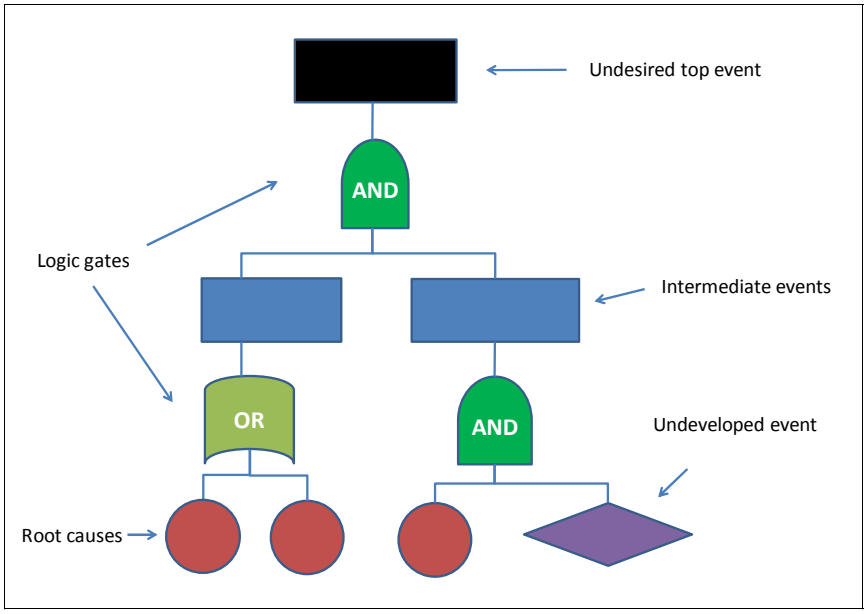


FIGURE 9: FTA DIAGRAM EXAMPLE

The philosophy and application of the Fault Tree analysis was first published in reports issue by Boeing in 1964 and 1968. Those reports included initial introduction of the basic concepts of FTA and the method for diagraming events to be analyzed with images of the graphic symbols. In addition it included a six step process to conduct the Fault Tree Analysis. Since these reports were issued the method itself and the process to conduct it has evolved in line with changed environment, better computers and more diverse applicability of the method. Currently there are several approaches of conducting FTA that have been described by users adapted for each case. This thesis follows a common approach of conducting the FTA, based on the original definitions as described in the following five steps.

Step 1: Define the undesired top event to study.

Importantly the top event needs to be well defined. It should not be too broadly defined but rather more specifically and preferably include both what the event is and when it happens. To

identify the top event the inclusion of experts in the process is necessary as a wrongly selected top event leads eventually to incorrect results.

Step 2: Obtain an understanding of the system.

Familiarize and study the system as much as possible. Identify all relevant events that can lead to or have some affects in the undesired top event actualizing. Also how and when these events have any effect on each other, sequentially or simultaneously. Continue this identifications of events downwards until root causes have been identified. This is performed with observations of the system and inclusion of expert knowledge in the process.

Step 3: Construct the fault tree.

After having identified and defined the undesired top event and obtained understanding of the system next step is to construct the fault tree. Fault tree is among other based on logic “OR” and “AND” gates, events and root causes. See figure 11 for example and Appendix 1 for full list of graphic symbols.

Step 4: Evaluate the fault tree.

After the fault tree has been constructed it is evaluated and analyzed for possible improvements. In addition it is tempted to assign probabilities to root causes, consequently calculate upwards the tree and identify which events are most likely to cause the undesired top event and rank them. Probabilities are calculated across the logic gates, multiplied across an “AND” gate and added across an “OR” gate. That provides necessary information for the final step.

Step 5: Control the hazards identified.

The final step is simply to identify actions that can assist in eliminating or decreasing the likelihood of root causes affecting upwards the tree to eventually affect the undesired top event in actualizing.

4. Research findings

4.1 Risk assessment

4.1.1. Scope and execution

Risk assessment is a systematic process for identifying, analyzing and evaluating risk, as has been described in chapter 2.5 of this thesis. In addition there can be further benefits of performing a risk assessment. For example it can create awareness of hazards, known and unknowns, which can improve or add preventative actions. Also it can assist in reviewing current controls that are in place and their effectiveness. Both of these benefits surely can and will increase security and viability of companies and their operations. This increases the value of the risk assessment process even if no new hazards are identified.

