Master's thesis

2019

Christoffer Vikebø Nesse

Master's thesis

NTNU
Norwegian University of
Science and Technology
Faculty of Engineering
Department of Mechanical and Industrial Engineering

NTNU
Norwegian University of
Science and Technology

Christoffer Vikebø Nesse

Ice Management with System Theoretic Process Analysis (STPA) for Marine Operations in Arctic Environments

June 2019

NTNU
Norwegian University of
Science and Technology

NTNU
Norwegian University of
Science and Technology

Ice Management with System Theoretic Process Analysis (STPA) for Marine Operations in Arctic Environments

Christoffer Vikebø Nesse

Mechanical Engineering
Submission date: June 2019
Supervisor: Yiliu Liu
Co-supervisor: HyungJu Kim

Norwegian University of Science and Technology
Department of Mechanical and Industrial Engineering

Preface

Ice Management with System Theoretic Process Analysis (STPA) for Marine Operations in Arctic Environments is a master thesis in the RAMS group at NTNU as part of the study program Mechanical Engineering. It was carried out the spring semester of 2019.

The project was done in parallel with research projects under the High North Programme. In December 2019 I was granted the opportunity to have a brief visit to the Korea Maritime and Ocean University (KMOU) and the Korean Research Institute of Ship and Ocean (KRISO), and to participate at the seventh Arctic Partnership Week which was held in Busan, South Korea.

This Master thesis is built on my specialisation project that presented a literature study and an overview of ice management, traditional hazard analysis methods, STAMP and STPA. In the master thesis, I have continued this literature study and further investigated if and how STPA should be applied to ice management.

It is assumed that readers have extensive knowledge about reliability engineering and fundamental knowledge about systems engineering. However, brief explanations are provided for most concepts to assist those who might have an interest in this topic but are only familiar with ice management. It is also assumed that most readers have limited knowledge of ice management.

Trondheim, 2019-06-11

Christoffer V. Nesse

Christoffer Vikebø Nesse

Acknowledgement

Firstly I would like to thank my supervisors Professor Yiliu Liu and Associate Professor HyungJu Kim, for their invaluable and constructive feedback and advice throughout my final year at NTNU. I feel lucky to have had both of you as my supervisors. It has been a true joy. When I have struggled, you have always kindly helped me, shared your knowledge and motivated me to find the best path forward. Thank you for the cooperation so far – I hope that we will work together on exciting projects in the future.

Secondly, I would like to thank friends and family for continuous support and motivation. I would also like to thank Tekna, the Student Democracy at NTNU, other organisations I have been affiliated with and Singsaker Studenterhjem for enriching my years in Trondheim and at NTNU. Lastly, I would like to thank Framo AS for economic support throughout my studies, which have enabled me to spend more time doing the things I love.

C.V.N.

Executive Summary

For the past century, the Arctic has been attracting brave researchers and adventurers, but inaccessible for most. Advancements in technology and changes in the climate are rapidly changing this, making the Arctic region more accessible. For the industry, this change is desirable. Usage of the Northern Sea Route through the Arctic, which is a shortcut, is of great interest to everyone somehow involved in or benefiting from global trade. Also, approximately a sixth of the world's undiscovered hydrocarbons and other minerals may be found north of the Arctic Circle, resources that might need to be extracted over time to meet future energy demands.

Marine operations in harsh Arctic environments must handle severe weather and ice conditions. Ice management is all measures that can be made to reduce risk from any ice feature and is necessary to ensure safe marine operations. In this master thesis, I have scratched the surface of the state of the art research relevant to ice management and found that many challenges remain to be solved. Efficient ice management operations depend on reliable monitoring and surveillance of ice features, which in itself is difficult to accomplish. Large amounts of data are gathered and translated into decision, and navigational support for the crew's on vessels in transit through the Arctic, or on icebreakers protecting different floating structures from ice conditions. Computational and numerical simulation tools are used to evaluate identified threats and hazardous situations. Most of these are not publicly accessible, or commercially available (yet), and are also subject to improvement. These simulation tools may likely be a source of new flaws.

In this master thesis, I have identified some general challenges concerning ice management, and some of these are of importance when it comes to identifying hazards, and to determine how these should be avoided or mitigated. Complex component, system and human interactions might lead to unidentified hazardous scenarios. Traditional hazard identification methods were not developed for the intent of analysing modern complex sociotechnical systems, which ice management systems are, and several limitations are identified. A rather novel approach to hazard identification, system-theoretic process analysis (STPA) has been developed to efficiently identify flaws that modern systems introduces, are presented in this master thesis. A case study on ice management have been conducted using the STPA method, and it is compared to a case study using FMECA. In this master thesis, I have evaluated whether or not STPA should be applied to ice management, if it should be used in combination with other methods, or if it is not suited whatsoever.

Samandrag

Det siste hundreåret har Arktis vore forlokkande for modige forskarar og eventyrarar, men utilgjengeleg for dei fleste. Klimaendringar og framsteg i teknologi endrar dette raskt, noko som gjer den arktiske regionen meir tilgjengeleg. For industri opnar denne endringa opp for nye moglegheiter. Bruk av Nordvestpassasjen gjennom Arktis, som i utgangspunktet er ein snarveg, er av stor interesse for alle som på eitt eller anna vis er involvert i, eller dreg nytte av, global handel. Om lag ein sjettedel av verdas uoppdaga hydrokarbon samt andre mineral er òg å finne nord for Polarsirkelen, ressursar som truleg må utvinnast over tid for å møte framtidige energibehov.

Marine operasjonar i Arktis må handtere både tøffe vêrforhold og isforhold som sjøis og isfjell. Isstyring (ice management) er alle tiltak ein kan gjere for å redusere risiko ved isforhold, og er nødvendig for å sikre trygge marine operasjonar. I denne masteroppgåva har eg gått gjennom toppmoderne forsking som er relevant for isstyring, og funne ut at det er fleire utfordringar som framleis må løysast. Effektiv isstyring er avhengig av påliteleg overvaking av is, noko som i seg sjølv er vanskeleg å få til. Store mengder data vert samla og omsett til avgjerd- og navigasjonsstøtte for mannskap på fartøy i transitt gjennom Arktis, eller på isbrytarar som vernar ulike flytande konstruksjonar frå isforhold. Berekningsverktøy og numeriske simuleringsverktøy vert nytta til å evaluere og identifisere truslar og farlege hendingar. Dei fleste av desse er ikkje offentleg eller kommersielt tilgjengelege (endå), og blir stadig forbetra. Det er sannsynleg at desse simuleringsverktøya kan vere kjelde til nye typar feil.

I denne masteroppgåva har eg identifisert nokre generelle utfordringar med isstyring. Nokre av desse er viktige når det gjeld å identifisere farar og for å bestemme korleis ein kan unngå eller redusere desse. Komplekse interaksjonar mellom komponentar, system og menneske kan føre til uidentifiserte farlege scenario. Tradisjonelle fareidentifikasjonsmetodar vart ikkje utvikla for å analysere moderne komplekse sosiotekniske system, slik som isstyringssystem, og fleire avgrensingar er identifiserte. Ei relativt ny tilnærming til fareidentifikasjon, systemteoretisk prosessanalyse (STPA) som er utvikla for å effektivt identifisere feil som moderne system introduserer, er lagt fram i denne masteroppgåva. Ein eksempelstudie om isstyring har blitt utført ved hjelp av STPA-metoden, og det er samanlikna med ein eksempelstudie med FMECA. I denne masteroppgåva har eg vurdert til kva grad STPA skal nyttast til isstyring, om metoden skal nyttast i kombinasjon med andre meir tradisjonelle metodar, eller om den ikkje skal nyttast i det heile.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Background and Motivation

For the past century, the Arctic has been alluring for pioneers, researchers, and adventurers. An exotic haven for the few, that now is in the interest of the many. The Arctic is a laboratory for the effects climate change has on the earth and continues to be an essential area for many fields of research. Resources in the Arctic are far from scarce and are becoming easier accessible as technology and knowledge advances, and ice levels decrease. An assessment of the U.S. Geological Survey proposes that about 30 % of the world's undiscovered gas and 13 % of the world's undiscovered oil may be found north of the Arctic Circle (Gautier et al., 2009). This region offers enormous values that have been, and still are, difficult to harvest safely and effectively. Marine operations are necessary to conduct research expeditions, and arguably to keep up with future energy demands.

As Earth's climate is changing, it is shown by Lindsay and Schweiger (2015) that annual mean ice thickness in the Arctic has decreased by almost two thirds from 1975 to 2012. Figure 1.1 shows a trend that not only is the sea ice getting thinner, it is also shrinking in extent. Figure 1.2 shows the reduction of the maximum sea ice extent in the winter months. According to Desch et al. (2017), the late-summer Arctic will likely be ice-free as soon as the 2030s. This makes new shipping routes through the Arctic more readily available, which are of great interest to shipping companies. However, marine operations in the Arctic, especially yearlong operations, will remain challenging. Permafrost onshore, severe ice conditions offshore, isolation, lack of infrastructure and winters with continuous darkness sets the tone. Challenges of marine operations in harsh Arctic environments are linked to the risks of operating there. Marine structures require special design to withstand the extra loads the environment provides, and often rely on ice management support. Monitoring and surveillance of ice and weather conditions are not trivial, interpretation and translation of data sets to useful threat identification and evaluation to support physical ice management operations are difficult. Increased Arctic exploitation is

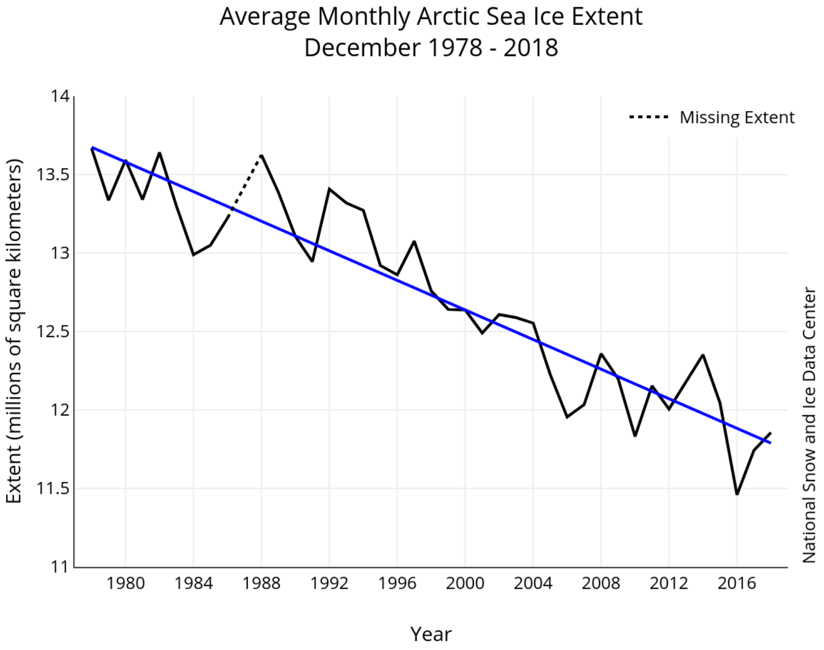


Figure 1.1: Arctic sea ice extent, monthly average from 1980 to 2018. Credit: National Snow and Ice Data Center.

dependent on advancements in ice management. Efforts are being made to enable this, and advancement in technology generally leads to more complex systems. Traditional hazard identification methods might not be sufficient, and new approaches may be necessary to ensure safety in the ice management systems of the future.