This research is executed from the perspective of a company owning the supply chain referred to as the customer. With a focus aimed at a specific link of the supply chain being maritime transports of a containerized cargo to and from Iceland. As such it is important to start by defining exactly what is included in that link of the chain. Containerized means that the cargo has been put into a container and transported in it from start to end. That fact in itself highlights the importance of the containers in the process and thereof their usage pre and post the maritime transport needs to be considered. From observations of the operations of Eimskip and Samskip the scope for risk assessment is defined as the following process whereas the customers are at each end delivering the cargo at departure terminal and receiving the cargo at arrival terminal. The process consists of the following main five steps, each following the last.

1. Cargo is received at departure terminal in a container or loaded into a container
2. Container is transported to port side and loaded on board the vessel
3. Vessel departs, sails to destination port and docks
4. Container is unloaded from the vessel and transported from port side to delivery site
5. Container is delivered or unloaded and cargo delivered

The execution of both of the techniques utilized here to perform the risk assessment is done with the assistance and necessary valuable inputs from employees in the field of shipping, collectively referred to as the experts. The experts work in vessel management, terminal handling, container management and security management, with knowledge on all of the above steps in the scope. All of the experts are currently employed with the Icelandic shipping companies and have significant experience in their field to share.

4.1.2 FMEA

The process of conducting a FMEA is performed in ten separate steps, as described in chapter three, where results from each step are documented in the FMEA worksheet (see appendix 2).

Step 1: Identify components and associated functions.

In as complex transport mode as maritime transport there are countless components involved in the process. For simplicity we identify three groups of components

Containers: For dry or refrigerated cargo, either 20 feet or 40 feet in size. Their function is to contain the cargo being transported.

Vessels: Container vessel ranging from 505-1.457 TEU in size. Their function is to carry the containers over the sea from port to port.

Terminal equipment: Cranes, trucks, forklifts, etc. Their functions are to transport containers to and from vessel as well as loading and unloading containers on board the vessels.

Step 2: Identify failure modes.

Potential failure modes for the three component groups have been identified with the experts and documented into the worksheet. Number of potential failures per component groups was as follows.

Containers: Five potential failures modes.

Vessels: Seven potential failures modes.

Terminal equipment: Eleven potential failures modes.

The failure modes range from a minor events such as a collision between two containers to a major event such as grounding or a collision of a vessel to another vessel or port facilities.

Step 3: Identify effects of the failure modes.

As the perspective of the research is from the customers viewpoint the effects for each potential failures are identified on the cargo being transported owned by the customer. Consequently it can result in different failure modes having the same or similar effect on the cargo. The effects can be grouped in three main categories.

Cargo is damaged: Eight potential failure modes.

Cargo delivery is delayed: Seven potential failure modes.

Other (Cargo is lost or combination of the above): Eight potential failure modes.

Step 4: Determine severity of the failure mode.

The severity of each failure mode are estimated subjectively from know-how and experience of the experts using the severity ranking table (table 1) and documented in the worksheet. The potential failure modes receiving the highest severity ranking were the following.

Potential failure mode	Severity ranking
Grounding of vessel	9
Containers not secured correctly	8
Container holed, torn or cut in a collision	8
Mechanical breakdown of reefer container	8
Temperature settings incorrect in reefer container	8

TABLE 6: FMEA TOP SEVERITY FAILURE MODES

Step 5: Identify causes of the failure mode.

For each of the identified failure modes causes have been identified and described in the worksheet. They range from internal factors, human errors such as recklessness and lack of knowledge to external factors such as bad weather.

Step 6: Determine probability of occurrence.

Historical data of the failure modes frequency is not available. Consequently probability of the failure modes occurrence is estimated subjectively with the experts using the occurrence ranking table (table 2) and documented in the worksheet. The potential failure modes receiving the highest occurrence ranking were the following.

Potential failure mode	Occurrence ranking
Temperature settings incorrect in reefer container	4
Container holed, torn or cut in a collision	4
Vessel capacity overload	4
Bad weather conditions	4

TABLE 7: FMEA TOP OCCURRENCE FAILURE MODES

Step 7: Identify controls.

Current controls that are in place have been identified and described in the worksheet. It includes items such as training and education for operators as well as docking and maintenance of equipment.

Step 8: Determine effectiveness of current controls.

The effectiveness of the controls is estimated subjectively with the experts from their knowledge using the detectability ranking table (table 3) and documented into the worksheet. The potential failure modes receiving the highest detectability ranking were the following.