STAMP (Systems-Theoretic Accident Model and Processes), as well as *Systems Theory,* and the *Hierarchical Sociotechnical Framework* (Rasmussen, 1997) which STAMP is built on, is best described in the book *Engineering a Safer World: Systems Thinking Applied to Safety* by Leveson (2012). STAMP has many applications, one of which is STPA (System-theoretic process analysis), are introduced in this book. STPA has recently been revised, and the *STPA Handbook* by Leveson and Thomas (2018) describes this method, why it is necessary, and how it may be used efficiently. Risk assessment books such as Rausand and Høyland (2004), Rausand (2011) and Rausand (2014) have also been used to make comparisons to more traditional hazard analysis methods because I have grown familiar them throughout my studies. STPA is a rather novel approach. However, several case studies are available with a wide range of applications in different sectors and domains, generally concerning safety. STPA has been proven effective in terms of hazard identification in modern complex sociotechnical systems, which most interesting developments today may be said to be. This literature has been used to describe the STPA process.

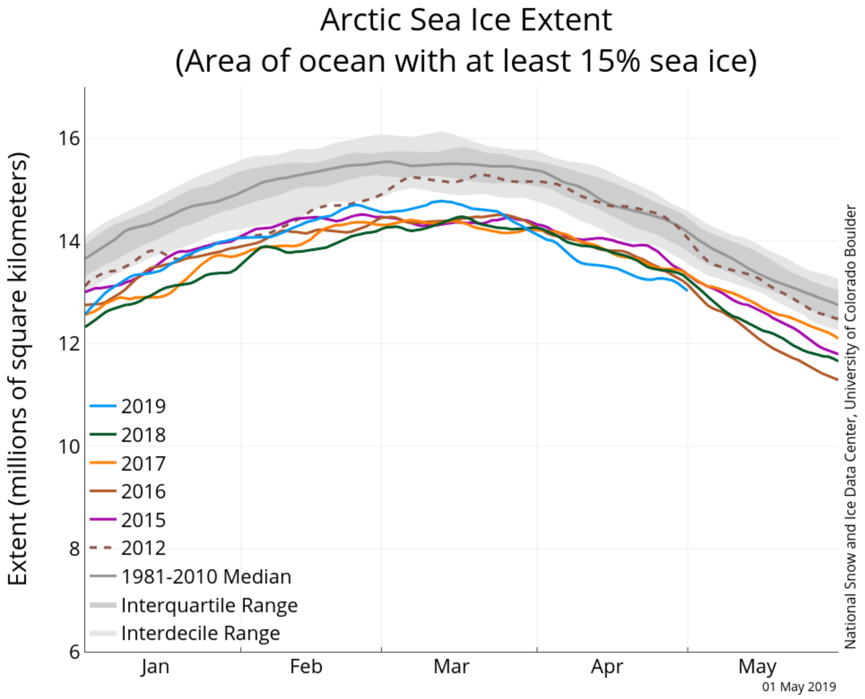


Figure 1.2: Arctic sea ice extent as of May 2019. Credit: National Snow and Ice Data Center.

Literature shows an augmenting interest in marine operations in harsh Arctic environments, and many projects are funded to enable this development. In this master thesis, I have continued to understand more of the work being done concerning ice management through a literature study, a process I started in my specialisation project (Nesse, 2019). The scope of this master thesis, or perhaps even a PhD thesis, is too small to completely describe all the state of the art research being done with respect to ice management. I have scratched the surface of ice management of marine operations in harsh Arctic environments. Fundamental knowledge on STPA is well established, but the focus of those familiar with the method has not been on ice management. In this master thesis, I have become familiar enough with ice management and STPA to apply it to case studies. This work has helped me to learn enough to give some advice on whether or not STPA should be applied to ice management, and provide some suggestions for further work.

1.2 Problem Description

The marine operations in the harsh/arctic environments will meet manage challenges from uncertainties and unknown challenges. Many accidents are due to interdependencies and interactions between the different elements in a complex system. Traditional reliability and risk analysis approaches, such as FMECA and FTA, are not effective any more. Researchers are turning to a new safety analysis and hazard identification approach - System Theoretic Process Analysis (STPA), where accidents are regarded as control problems, and preventing accidents is done by enforcing constraints on component behaviours and interactions.

STPA has yet not been applied to ice management, and the student will employ STPA for ice management for a marine operation in harsh Arctic environments, and determine whether or not STPA should be applied to ice management.

1.3 Objectives

The main objectives of this master thesis are to:

1. Establish fundamental knowledge of ice management and STPA.

2. Conduct a case study related to ice management of icebergs using FMECA and using STPA. Compare the two case studies and identify the advantages and limitations of the two methods.

3. Evaluate whether or not STPA should be applied to ice management, if it should be used in combination with other methods, or if it is not suited whatsoever.

1.4 Approach

The objective of this master thesis has been to establish fundamental knowledge on ice management and STPA, to use this knowledge conducting a case study, and to enable me to evaluate to what extent STPA should be used for ice management. STPA is a well-established method, and it has been easy to find literature to describe the STPA process. To learn more about the limitations and advantages of STPA, I compared the STPA case study with a case study using a more traditional hazard analysis method (FMECA).

Studying ice management, I found that approaches such as Bayesian belief network are being used in combination with traditional hazard analysis methods. I also decided to describe some of these applications in my specialisation project, as they could be interesting to use in combination of STPA. Based on this work, and the case studies in this master thesis, I have been able to evaluate whether or not STPA could be more suited for ice management applications in combination with other methods.

Ice management is not as well established as STPA, and this was the most intense part of my literature study. A lot of information on work being done was available, and it was difficult to determine what was most relevant. I prioritised to study STPA before ice management, to make it easier to understand which parts of ice management that are most relevant for a case study, and what information I needed to obtain. To further my understanding of ice management, which is entirely new to me, I have read and used both state of the art and more established literature.

In December, while finishing my specialisation project, I had the opportunity to have a brief visit to the Korea Maritime and Ocean University (KMOU) and the Korean Research Institute of Ship and Ocean (KRISO), and to participate at the seventh Arctic Partnership Week which was held in Busan, South Korea. Here I learned much about the state of the art research being done and was even more humbled over how little I can cover in a specialisation project, and a master thesis. I have not gone into deep into the details of different parts of ice management, but rather taken a broad and shallow approach. I dug somewhat deeper into iceberg management, and how icebergs are handled by ice management vessels, to help myself conduct a case study where icebergs were the only threatening ice feature. Even though I have only applied STPA to a small part of ice management, I think it is adequate to be able to say something about the future of STPA in ice management.

1.5 Limitations

The scope of ice management in this master thesis has been narrowed down to ice management of marine operations in harsh Arctic environments. This is a broad field of study, and I have only scratched the surface of ice management. A complete, or more thorough analysis of ice management, could have been useful, though not possible to do in the scope of a master thesis, perhaps not even in a PhD thesis.

For the case study, the scope of ice management has been further limited to a specific marine operation located in an area not infested by sea ice, and that the only threatening ice feature is icebergs. The literature study has focused on ice management in general and STPA in particular. The objective of conducting this case study is to learn more about the STPA methods applicability to similar problems, and not to do a complete in-depth study. The case study is held to a high-level.

1.6 Contributions

This master thesis establishes fundamental knowledge on ice management and STPA, and a potential contribution of this may be to ensure the safety of future marine operations in Arctic environments. Identifying present and future challenges of ice management, and other facets of importance with respect to threat identification in ice management may shed light on the necessity of a new approach to hazard analysis in this domain.

Through literature study and case studies, STPA and traditional hazard analysis methods are compared. Potential contributions may be an improvement of the STPA method itself, fortifying a new area of use for the STPA method, as well as more knowledge on how hazard identification should be conducted when ice features pose significant threats. Another potential contribution of this master thesis may be to identify the best way forward searching for an optimal hazard analysis method for marine operations in Arctic environments.

1.7 Structure

This master thesis starts with a short preface that contains practical information about what I have done, and where the work has been carried out. Following this acknowledgement are given, and an executive summary in both English and Norwegian states what has been done and why this work is important.

Chapter 1 sets the scene with background and motivation, problem description, and the project scope of this master thesis including objectives, approach, limitations, contributions and this outline summarising what is found in the rest of the master thesis. Chapter 2 introduced ice management and its necessity, which is the theme of the case studied later in this master thesis.

Chapter 3 briefly introduces FMECA and some of the method's advantages and limitations. Following this, a case is studied using FMECA in Chapter 4. Chapter 5 introduces STPA, the foundation it is built on, the need for a new hazard identification method and the method's advantages and limitations. Following this, the same case that was studied using FMECA is studied using STPA in Chapter 6.

Chapter 7 provides a comparison between the two case studies specifically, and the two methods in general. Also, suggestions on how future hazard identification could be conducted are discussed. Further conclusions, discussions and recommendations for further work are provided in Chapter 8.

Appendix A contains acronyms, and Appendix B and C contains a list of terminology used in ice management and STPA respectively, for those not familiar with these topics. Appendix D contains much of the findings in the STPA case study. Finally, the bibliography is found.

Chapter 2

Ice Management

2.1 Definition Harsh Arctic Environments

The Arctic Council have defined Arctic boundaries of the Arctic landmass into three zones, the High Arctic, the Low Arctic and the Subarctic (i.e. south of the Arctic), depending on climate and vegetation. For the maritime Arctic, a similar definition based on climate is also made, and it correlates to the maximum ice cover extension on a given date each year. This definition is as we see in Figure 1.1 varies from year to year.

Regions outside this definition are not relevant for ice management (expect from perhaps a drifting iceberg or two that may be handled by offshore supply vessels). Usually, all marginal seas that are shown in Figure 2.1 are included when discussing the Arctic Ocean. However, for operations in the Arctic Gürtner et al. (2012) suggests a definition in terms of severity of the ice conditions:

☞ **Workable Arctic**: Almost all-year open water, area governed with cold temperatures and darkness, no sea ice but icebergs may occur (e.g. Barents Sea, East Coast Canada).

☞ **Stretch Arctic**: Considerable open water season but intrusion of first-year and potentially multi-year sea ice wintertime (e.g. Russian Arctic, Chukchi Sea).

☞ **Extreme Arctic**: Limited open water season together with severe first-year and multi-year sea ice, as well as glacial ice (e.g. North East Greenland).

These are useful distinctions when discussing all surface operations, e.g. station-keeping, transportation and or convoys, which is becoming more and more attractive as ice concentrations are reduced (and perhaps also as ice management operations are improving). When drilling is of interest, the ocean depth is of great significance. Hamilton (2011) distinguishes between deep and shallow waters in the Arctic:

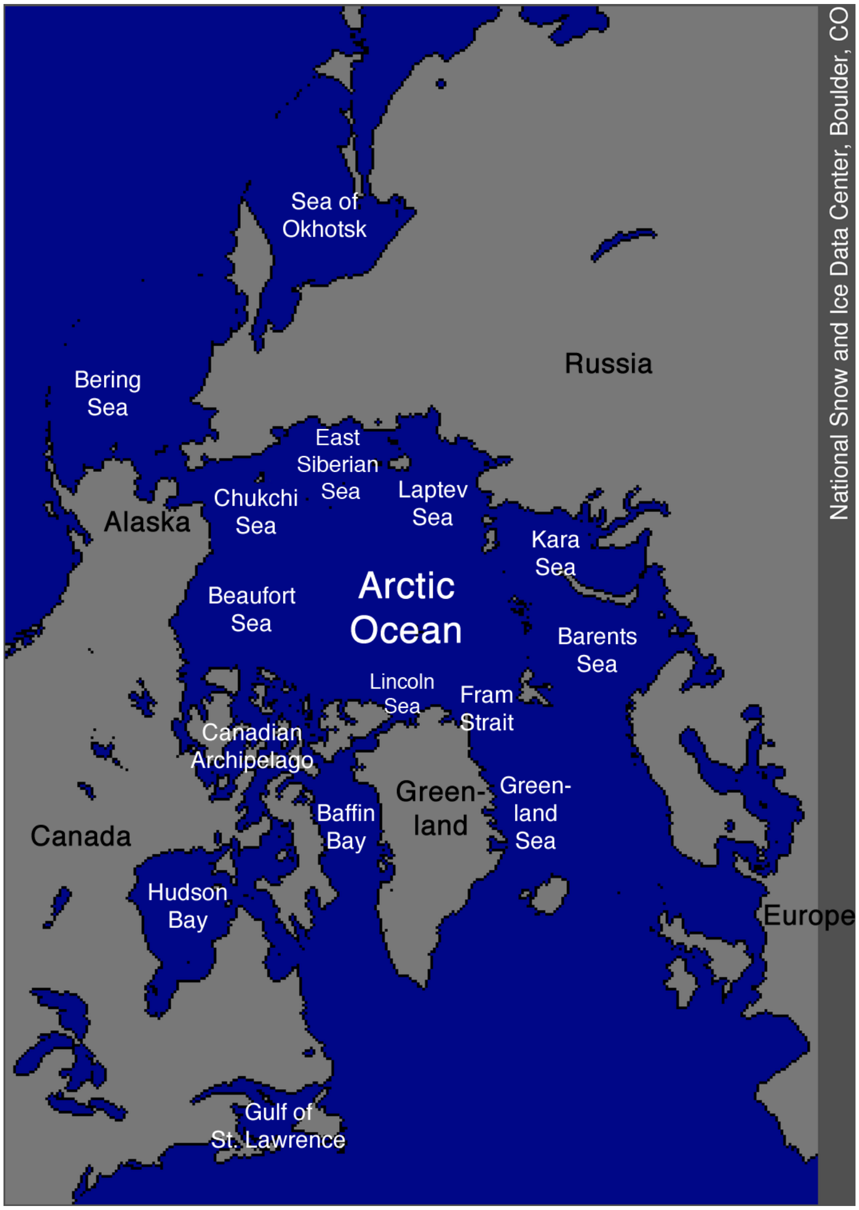


Figure 2.1: The Arctic Ocean. Credit: National Snow and Ice Data Center (NSIDC, 2018)

☞ **Shallow Arctic water**: Less than 100 meters deep

☞ **Deep Arctic water**: More than 100 meters deep

In the Arctic deep waters is defined as waters deeper than 100 metres, which is rather shallow compared to other offshore operations that are only affected by weather conditions such as wind, currents and waves. This conservative distinction is made in the Arctic because of the extra difficulty provided by severe ice conditions. Many factors are affecting whether or not an area can be classified as harsh Arctic environments. For the case studies in this master thesis, an arbitrary area with only icebergs will be evaluated, i.e. not infested with sea ice.

Section 2.2 defines and describes the necessity of ice management in harsh Arctic environments. Mastering Arctic conditions are of interest to many stakeholders. The region is rich on resources, and all year round shipping through this region would impact global trade.

2.2 Necessity of Ice Management in Harsh Arctic Environments

Depending on both geography and industry considered, ice management can mean numerous different things. The Snow & Ice Management Association (SIMA) in the U.S have created a glossary for the snow and ice management industry, i.e. those that work with service for private property owners or government agencies that hire private snow contractors to service streets, facilities and sidewalks. SIMA (2017) defines ice management as:

☞ **Ice Management** is the mitigation of ice accumulation or potential ice accumulation using chemical or physical processes.

When it comes to ice management of marine operations in harsh arctic environments and other regions infested by sea ice and icebergs, a different definition may be useful. In his review of experiences within ice and iceberg management, Eik (2008) found no unambiguous definitions of ice management. Depending on regions and ice features of relevance terms varied. There are similarities to sea ice management and iceberg management, so the two are not differentiated between in his proposed definition:

☞ **Ice Management** is the sum of all activities where the objective is to reduce or avoid actions from any kind of ice features.

Slightly modified, this definition includes, but is not limited to:

- Surveillance and monitoring of ice features
- Threat identification and evaluation of ice features
- Physical management of ice features
- Procedures and training

These bullet points do, in general, apply to all ice features. However, it is often practical to differentiate between sea ice management and iceberg management, as I will show later in this chapter. However, the case studies in this master thesis are limited to icebergs. This theory considers all ice features, i.e. general ice management of marine operations in harsh Arctic environments as it is defined in 2.1, and particularly how threat identification is made.

There is much motivation to improve ice management operations in the coming years for those that desire a higher level of activity in the Arctic. The Arctic is vulnerable, and one of the places where the effects of climate change seem to appear first. In a survey on *Arctic public opinion* by Gordon-Foundation (2015) when asked about the greatest threat to the Arctic, most respondents point to the environment. Other common responses included environmental damage not tied explicitly to climate change (e.g., pollution), resource exploitation, and oil and gas exploration. Ice management is necessary to ensure safe operations, avoid significant accidents, and at least not worsen public opinion.

Interest in the Northwest Passage (NWP) and Northern Sea Route (NSR) shown in Figure 2.2 is augmenting, as it will be shorter and therefore also cheaper due to reduced expenses per ton of freight transported. Unfortunately, it does not appear to be the case that increased use of the NSR contributes to any noteworthy climate benefits, as the additional impact of emissions in the Arctic more than offsets the effects of shorter voyages (Lindstad et al., 2016). To further develop NSR transit shipping, year-round commercial navigation is necessary. Milakovića et al. (2018a) points to the development of maritime infrastructure and icebreaker support along the NSR and less severe ice conditions as important factors, i.e. ice management is one of the factors that must improve.

Significant parts of the worlds undiscovered hydrocarbons rest in the Arctic (Gautier et al., 2009). It is shown by Hamilton (2011) that about 50 % of the undiscovered oil resources in the Arctic are in deep waters, and 75 % of these are in areas with severe ice conditions, practically unavailable for us today with state of the art technology. There are few examples of successful operations in deep waters. Some have been made in the Canadian Grand Banks where waters are deep but are in an area without severe ice conditions (Eik, 2008). To ensure safe marine operations in harsh Arctic environments, ice management will be necessary.