Potential failure mode	Detectability ranking
Cargo stacked incorrectly	7
Temperature settings incorrect in reefer container	7
Container holed, torn or cut in a collision	6

TABLE 8: FMEA TOP DETECTABILITY RANKING

Step 9: Calculate risk priority number.

The risk priority number is calculated by multiplying the severity ranking, the occurrence ranking and the detectability ranking and results documented in the worksheet.

Step 10: Determine actions to reduce risk of failure mode.

Actions have been analyzed and suggested where applicable for the key risk factors. No identified failures required immediate action but were scheduled with later targeted completion dates without fixing the date. Many failure modes did not receive any suggested actions but should be scheduled to be reviewed again at a later date and regularly from thereon.

4.1.3 FTA

The process of conducting a FTA is performed in five separate steps as described in chapter three. How each step was performed is described in this chapter.

Step 1: Define the undesired event to study

In the process of defining the undesired top event it is necessary to review the problem description in chapter one and specifically the research questions. Questions number 1 asks:

> What are the key risk factors in Iceland that can interrupt or break the supply chain, focusing on maritime transport?

Considering the guideline to define the undesired top event not too broadly and also both what the event is and when it happens, the following definition is proposed.

> The supply chain disrupts during the maritime transport

Step 2: Obtain an understanding of the system

The system, in this research the five steps of maritime transport and related operations, as described in chapter 4.1.1 is reviewed and observed thoroughly and systematically. In addition the experts add to the research their experience and knowledge of the system. Possible events leading to the previously defined undesired top event are discussed and identified as well as

their effects on each other, what underlying events exists and so on until root causes are identified. There are eight intermediate events defined directly below the top undesired event as follows.

Top level intermediate event
Vandalism
Service reliability
Oil crisis
Natural disasters
Equipment failure
Labor crisis
Authorities
Economic crisis

TABLE 9: FTA TOP LEVEL INTERMEDIATE EVENTS

Step 3: Construct the fault tree

With the undesired top event defined along with all identified events leading to it and all root causes there below, the fault tree is constructed from the building block as described in appendix 1 using Microsoft Excel.

Step 4: Evaluate the fault tree

After the fault tree has been constructed it is reviewed and scanned for possible improvements, additions or eliminations. Finally once final structure has been agreed upon it is attempted to assign probability values to the root causes. As there exist very limited historical data on frequency of theses root causes actualizing the probabilities are assigned subjectively. Once completed the probabilities are calculated upwards the tree over the logic gates which provides ranking of the main events leading to the undesired top event actualizing.

Step 5: Control the hazards identified

The analysis and calculations performed in step 4 provide an identification of the key risk factors. Reviewing those factors proposed actions to control the risk are presented in following chapters.

4.2 Key risk factors

Identifying the key risk factors relates to responding to research question 1 introduced in chapter one of this research. The first two steps in the risk assessment process, the identification and analysis provide us with the key risk factors. The results from the two techniques provided mostly separate key risk factors as was expected considering the different approaches.

4.2.1 FMEA

Performing steps 1-9 in the FMEA analysis provides the risk identification and analysis. There are twenty three potential failure modes identified. Out of those there are five that stand out having considerably higher risk priority numbers and are consequently considered key risk factors. Those risk factors are listed as follows from the highest RPN to the lowest;

1. Container is holed, torn or cut in a collision during the transit and loading of it onto the vessel due to recklessness of operators handling the container.

   Severity is high as it can result in that seawater gets into the container and damage the cargo if it cannot withstand water.

   Occurrence is occasional and size of fractures varies.

   Detectability is relatively moderate as for example often there have been placed immediately another containers on top of the damaged one which conceal the fracture.

2. Temperature settings on a reefer container are incorrectly set due to incorrect instructions from the customer.

   Severity is high in this case. As this can result in two scenarios, either a frozen product will thaw because the temperature was set to high and therefore it will most likely be fully damaged or a fresh product gets frozen because the temperature was set to low and then it will most likely be less valuable.

   Occurrence is infrequent.

Detectability in this case is occasional as internal processes at the transport company designed to catch this do not reach outside the company. It is only detected if employees checking the temperature second guess the instructions and contact the customer.

3. Sailing between ports in unexpectedly worse weather than was forecasted.

   Severity is relatively high as this usually result in delay of the vessel and consequently delivery of the cargo but it can also result in damage of the cargo due to roll of the vessel and in infrequent worst case scenario loosing container off board.