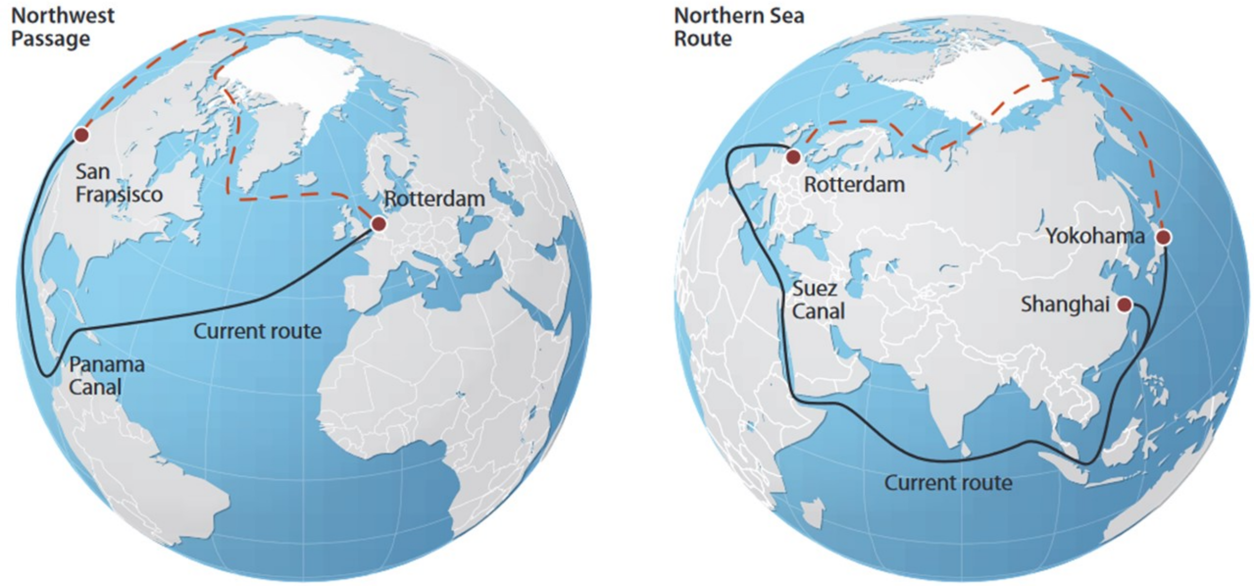


Figure 2.2: Sea routes. Credit: Arctic Monitoring and Assessment Programme (AMAP, 2011)

The necessity of ice management has been discussed in this section. There is no such thing as an unambiguous ice management process, and this is not provided in this master thesis. However, what I consider to be the most critical parts of ice management to be familiar with to be able to identify hazards are the focus in the rest of this chapter. In particular, the focus will be on:

- Surveillance and monitoring of ice features.
- Threat identification and evaluation of ice features
- Physical management of ice features

The extent to and implication of each part listed above would vary significantly on the characteristics of each given project. In addition to these aspects, data sources and expert judgement is briefly discussed in Section 2.6 In Section 2.7 some general challenges with ice management are mentioned, and some specific challenges related to threat identification are pointed out.

A different approach to describe an ice management process concerning threat identification would be to investigate how this is done today. What is of interest in marine operations in harsh environments not infested with ice, and built on this to deduce which additional steps or refinements that would be necessary. E.g. to account for loads from ice features designing ships or platforms and determining how much ice management resources that are needed. Albeit much knowledge on structural engineering would be necessary, and this approach is considered to be out of scope for this master thesis. Section 2.3 provides some insight into the factors of importance to threat identification, which is the focus of this master thesis.

2.3 Surveillance and Monitoring of Ice Features

For ice management operations, several factors must be taken into account, and work is done on several levels to monitor ice features, and different aspects are important to various operations. In this section, I will describe the generality of surveillance and monitoring of ice features, and what kinds of ice features that are of interest to different types of operations.

2.3.1 What should be Monitored?

Necessary information to plan and conduct a marine operation in the Arctic vary considerably in terms of the geographical region and time of year of operation as well as the type of operation it is. We know that in parts of the Arctic defined as the *workable Arctic*, such as of the coast of Canada in the Barents Sea, there might not be necessary to consider ice management resources with respect to sea ice, and one may limit the efforts of monitoring, threat identification and physical management to drifting icebergs. On the other hand, areas such as North East Greenland are in what we define as the *extreme Arctic*, where operations are dependent on extensive ice resources.

Operations to rescue people from sinking vessels or to clean up oil spill after an accident might require immediate and real-time information, and depend on systems to evaluate ice velocity, ice trajectory and such to be able to respond to an accident immediately. Shipping routes, on the other hand, are planned, and highly detailed information is not necessary. Information about where the marginal ice zones usually lie and some information on ice features might be sufficient to decide on necessary ice class of the vessel and to what extent ice support is needed depending on the time of the year the transit takes place. However, during operation, a higher level of information is required.

This master thesis will have some limitations. In the case studies, we are not concerned with operations in harshest Arctic environments, where ice features are severe. However, in these environments, the necessary information needed for each operation varies a lot, and it is both impractical and expensive to attain too much information. What is needed for each operation should be determined in the planning phase. Such as for the planning of a shipping route some information is available in different data sets, and these are described further in Section 2.6 *Data Sources and Expert Judgement.* All operations in harsh Arctic environments need some ice management resources and tools to evaluate threats to assist personnel operating ice management resources. Ice management resources may be, e.g. the design of the vessel or supporting vessels such as icebreakers. Threat identification and evaluation are discussed further in Section 2.4 *Threat Identification and Evaluation of Ice Features.*

Weather conditions are also of importance, as it affects the ice features, and are by themselves sources of threats. However, weather conditions will in this chapter only be discussed indirectly with respect to how they are relevant for ice features. This section will focus on the tools used to accumulate information about ice features, at the time it is needed, and their limitations and advantages. Table 2.1 shows some parameters that are of importance with respect to sea ice management and iceberg management, and related weather conditions that may affect these parameters. This is not a complete list of what is important to monitor, but gives a simplified overview. Composition of ice in an area are not homogeneous, so it is important to consider the morphology of ice parameters, marginal ice zones, fast ice boundary, etc. Weather conditions such as storms might lead to deformation of ice, new icebergs because of calving, fast ice breakout, ice push events etc.

Table 2.1: Parameters of importance with respect to sea ice and iceberg management and related weather conditions

Sea ice parameters	**Iceberg parameters**	**Related weather conditions**
Ice concentration, type, strength and thickness	Size of icebergs	General weather, global temperature changes
Sea ice velocity	Iceberg velocity	Wind and current speed
Sea ice trajectory	Iceberg trajectory	Wind and current direction and Coriolis forces
Floe size (new ridges)	Number of icebergs (density)	Storms, leading to calving and large scale cracking

As mentioned, weather conditions and monitoring of this is not discussed directly, but indirectly concerning how they affect ice parameters. When it comes to preventing accidents and ensure safe operations weather conditions must be considered independently, and are described further in Section 2.4.3. Weather conditions such as wind, waves and currents can lead to hazardous situations when no ice features are present. Reduced visibility and or harsh weather can make it harder to navigate and lead to collisions, grounding, etc., and it may lead to a reduced capacity of monitoring, ice management and communication which may lead to hazards. Other factors such as human, organisational, software, component, etc. are also important, but are not the focus in this section.

2.3.2 How can Ice Features be Monitored?

There are several methods applicable to monitoring ice features, and the coverage of these methods vary greatly. After defining the scope of the project, trends in ice features, perhaps in combination with monthly data sets making comparisons might be adequate to determine the level of ice management resources needed for an operation in a given location at a given time of year. As conceptualisation of the project finishes and the detailed analysis starts, there might be necessary to attain more detailed information. Figure 2.3 shows coverage of some different approaches to ice monitoring. For example, some satellites may provide information on the day-to-day movements of the ice, and also macro-trends over more extended periods, providing imagery showing everything from 10 meters to hundreds of kilometres. In comparison, drifting buoys may give much more detailed information, but at a smaller scale.

- **Long term monitoring:** Planning. Definition of project and conceptualisation
- **Medium term monitoring:** Simulations, threat identification, redesign and verification
- **Short term monitoring:** Operation. Real time threat evaluation and ice management.

None of the methods is efficient by themselves in terms of providing a deep insight into ice conditions. It might be costly to get very detailed information about the ice features in a given area in real time, and at the same time, this information is not necessary for the early planning of a project and hazard identification. For this more long-term data studying data sets and ice charts might be sufficient.

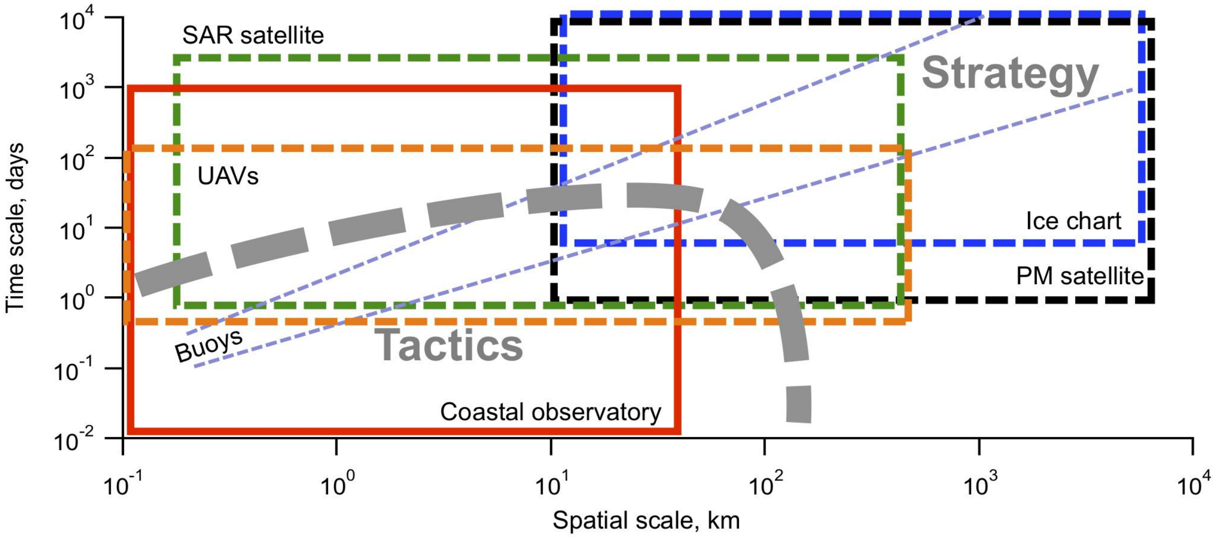


Figure 2.3: Schematic of spatial and temporal resolution and coverage of some sensor systems (Eicken et al., 2011)

2.3.3 Sensor Platforms

There is a wide range of sensor types and sensor platforms available, which may be used to fill the gaps when available data is not sufficient during planning or to accumulate necessary data during a marine operation. Every type of sensor platform as shown in Table 2.2 provide vast amounts of data, but still, it is argued that two or more systems must be used in combination to give enough information (Eik, 2008). Different kinds of sensors apply to these sensor platforms, and therefore, one sensor platform alone has difficulties providing all the information needed to make good decisions.