   Occurrence is occasional considering the whole year but there is seasonality as frequency increase during the winter months.

   Detectability is moderate and depends on accuracy of weather forecasts.

4. Cargo is stacked incorrectly into the container due to incorrect instructions from the customer.

   Severity has moderate effects as cargo is most likely only damaged if there is rough sea during the sailing leading to that the cargo shifts or rolls inside the container, consequently getting damaged.

   Occurrence is infrequent.

   Detectability in this case is occasional as internal processes at the transport company designed to catch this do not reach outside the company.

5. Temperature settings on a reefer container are incorrectly set due to recklessness of employees handling the container.

   Severity results in same effects as for item nr. 2.

   Occurrence is occasional.

   Detectability is considered high as internal controls are in place.

4.2.2 FTA

Performing steps 1-4 in the FTA provides the risk identifications and analysis. There are eight intermediate events defined as events leading to the top undesired event including below it

further more six intermediate events rooting from total of twenty-three causes. Of those eight there are four that have significant higher probabilities and can be considered as key risk factors. Those events are listed below, including root causes and effects, in order starting from the event estimated to have the highest probabilities.

1. Economic crisis, rooting from currency or credit crisis.

   Extreme unexpected currency devaluation or restrictive capital controls can lead to the currency crisis.

   Insolvency of the transport company or a liquidity shortage can lead to the credit crisis.

   Both in fact have the same effects that the transport company will be unable to make payments to its vendors such as oil and port services and consequently be unable to provide service.

2. Natural disasters, rooting from extreme weathers, volcanic eruptive or earthquakes.

   Floating icebergs or storms can lead to extreme weather conditions.

   All these events have the effects that sailing schedules may be delayed or cancelled and if weather is unexpectedly worse than forecasted it can damage the cargo on board because of vessel roll or even lead to containers falling of board, leading to total loss of cargo.

3. Vandalism.

   Security breach into suppliers IT system or terminal area can open up for extremist group vandalisms.

   The effects can be delay in operations while damages are being fixed.

4. Equipment failures.

   Lack of renewal, bad treatment or low maintenance can lead to equipment failures.

   This can have the effects that the transport company is unable to provide service as replacement equipment or spare parts are unavailable, this specifically refers to large specialized equipment where there are few items in use, such as vessels and port side cranes.

5. Discussions

The study of risk in the supply chain has for the last decades been gradually receiving more attention within the academic environment as number of published researches in the area has increased. Same growth in attention can be seen within corporations relying on secure supply chains although seemingly still behind the academic environment as was demonstrated in the literature review chapter of this thesis. This increase follows in line with corporation's global expansion to new markets last decades and its continuous search for new and cheaper manufacturing sites. The downside to this expansion is among other added complexity and increased risk that can quickly erase the benefits received from more sales or cheaper manufacturing costs. Consequently it is important for corporations to catch up more quickly on academic researches and put more efforts into testing and developing better methods to identify and analyze risk in the supply chain. This task can be very complicated and extensive specifically considering the added complexity of supply chains in today's environment. It is fair to say that corporations face a challenge to develop the right method that gives the most valuable information.

This thesis attempts to attack this challenge for a specific link in the supply chain being maritime transport to and from Iceland. It was done by proposing two research questions as described in chapter one with the focus and main attention to the first one on identifying key risk factors. A literature review was performed, starting from the definition of risk in general and narrowed down to risk in supply chains and specifically maritime transport, in additions ISO standards on risk management and risk assessment were studied. Following the literature review two separate techniques called FMEA and FTA were selected from range of techniques suggested by the standards. Description of those techniques, reasoning for their selection and how the techniques are performed in general is described in chapter three.

The research is performed from the perspective of the owner of the supply chain utilizing a service provider for maritime transport. It is limited to containerized cargo and the scope of the chain is defined between departure and arrival terminals. The two selected techniques are

performed with the assistance of experts in maritime transport and the processes are described in detailed steps in chapter four along with its results.