Table 2.2: Overview of sensor platforms and types. Adapted from (Haugen et al., 2011)

	Platform				
Sensor Type	Satellite	UAV	Shipboard	Buoy	Underwater
Optical (VNIR and TIR)	x	x	x		
Laser altimeter/scanner	x	x			x
Radiometer	x	x	x		
SAR	x	x			
Marine radar			x		
Scatterometer	x	x			
Radar altimeter	x	x			
Acoustic techniques			x		x
Meterological suite		x	x	x	
Oceanographic			x		x

Further description of sensor types and their applicability is provided by Haugen et al. (2011) who gives a comparison of different sensor platforms in terms of coverage, resolution, and cost per area when installed on satellites, UAVs (unmanned aerial vehicles), ships, buoys, USVs (unmanned surface vehicles) and underwater solutions (sub-sea) which are reproduced in Table 2.3. "Different sensors have both appealing features and inherent drawbacks that influence the measured quantities. These properties are important to consider when choosing which sensors to utilise on a platform." Cost is essential for obvious reasons, but the resolution is also crucial when choosing which combinations of sensors and sensor platforms to use. There is some overlap between different sensor platforms, but to attain detailed enough data to be able to identify and evaluate threats efficiently, the resolution must be of a certain quality.

Table 2.3: Comparison of sensor platforms. Adapted from Haugen et al. (2011)

Platform	**Coverage**	**Spatial resolution**	**Temporal resolution**	**Cost per area**	**Suggested area of operation**
Satellites	Excellent	Intermediate	Low	Intermediate	Distant
UAV	Very good	High	Intermediate	Intermediate	Close to distant
Shipboard	Low	Intermediate	High	Low	Close
Buoys	High	Sparse	Intermediate	High	Close to int.
USV	Intermediate	Sparse	Low	High	Intermediate
Subsea	Good	Excellent	Intermediate	Intermediate	Close to int.

In this master thesis, an objective is not to determine which sensor platform or sensor types that are best for a set of different marine operations that require ice management resources.

But to investigate whether or not the methods of identifying hazardous scenarios are sufficient today is. Traditionally all of the above platforms and visual observations have been used, but in recent years subsurface ice intelligence systems have been more and more used, as technology has improved. The futuristic ice management scenario in Figure 2.4 also show the use of aerial drones. Efforts are also being made to enhance sub-surface monitoring, which have huge potential and have been shown to travel further and further under the ice. "Now we know that these systems are reliable. Also, ice-characteristics are more distinct underwater, and is not dependent on weather-conditions (Eik and Løset, 2009)."

In harsh arctic environments, ice features and other parameters influencing the marine operation may change rapidly. Figure 2.4 shows how an example of an advanced autonomous futuristic ice monitoring system retrieving data using both stationary sensors and a mobile sensor platform consisting of satellites, aerial drones and underwater vehicles. Data are feeding the ice management resources (three icebreakers) with information on how to best manage the incoming ice. If this is the future of ice management monitoring, it is safe to say that the systems used are becoming more and more complex. Extensive use of such software is necessary to succeed in implementing autonomous sensor platforms.

2.4 Threat Identification and Evaluation of Ice Features

Threat identification and evaluation happens in several phases, in the same way as monitoring. Threat identification is of interest in the design phases of marine structures to determine design features in harsh Arctic environments and to decide which ice management resources is necessary for the given operation. Several tools are being developed both to improve the planning of projects (project future ice features), and numerical tools and weather forecasts used to enable real-time decision support that helps ensure safe operations.

It is out of the scope of this master thesis to go into detail on all the various simulation tools and approaches to identify threats. But systems to monitor ice features and estimate ice loads that must be mitigated are getting increasingly more complex. Rather simple, but successful operations, as described in (Moran et al., 2006) are not representative of future operations in the Arctic. To benefit from the riches that lie in mastering Arctic operations, we must conquer the challenges that lie ahead. In doing so, new sources of flaws might become apparent, and traditional hazard identification might no longer be adequate, as indicated in Chapter 5.

For threat identification of ice features, the region of interest to our operation might as well determine whether threats from sea ice, icebergs or both are of importance. As described in Section 2.3 parameters are quite different, necessary sensor platforms to have adequate surveillance may vary significantly and with that relevant threats. Threat evaluation of icebergs might be limited to the number of icebergs, their size and trajectory, as environments infested with

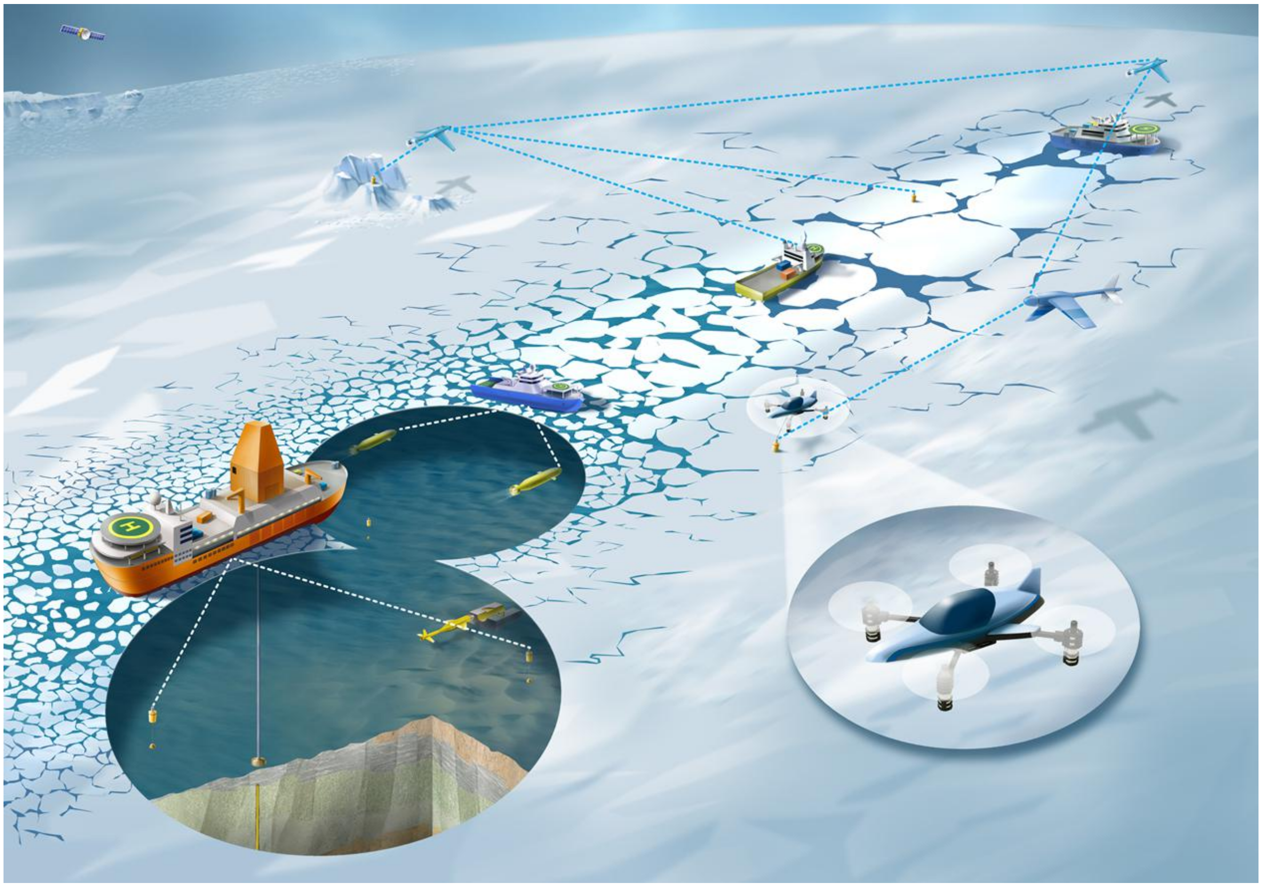


Figure 2.4: Future of ice management (Skjetne et al., 2014). *Copyright: NTNU. Illustration: Bjarne Stengberg*

sea ice rarely have large icebergs in them. For sea ice management, more detailed information is necessary, as the interactions in sea ice are more complex than drifting icebergs. Weather conditions, morphology, and ice parameters such as concentration, type (age/strength), thickness and more may be of interest.

2.4.1 Simulation Tools and Processing Data

Ice conditions in the Arctic may change rapidly, and it is difficult, if not impossible, to be confident that decisions made concerning navigation of a vessel or icebreaker fleet are by just relying on crew experience. Control and decision systems are helpful to process and translate vast amounts of data into real-time decision support. Any effort to improve and develop ice observer systems that, e.g. are automated and by the help of computes may aid vessel crew is of interest (Haugen et al., 2011).

There is a wide range of simulation tools available, though not all publicly available or commercially ready. Section 2.6 on data sources discussed briefly available data sets, but not in much detail. In terms of hazard identification and making improvements to this in ice management, I will not focus on the data sources, but rather how they are interpreted and errors that might occur doing this. Open source data and expert judgement are often used in simulations, and then testing, e.g. with available data, or real trials are performed to verify suggested models. In my opinion, an optimal model needs to use real-time data from ice features nearby to ensure correct input.

2.4.2 Some Software Tools for Simulation and Decision Support

In addition to data sets, data obtained by ice monitoring may be daunting and time-consuming to process without computational support. This is not an extensive analysis of all available software tools to identify hazards and support ice management, but rather just some examples of different software available. AIMS (Aker Arctic's ice management suite is a tool that maps incoming ice conditions into outgoing ice conditions, as the actions of ice management vessels affect the ice conditions approaching, e.g. a dynamically positioned vessel, that must itself be positioned appropriately to withstand loads of the incoming sea ice (Neville et al., 2016). This tool requires discrete floe size categories as input, and are still being modified. It has not yet been tested in the extreme Arctic.

Simulation of the ice management process is useful in terms of determining how the deployment of icebreaker fleets may be optimised for a set of ice conditions (Hamilton et al., 2011), and a lot of work is being put down into developing better tools for this. (Metrikin, 2014) provides a software framework for simulation station-keeping of a vessel in discontinuous ice. To build advanced software tools, it is necessary to have extensive knowledge about how ice behaves. SIBIS (Simulation of Interaction between Broken Ice and Structures) investigates just what the abbreviation says (Metrikin et al., 2015). Tools like this may be used to meet challenges of measuring ice loads directly with conventional methods Kjerstad et al. (2018), a project supported by ExxonMobil, that proposed a method for *real-time estimation of full-scale global ice loads on floating structures.*

2.4.3 Estimation of Parameters

This master thesis is not an extensive analysis of all measures that might be used to improve parameter-estimation in the ice management process but meant as an example of the work being done to enhance preliminary analysis before operations are executed, or to develop simulation models. In several instances, data available is scarce and based on little information, future ice conditions might need to be predicted.

Methods to interpret and improve the usefulness of sea ice images are being developed, in response to the fact that not all imagery from, e.g. satellites have good enough resolution, or weather conditions might lead to lower quality images that need to be processed to give necessary information. Ice management operations cannot be utterly dependent on complete input data at all times, as weather and ice conditions make that difficult. A method proposed by (Zhang and Skjetne, 2014) manages to take low-resolution imagery and identify individual ice floes, and with that new piece of information "calculate the position, size and shape of each ice flow, the ice concentration, and the floe size distribution."

A method for estimating ice thickness based on WMO egg code when ridging parameters is scarce is proposed by (Milakovića et al., 2018b). Information on both undeformed ice (level ice) and deformed ice (mainly ridges) are needed to estimate necessary ice resistance of a marine operation in the Arctic. However, ridging parameters are often missing in these egg codes. Expected ice along a planned route may be underestimated by as much as 29 % using this approach without ridging parameters.

If WMO ice thickness ranges are swapped, when ice ridging parameters are missing, with equivalent-volume ice thickness ranges (EVITRs) that accounts for both for the level ice and the deformed ice features the same case study found that an underestimation of expected ice could be reduced from 29 % to 2 %. For as long as ridging parameters often are unavailable, this novel approach might be useful in determining expected The method is based on correlating the amount of deformed ice to the stage of development of the ambient level ice, by analysing a series of ice thickness profiles for a particular area and season. Several more examples could have been provided.

2.4.4 Additional Sources of Threats for Marine Operations in the Arctic

In this subsection I will allow myself to be a bit suggestive, trying to think of possible additional sources of hazards related to ice management (other than those directly related to not managing to mitigate peak loads from ice).

Is there a chance that ice management systems grow so complex that crew (if any) are incapable of mitigating risk without decision support provided by the mentioned tools (and all the unmentioned tools)? For these tools to function optimally, a lot of input data are necessary. Will there be situations with lousy weather and ice conditions that they may cripple these systems?

A root cause analysis for Arctic marine accidents from 1993 to 2011 was done by Kum and Sahin (2015), and "[...] results indicate the significance of crew training and competence requirements and as well as more Arctic navigation training centres. The analysis proves that safety is a real problem in the Arctic region, and marine accident analysis is a significant gap for the researchers." Fuzzy fault tree analysis (FFTA) was used to determine significance of basic events with respect to the top events by using the *Fussel-Vesely importance measure* (F-VIM), which is the probability that at least one minimal cut set that contains a basic event has failed at time *t*, given that the system has failed at time *t*.

FFTA were made for the top events *collision* and *grounding*. The most significant basic events were often related to communications problems, inexperience and ice features. For collision, the most significant basic event in terms of F-VIM and likelihood were *communication failure vessel to icebreaker or tugboat*, and for grounding the equivalent was grounding as ice floes stuck between the bottoms. For this type of study, there are limited data sources, and expert judgement had to be used to determine the probability of each basic event. Better analysis of accidents similar accidents and other types of ice-navigation related failures such as icing, stuck in ice are machinery failures necessary.

This tells me that improvements in ice surveillance and monitoring and threat identification and evaluation of ice features are not the only necessary steps to ensure safe marine operations in harsh Arctic environments. Important causes of accidents in this root cause analysis are human errors and organisational errors. Section 2.3 also points to a future with more complex systems of monitoring software errors and complex interactions may become more critical. More research is needed on accidents in the Arctic, particularly for larger operations where successful ice management is vital.

Additionally, ice management resources such as icebreakers may also provide additional sources of threats. (Zhang et al., 2017) and (Goerlandt et al., 2017) discussed safety distance modelling for ship escort operations in the Arctic. In severe conditions, there are scenarios where icebreakers may collide with the escorted vessel, or with each other. In some instances, ice management support is needed from more than one icebreaker, and there is a trade-off between the distance between these and the protected vessel/platform, and the risk of them colliding with each other.

2.5 Physical Management of Ice Features

The objective of physical management of ice features is to prevent hazardous scenarios from occurring, i.e. deflecting icebergs and reducing loads from sea ice. Ice monitoring and threat evaluation of ice features are performed in the early planning of marine operations to determine necessary ice management resources. Vessels, platforms, etc. stationed or on transit through harsh Arctic environments are designed to withstand more than equivalent vessels and platforms in other regions of the world. *DNVGL*, an international accredited registrar and classification society, have published *rules for classifications of ships* (DNVGL, 2017). Classifications similar to this one may be used to determine which specifications a vessel needs, as detailed specifications are also listed for operations in ice-infested areas.

Table 2.4: Polar Class (PC) notation from (DNVGL, 2017)

Polar Class	Ice Description (based on WMO Sea Ice Nomenclature)
PC-1	Year-round operation in all Polar waters
PC-2	Year-round operation in moderate multi-year ice conditions
PC-3	Year-round operation in second-year ice which may include multi-year ice
PC-4	Year-round operation in thick first-year ice which may include old ice
PC-5	Year-round operation in medium first-year ice which may include old ice
PC-6	Summer/autumn operation in medium first-year ice which may include old ice
PC-7	Summer/autumn operation in thin first-year ice which may include old ice

Ship notations such as the Polar Class in Table 2.4 are made used to ease the work of owners, designers and administrations in classifying ships correctly based on the intended use, and so that it is easier to find ships withstanding requirements. In this classification, it is also made clear that ships with a polar class notation from PC-1 to PC-6, may be given the additional notation *Icebreaker*.

In other parts of this classification and different classifications, a wide range of rankings of icebreakers are available. These are with respect to the loads an icebreaker is capable of withstanding. Operations in the Arctic are often well planned and executed with large safety margins. Improvements in ice management are interesting to ensure the safety of projects as they are today, but to extend the reach of marine operations further into harsh Arctic environments. However, the correct classification of vessels does not guarantee successful ice management operations. Effective physical ice management requires training. Field trials of physical ice management (Neville et al., 2016) showed that the crew's ability was crucial to succeed.

Figure 2.5 illustrates the impact physical ice management may have, here for a Dynamic Positioned (DP) vessel. Cost of design may be considerably reduced, since physical ice management, when effective, may reduce peak loads. The large peak is with respect to loads that the ice management resources cannot handle, so solutions to safely disconnect a drilling vessel are introduced instead of having a much higher number of ice management resources available.

2.5.1 Iceberg Management

Preventing collision with icebergs are often the focus in areas not infested with sea ice. Earlier in this chapter, it is mentioned important iceberg parameters are the density of icebergs (how many), their size, trajectory (velocity and direction), etc. For areas that are not infested with sea ice, it is not necessary to have vessels classified as icebreakers to manage icebergs physically. Vessels may be used to tow away icebergs, and water cannons may be used to change their trajectory (Skjetne et al., 2014). This brief explanation may make iceberg management sound rudimentary, but must, of course, be considered. Eik (2008) points out that we know very little

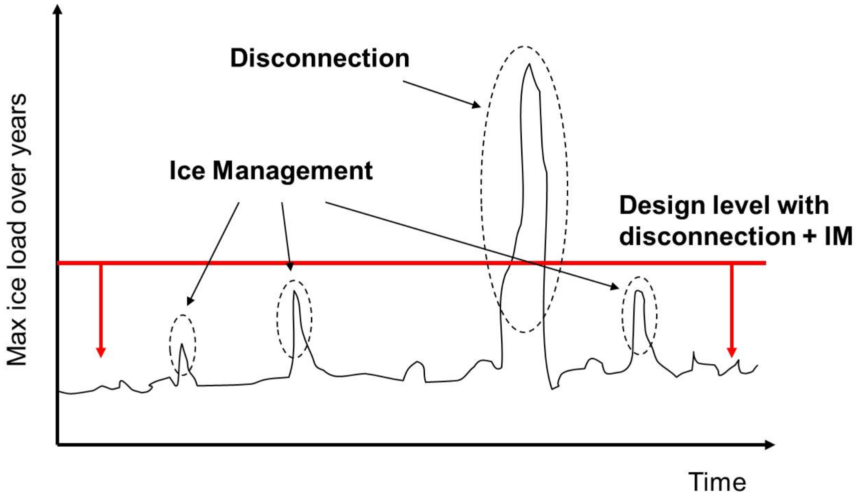


Figure 2.5: Effects of ice management (Skjetne et al., 2014) *Illustration: Sveinung Løset*

about how to handle icebergs that have frozen into the sea ice.

2.5.2 Sea Ice Management

Some more focus has been put on sea ice management. Various kinds of ice features call for different ice-breaking strategies. Depending on the ice management resources needed, it is normal to deploy everything from 1 to 3 icebreakers. Figure 2.6 shows a description of how two icebreaker vessels may navigate to mitigate risk from ice while protecting a vessel (large blue dot is protected vessel) from incoming sea ice.

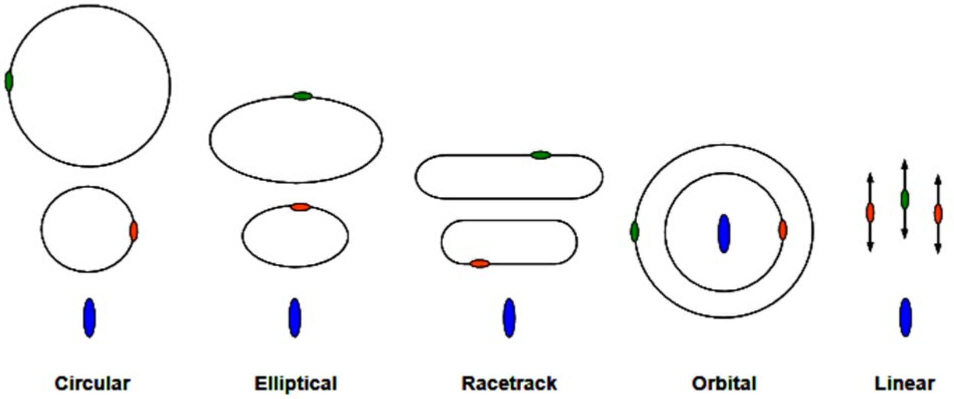


Figure 2.6: Examples of ice management fleet deployment patterns (Hamilton et al., 2011)

Not only must the number of icebreakers and deployment patterns be considered, but also which icebreaker classification that is necessary. Figure 2.7 shows a physical ice management operation in practice. When protecting a vessel, the goal is to keep the protected vessel within a managed sea ice channel. Software similar to that discussed in section 2.5 may be used to provide icebreakers with information of where to navigate to always have the protected vessel within such a sea ice channel with lower ice loads.