The process of performing the FMEA technique was relatively quick and easy. The knowledge and assistance of the experts was extremely valuable and relevant, they quickly understood the method and were fast and much alike in their approach and inputs. There were little difficulties in identifying the items, the processes and potential failure modes and effects. The complications were to assign the rankings of severity, occurrence and detectability. The main complications with assigning severity ranking were twofold. Firstly that different type of cargo is differently vulnerable to collisions or other external effects. For example if a container is holed leading to seawater flooding in, it can have severe effects on food cargo but none on equipment such as cars. Secondly that customers with high and frequent volume of shipments are less effected of single failure mode than customers with few or single shipments. This was resolved by always considering the cargo being delicate and owned by low volume customer. The main complication with assigning occurrence and detection ratings was the lack of historical data. Consequently it had to be estimated subjectively from experience of the experts and their best guesstimates.

The process of performing the FTA was naturally different from the FMEA, not necessary more difficult but challenging in other thinking process. It required few brainstorming sessions and discussions about possible external events that could lead to the defined undesired top event actualizing. Once the thinking process was adjusted the first steps of defining the top event, understanding the system and identifying intermediate events were relatively quickly completed as was constructing the tree. The main complication came up around assigning probability values to the root causes. As with the FMEA process a lack of historical data was challenging and even more in this case as it was dealing with events that in some instances are extremely rare. Also challenging to consider was that some of the identified root causes are very relevant today as labor crisis and volcanic eruptive but perhaps not in a normal year. Consequently the probabilities were estimated subjectively for what was considered average normal year.

The two techniques provided different results as was expected from the different approaches that are taken. From the results of each technique there are selected those that have significantly higher priority numbers or probabilities. That is not undermining the importance of other identified risk factors, but simply carving out those that should receive attention first. Below table shows the key risk factors identified by both techniques classified according to Christopher and Peck's risk categories.

Risk category	Key risk factor	Research technique
Process	Container is holed, torn or cut in a collision during the transit and loading of it onto the vessel due to recklessness of operators handling the container.	FMEA
	Temperature settings on a reefer container are incorrectly set due to recklessness of employees handling the container	FMEA
Control	Equipment failures, due to lack of renewal, bad treatment or low maintenance	FTA
Supply	Temperature settings on a reefer container are incorrectly set due to incorrect instructions from the customer	FMEA
	Cargo is stacked incorrectly into the container due to incorrect instructions from the customer	FMEA
Environmental	Sailing between ports in unexpectedly worse weather than was forecasted	FMEA
	Economic crisis, rooting from currency or credit crisis	FTA
	Natural disasters, rooting from extreme weathers, volcanic eruptive or earthquakes	FTA
	Vandalism, security breach into suppliers IT system or terminal area can open up for extremist group vandalisms	FTA

TABLE 10: KEY RISK FACTORS PER RISK CATEGORY

As can be seen in the above table the three of the four of the FTA key risk factors are classified as environmental risk and one as control risk, which is in line with the top-down approach. The five FMEA key risk factors are classified as process, supply and environmental risk. In addition there were identified several risk factors with lower RPN, such as mechanical breakdowns, that would be classified as control risk. This results in risk factors identified with the FMEA technique are touching wider scope of risk categories while the FTA technique is very much focused on the environmental category. That does not highlight importance or relevance of FMEA above FTA

but simply demonstrates the difference in the approaches and also importantly it shows the wider spectrum of identified risk factors the methods provide combined.

This research demonstrates that both FMEA and FTA are relevant and feasible when performing a risk assessment on the supply chain. The two techniques surely do supplement each other by providing wider and more thorough risk assessment by identification of separate risk factors. The results gained from this risk assessment provide valuable insight and understanding of the maritime transport link in the supply chain and what risk factors can possibly interrupt the chain.

Finally to mention is that this thesis demonstrates step by step the process of how both the techniques were performed which can be reused and adjusted if needed to specific requirements of a company utilizing maritime transport to and from Iceland as part of their supply chain. Consequently act as starting point of their own risk assessment and possibly be compared to other techniques.

6. Conclusion

The objective of this research was to perform a risk assessment and answer two research questions that were defined in chapter one, with the main weight and attention to the first question;

1. What are the key risk factors in Iceland that can interrupt or break the supply chain, focusing on maritime transport?

Of all the identified risk factors there were nine that were identified as key risk factors. Five identified with the FMEA technique and four with the FTA technique. These risk factors are summarized in the below tables and ranked according to their RPN or probability values from the highest to the lowest.