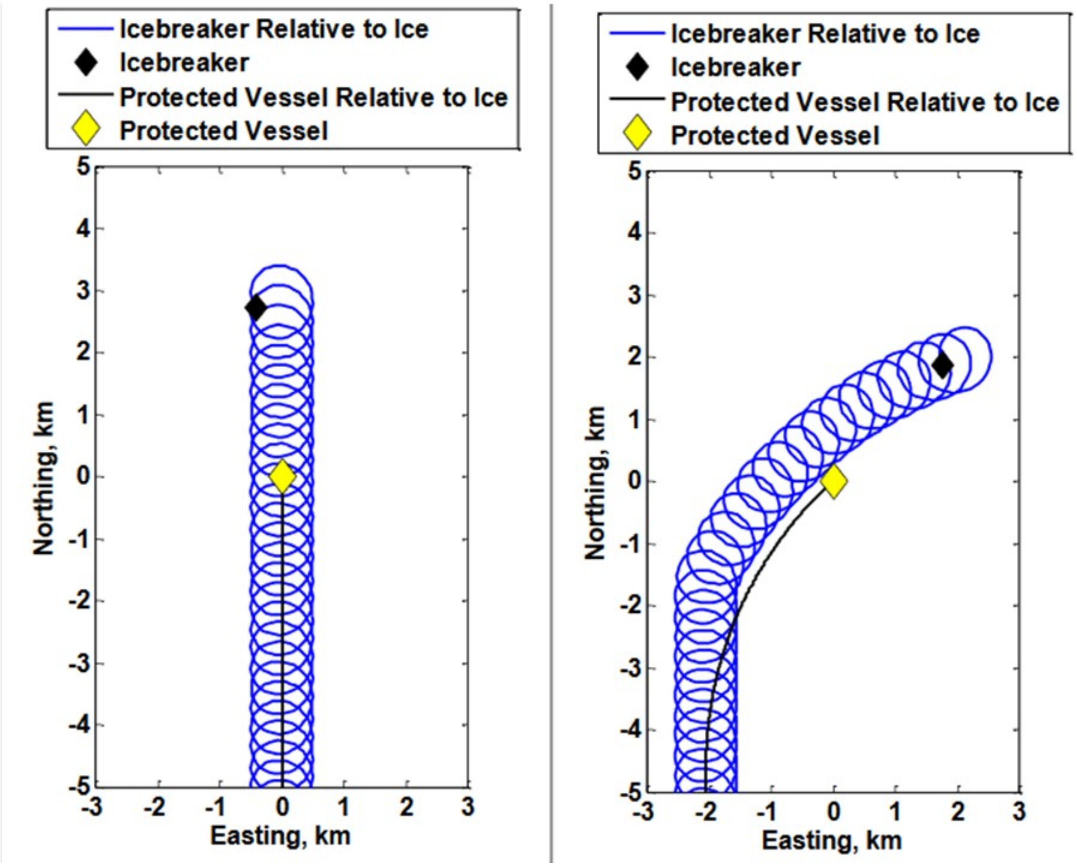


Figure 2.7: Physical ice management, one icebreaker and one protected vessel. Successful operation (left), and unsuccessful (right) (Hamilton et al., 2011)

2.6 Data Sources and Expert Judgement

Reliable information is vital to ensure safe marine operations in the Arctic but compared to open waters, we have little experience and need ice intelligence. Monitoring of ice features are done for most marine operations in harsh Arctic environments because historical data, expert judgement is mostly useful in the early planning of operations (they might also be helpful as input in different simulations, numerical analysis, and where no other data is available).

For example, American and British submarines equipped with sensors have been collecting data about the underwater surface of Arctic ice since the 1970s and is openly available on websites of the American National Snow and Ice Data Center (NSIDC). Another example is the Arctic Coring Expedition (ACEX) (Neville et al., 2016), that aimed to gather data in areas with high ice concentration, which has many applications, such as verifying models. CIS, ISIS, ICEWATCH, ICEMON and NASA are other examples of projects and organisations that have available data relevant to ice management. A full list of data sources are not provided.

In situations where data is scarce, and deployment of ice observation systems are impractical, we might need to make use of expert judgements. Generally, little data is an issue for hazard identification methods that do not handle uncertainty well, which BBNs provide a natural framework for (Sigurdsson et al., 2001).

2.7 Current Challenges with Ice Management

Operations in the Arctic have been done for over 60 years, but still, we are relatively inexperienced in the field of Arctic operations. To identify current challenges with Ice Management, I have attempted to structure and gather suggestions for further work in the available literature I have managed to look at so far during my work along with findings in this chapter.

Challenges in data sets: Several studies are done to improve simulation tools, based on available data sets. Data is scarce, and for some simulations, different data is needed. Some studies focus on how to better estimate parameters that are required for these simulations. Milakovića et al. (2018b) used EVITRs to calculate ice thickness along a planned route for a vessel, and argues that similar data sets should be made that are both area- and season-specific for the entire Arctic basin. Section 2.6 briefly pointed at the fact that from time to time expert judgement is necessary for providing sufficient data to perform preliminary analysis. This is not unique to ice management, but the scarcity of data leads to a need to further improve simulation tools for decision-making both during operations and with respect to planning.

Challenges in standards and regulations: Standards such as ISO 19906:2010 *Petroleum and natural gas industries – Arctic offshore structures* have some limitations according to Eik (2010), concerning some calculations. Calculations in the standard are deterministic and have some simplifications. The standard does not consider the mild climate when calculating the frequency of peak loads, and it is essential to understand that peak loads do not always occur during extreme weather.

Challenges in monitoring: Several efforts are being made to improve sensor platforms, aerial drones and underwater solutions may offer less costly alternatives for monitoring ice features. Sound ice observer systems, however, require investments, and at some instances, they might not be able to gather data when weather and ice conditions are severe. Ice observer systems must be reliable to ensure that necessary data is provided at all times. Eicken et al. (2011) stated that there was a clear need for further work on sensing systems at high spatial and temporal resolutions. Improvements are still being made on this field, and "translating such risks into operational procedures, and response frameworks may require further work, in particular in applying approaches developed for low latitudes or onshore Arctic environments." As we become more dependent on our ice observation systems, our operations may become vulnerable to faults in these software-intensive systems.

Challenges in threat identification: The phenomena we are trying to simulate are very complex, and it is difficult to make good predictions because of the complexity of ice interaction. Also, limitations in quality and or availability of good initial and boundary conditions are important steps to overcome to make better predictions and provide better decision support for ice management in the future. Real-time support is often important, so making computational models more complex is not necessarily the solution. There might be a tradeoff between when decision support may be provided, and to how helpful this support may be (Haugen et al., 2011). Important new causes to accidents may be complex interactions between human and software as tools used for ice management continues to develop.

Challenges in physical ice management: This tells me that improvements in ice surveillance and monitoring and threat identification and evaluation of ice features are not the only necessary steps to ensure safer marine operations in harsh Arctic environments. If routes such as NWP and NSR becomes more used, it is crucial that vessel crew on icebreakers undergoes sufficient training. Breaking sea ice for ice management is different from merely navigating through sea ice. Neville et al. (2016) shows that successful ice management operations today are highly dependent on the crew's ability and experience. Ice management itself may lead to more hazardous situations. More work needs to be done in managing threats of collision when protecting ships in convoy, or when several vessels are involved in ice management operations around a protected stationary vessel Zhang et al. (2017) (Goerlandt et al., 2017).

To meet some of the challenges in ice management, this master thesis evaluates the need for a new threat identification method. The following chapters briefly introduce a traditional hazard analysis method, FMECA, and a case study relevant ice management using this method. Ice management systems are subject to complex component, system and human interactions. Therefore, a working theory for this master thesis is that the traditional hazard analysis methods are not adequate to identify all threats in ice management systems. Following the FMECA case study, a relatively new method, STPA, is introduced, and an equivalent case study is performed using this method.

Chapter 3

Failure Mode, Effects, and Criticality Analysis (FMECA)

3.1 FMECA Overview

Failure mode, effects and criticality analysis (FMECA) is an extension of failure mode and effects analysis (FMEA), and today, the terms are often used interchangeably. FMEA is a qualitative method to identify all failure modes, but in FMECA, these are also ranked according to their importance, i.e. how severe the failure modes may be. Different kinds of FMECA focus on failures in the design phase (design FMECA), failures that occur during manufacturing, maintenance or operation (process FMECA) and inefficiencies in larger systems (system FMECA). FMECA may be used in early phases as a top-down approach analysing failures in the most critical system functions, and it may also be used later in the process as a bottom-up approach to consider each component individually. There are four main steps in an FMECA, adapted from Rausand (2011), are 1) identify, 2) analyse, 3) review and 4) act.

"*Failure modes, effects, and criticality analysis (FMEA/FMECA):* This method is used to identify the potential failure modes of each of the functional blocks of a system to study the effects these failures might have on the system. FMEA/FMECA is primarily a tool for designers but is frequently used as a basis for more detailed reliability analyses and maintenance planning." (Rausand and Høyland, 2004).

3.2 FMECA Process

In the first step, system boundaries and functions are defined, and all necessary information about the system is identified. *In the second step* the system is broken into subsystems and illustrated using, e.g. functional block diagrams or hierarchical tree diagrams to make the further analysis more manageable. To save time and effort this is done in the highest possible level in the system, and the system should only be further broken down into subsystems until one reaches the component level if it is necessary to identify more detailed failure modes.

Later in the analysis step FMECA worksheets such as the one in Figure 4.2, is created. The FMECA worksheets may vary for each analysis, but in general, all elements (i.e. the smallest parts the system were broken into) are considered for all functions and all operational modes. Items are subject to further examination if critical failure modes are identified.