#	Key risk factor
1	Container is holed, torn or cut in a collision during the transit and loading of it onto the vessel due to recklessness of operators handling the container.
2	Temperature settings on a reefer container are incorrectly set due to incorrect instructions from the customer
3	Sailing between ports in unexpectedly worse weather than was forecasted
4	Cargo is stacked incorrectly into the container due to incorrect instructions from the customer
5	Temperature settings on a reefer container are incorrectly set due to recklessness of employees handling the container

TABLE 11:FMEA KEY RISK FACTORS

#	Key risk factor
1	Economic crisis, rooting from currency or credit crisis
2	Natural disasters, rooting from extreme weathers, volcanic eruptive or earthquakes
3	Vandalism, security breach into suppliers IT system or terminal area can open up for extremist group vandalisms
4	Equipment failures, due to lack of renewal, bad treatment or low maintenance

TABLE 12: FTA KEY RISK FACTORS

The other research question was considered secondary and it was not the intention to investigate current risk mitigation strategies in place at any company and their effectiveness but rather to generally understand what options are available and their applicability.

2. How can these risk factors be mitigated to avoid business interruptions?

To answer this question in an acceptable manner an extension of this research is required as deciding and implementing risk mitigation strategies is very much subjected to each customer and needs to be considered with current setup and processes already in place. Still, the final steps of both the techniques are intended to perform the last step of the risk assessment as defined by the ISO/EIC 31010:2009 standard. That is to evaluate the identified risk factors and make decisions on future actions. Therefor when performing both the techniques the following suggestions were made in the final steps which are summarized in the below table.

Key risk factor	Research technique	Suggested actions
Container is holed, torn or cut in a collision during the transit and loading of it onto the vessel due to recklessness of operators handling the container.	FMEA	Request enhanced review of container situation before vessel departure
Temperature settings on a reefer container are incorrectly set due to incorrect instructions from the customer	FMEA	Review and improve information flow to shipping company
Sailing between ports in unexpectedly worse weather than was forecasted	FMEA	Request enhanced fixtures on containers and more manning during bad weather months
Cargo is stacked incorrectly into the container due to incorrect instructions from the customer	FMEA	Review and improve information flow to shipping company
Temperature settings on a reefer container are incorrectly set due to recklessness of employees handling the container	FMEA	Request review and test of effectiveness of control process
Economic crisis, rooting from currency or credit crisis	FTA	Request information on financial standings of the shipping company
Natural disasters, rooting from extreme weathers, volcanic eruptive or earthquakes	FTA	Request information and review on extreme situation controls
Vandalism, security breach into suppliers IT system or terminal area can open up for extremist group vandalisms	FTA	Request review of security controls and enhancements if necessary
Equipment failures, due to lack of renewal, bad treatment or low maintenance	FTA	Request review of maintenance schedules and equipment status

TABLE 13: SUGGESTED RISK MITIGATION ACTIONS

Concluding from this it would be interesting to perform further analysis on the risk mitigation suggestions and evaluate their effectiveness, to do so an actual case study might be suitable. For further research it would also be interesting to perform this risk assessment with other techniques and compare their results to the ones received in this research. In addition it would be interesting to expand this research for larger scope of the supply chain and include for example distribution and trucking on land.

References

Adams, J. (1995). *Risk.* London: UCL press.

Carlson, C. (2012). *Effective FMEAs: Achieving Safe, Reliable, and Economical Products and Processes using Failure Mode and Effects Analysis.* New Jersey: Wiley.

Chopra, S., & Sodhi, M. (2004). "Managing Risk to Avoid Supply Chain Breakdown. *MIT Sloan Management Review, 46*(1).

Christopher, M., & Peck, H. (2004). Building the resilient supply chain. *Int. Journal of Logistics Management, 15*(2), 1-13.

Curkovic, S., Scannell, T., & Wagner, B. (2013). Using FMEA for Supply Chain Risk Management. *Modern Management Science & Engineering, 1*, 251-265.

Damodaran, A. (2008). *Strategic Risk Taking: A Framework for Risk Management.* New Jersey: Wharton School Publishing.

Dittmann, J. P. (2014). *Managing risk in the global supply chain.* Knoxville: University of Tennessee.

(2014). *Don't Play it Safe When it Comes to Supply Chain Risk Management.* Dublin: Accenture.

Eckberg, C. R. (1964). *Fault Tree Analysis Program plan.* Seattle: Boeing Aerospace Company.

Hixenbaugh, A. F. (1968). *Fault Tree for Safety.* Seattle: Boeing Aerospace Company.

ISO/IEC31010. (2009). Geneva: International Organization for Standardization.

ISO31000. (2009). Geneva: International Organization for Standardization.

Jüttner, U., Peck, H., & Christopher, M. (2003). Supply Chain Risk Management. *Int. Journal of Logistics: Research & Applications, 6*(4), 197-210.

Kahneman, D., & Tversky, A. (1982). Variants of Uncertainty. *Cognition*, 143-157.

Kaplan, S., & Garrick, B. J. (1981). On The Quantitative Definition of Risk. *Risk Analysis*, 11-27.

Khaiyum, S., & Kumaraswamy, Y. S. (2014). Integration Of FMEA And FTA For Effective Failure Management In Real Time Embedded Projects. *Integrated Journal of British, 1*(3), 12-25.

Larsen, W. F. (1974). *Fault Tree Analysis.* Dover: U. S. Army Picatinny Arsenal.

Manner-Bell, J. (2014). *Supply Chain Risk: Understanding Emerging Threats to Global Supply Chains.* London: Kogan Page Limited.

OED. (1997). Oxford: Oxford University Press.

PMBOK. (2013). Newtown Square, Pennsylvania: Project Management Institution, Inc.

(1980). *Procedures for performing a Failure Mode, Effects and Criticality Analysis.* Washington: Department of Defense.

Psaraftis, H., Panagakos, G., Desypris, N., & Ventikos, N. (1998). An analysis of maritime transportation risk factors. *International Society of Offshore and Polar Engineers* (pp. 477-482). Cupertino: ISOPE.

Singhal, P., Agarwal, G., & Mittal, M. (2011). Supply chain risk management: review, classification and future research directions. *Int. Journal of Business Science and Applied Management, 6*(3), 15-42.

Stamatis, D. H. (2003). *Failure Mode and Effect Analysis: FMEA from Theory to Execution.* Milwaukee: ASQ quality Press.

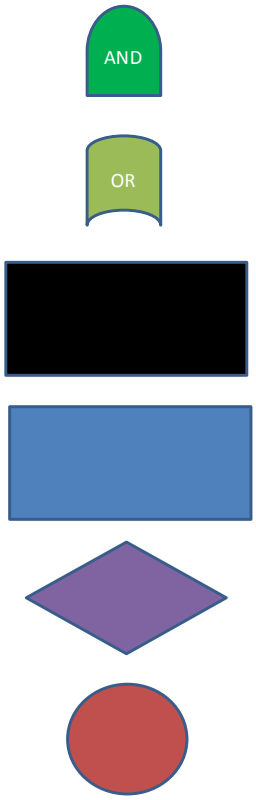
UNCTAD. (2006). *Maritime Security: Elements of an analytical framework for compliance measurement and risk assessment.* Geneva: UNCTAD.

UNCTAD. (2014). *Review of Maritime Transport.* Geneva: UNCTAD.

Zsidisin, G. A. (2003). A grounded definition of supply risk. *Journal of Purchasing & Supply Management, 9*, 217-224.

Appendices

Appendix 1 – FTA Graphic Symbols



AND gate - The above output occurs only if all below inputs occur

OR gate - The above output occurs if any below input occurs

Undesired top event

Intermediate event - The resulting event of different interacting events

Undeveloped event - Not further developed, insufficient information or insignificant

Root cause - Primary cause, not further developed

Appendix 2 – FMEA worksheet

Rating Before Action										Action Plan				Revised Rating			
Item identification	Function/Process	Potential failure mode	Potential effects of failure	Severity Rating (S)	Potential causes of failure	Occurence rating (O)	Current process controls	Detection rating (D)	Risk priority number (RPN=S*O*D)	Recommended actions	Responsibility and target date	Actions taken	Implementation closure date	S	O	D	RPN
What are the items in relevance	What is the process	What can go wrong ?	What is the impact if failure mode happens	A rating corresponding to the seriousness of an effect of a potential failure mode. (scale: 1-10. see ranking table)	What causes the failure mode to happen?	A rating corresponding to the rate a failure mode can occur, before any additional process controls are applied. (scale: 1-10. see ranking table)	What are the existing controls or procedures to detect and prevent failure modes	A rating corresponding to the likelihood that current controls will detect the potential failure mode before it happens. (scale: 1-10. see ranking table)	For a given potential failure mode, how bad the outcome is multiplied by how likely it would actually happen multiplied by what things are in place today to prevent or notice it before it happens	What actions can be taken to reduce occurence or improve detection	Who is responsible for the actions taken and when shall it be completed	What actions are taken?	When have actions been implemented fully?	Severity rating revised	Occurence rating revised	Detectoin rating revised	RPN number revised
Container	Load cargo into container	Loading performed badly	Cargo is damaged	3	Lack of experience	3	Training and education to employees working on loading	3	27								
		Tempterature settings incorrect	Cargo is damaged or destroyed	8	Incorrect instructions from customer	3	Review of customer instructions	7	168	Review and improve information flow to shipping company	Target date not fixed						
					Recklessness	4	Training and education to employees on container controls	3	96	Request review and test of effectiveness of control process							
		Cargo stacked incorrectly	Cargo is damaged in rough sea	6	Incorrect instructions from customer	3	Review of customer instructions	7	126	Review and improve information flow to shipping company	Target date not fixed						
					Lack of knowledge	3	Training and education to employees working on loading the containers	3	54								
	Maintain refrigeration	Mechanical breakdown	Cargo is damaged or destroyed	8	Lack of maintenance	2	Containers inspected regularly	4	64								
	Unload cargo from container	Unloading performed badly	Cargo is damaged	3	Lack of experience	3	Training and education to employees working on unloading	3	27								
Terminal handling / Crane & equipment	Transfer container to portside	Collision with other containers or equipment	Cargo is damaged	3	Recklessness during tranfer of the container	2	Training of employee operating the machinery transferring the container	3	18								
		Container overturned	Cargo is damaged	5	Recklessness during tranfer of the container	2	Training of employee operating the machinery transferring the container	3	30								
	Load container on board the vessel	Collision with other containers or vessel	Cargo is damaged	3	Lack of experience of crane operator	2	Training of employee operating the crane loading the vessel	5	30								
		Container holed, torn or cut in a collision	Cargo is damaged with seawater	8	Recklessness of crane operator	4	Training of employee operating the crane loading the vessel	6	192	Request enhanced review of container situation before vesseldeparture	Target date not fixed						
		Vessel balance incorrect	Cargo is damaged or lost in rough sea	8	Incorrect instructions or recklessness	2	Review of instructions	4	64								
		Preparation of ship manifest	Cargo delivery is delayed	3	Incorrect information	2	Review of informations	2	12								
		Vessel capacity overload	Cargo delivery is delayed	4	Excessive demand for transport	4	Cargo re-routed with other vessels	3	48								
	Unload container from the vessel	Collision with other containers or vessel	Cargo is damaged	3	Lack of experience or neglence of crane operator	2	Training of employee operating the crane unloading the vessel	5	30								
	Transfer container to delivery spot	Collision with other containers or equipment	Cargo is damaged	3	Recklessness during tranfer of the container	2	Training of employee operating the machinery transferring the container	3	18								
		Container overturned	Cargo is damaged	5	Recklessness during tranfer of the container	2	Training of employee operating the machinery transferring the container	3	30								
		Communication with customs authorities	Cargo delivery is delayed	3	Incorrect information from customer	3	Review of informations from customers	4	36								
Vessel	Preparation of containers for sea	Containers ar not secured correctly	Cargo is damaged or lost in rough sea	8	Recklessness of seaman	2	Training of employee operating on the vessel	2	32								
	Depart from port	Collision with another vessel or port facilities	Cargo delivery is delayed	3	Recklessness of vessel operator	2	Training of employee operating the vessel	2	12								
	Sailing with pilot to and from deap waters	Grounding of vessel	Cargo is delayed or damaged	9	Recklessness of vessel operator	2	Training of employee operating the vessel	2	36								
		Pilot unavailable	Cargo delivery is delayed	3	Harbour inefficiency	2	Planning with harbour authorities	2	12								
	Sailing in deap waters between ports	Mechanical breakdown	Cargo delivery is delayed	7	Lack of maintenance or age of vessel	2	Regular docking of vessel	3	42								
		Bad weather conditions	Cargo is delayed or damaged	7	Weather conditions are worse than predicted	4	Review of weather predictions	5	140	Request enhanced fixtures on containers and more manning during bad weather months	Target date not fixed						
	Docking at port	Collision with another vessel or port facilities	Cargo delivery is delayed	3	Recklessness of vessel operator	2	Training of employee operating the vessel	2	12								

Appendix 3 – FTA model