As part of the preparation of FMECA worksheets, failure rates and the consequences of each failure mode are listed. These may be sorted in different manors, e.g. by assigning a number from 1 that is very unlikely (once per 1000 years or more seldom) or minor consequences (small system damage) to 10 that is frequent (once per month or more often) or catastrophic (major injury or death of personnel). The failure modes are then ranked, either in a risk matrix, as shown in Table 4.1, or by calculating a risk priority number (RPN). The higher the RPN number, the higher the priority.

In the third step the process and results so far (i.e. system, FMECA worksheets, the ranking of risk) are reviewed, to ensure that the basis for decision-making in the final step is as thought out as possible. *In the fourth and final step,* it is time to act and implement the findings.

3.3 FMECA Advantages and Limitations

Table 3.1: Advantages and limitations FMECA. Adapted from (Rausand, 2011), (Teikari, 2014)

Advantages	**Limitations**
Structured and reliable method for breaking down complex systems and evaluating subsystems and components individually	Not suitable for multiple failures or complex interactions, and difficult to identify causes to hazards not related to component failures
The concept and application are easy to learn, the method is well know and templates are available for most kinds of analysis	Identifying failure modes and causes requires may be tedious, time-consuming and require domain expertise of the analysts

The FMECA method is not described in detail in this master thesis. FMECA worksheets and a method to rank risk are shown in Chapter 4 in the FMECA case study. Table 3.1 shows some strengths and weaknesses of the FMECA technique. More detailed information on how to conduct an FMECA may be found in standards such as SAE-ARP 5580, IEC 60812, BS 5760-5 and MIL-STD-1629A (Rausand and Høyland, 2004).

Chapter 4

Case Study: FMECA in Ice Management

In this chapter, I will perform an FMECA analysis as briefly described in Chapter 3. The purpose of this analysis is to protect an FPSO (Floating Production, Storage and Offloading) from a collision with icebergs to ensure steady production, and prevent the defined losses in Table 6.1. System boundaries are set to include the FPSO, IMVs (Ice Management Vessels), sensor platforms for ice monitoring (observation sub-system) and the area being monitored. Weather forecasts are external.

This case study has some limitations, as described in Subsection 1.5. It is assumed that the FPSO is located in an area not infested by sea ice and that the only threatening ice feature is icebergs. This analysis is performed on the same high-level as the STPA analysis in Chapter 6, so that the two methods could be compared in Chapter 7. For the FMECA analysis, the system is divided into three sub-systems, the FPSO, IMVs and sensor platforms (observation), and we do not go into great detail on the component level, which may be unfair to the FMECA method since it is one of its strengths as shown in 3.1.

The three subsystems are further divided into:

1. *Subsystem* FPSO:
   1.1 Disconnection mechanism
   1.2 communication system

2. *Subsystem* IMVs:
   2.1 Engine
   2.2 Physical ice management (2.2.1 Water cannon and 2.2.2 Towing system)
   2.3 Communication system

3. *Subsystem* Observation:
   3.1 Sensor platform (3.1.1 Satellite, 3.1.2 UAVs and 3.1.3 Shipboard)

This is also shown in Figure 4.1.

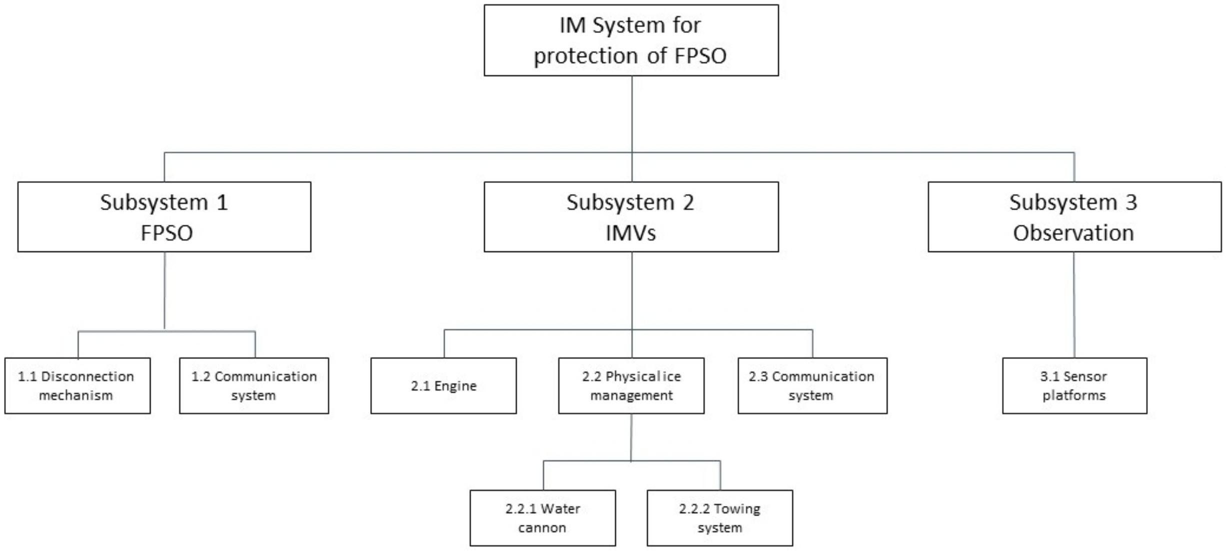
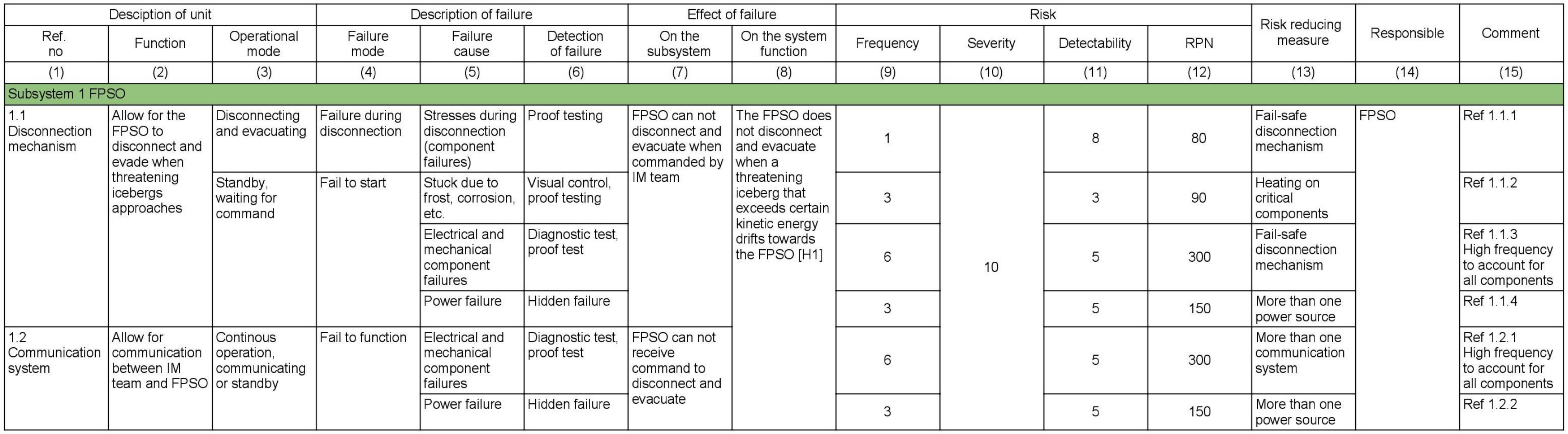


Figure 4.1: FMECA system

For this analysis, and to keep it on the same high-level as the STPA analysis in Chapter 6, we will not go further into the component level. The choice of sensor platforms for this case is not based on any in-depth analysis. Chapter 2 argues that a variety of sensor platforms is necessary to attain necessary data.

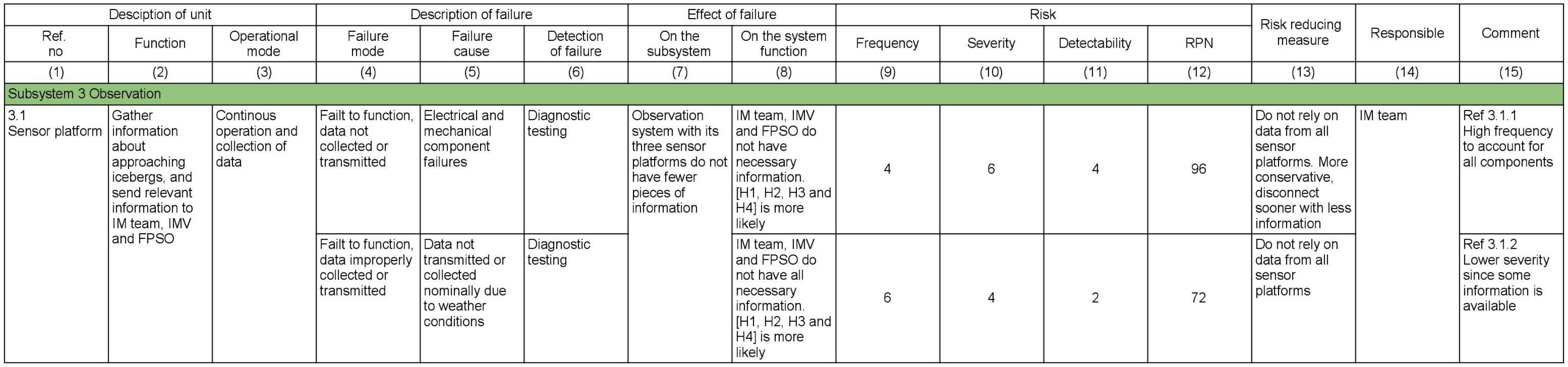
USVs and sub-sea satellites are considered unnecessary as we assume that there is little or no sea ice. Buoys are also considered to be inefficient since they are likely to drift just like the icebergs, and not detect any icebergs. Three sensor platforms were chosen for the FMECA analysis, satellites, UAVs and shipboard. These sensor platforms can carry all sensor types according to Table 2.2, and according to Table 2.3 the cost is intermediate or low per area, and they may cover various distances and resolutions. For the FMECA analysis we will not go down to the component level, nor the sensor types on each sensor platform, so this is considered to be adequate reasoning for which sensor types to use for this analysis. The purpose of this analysis is to be able to compare the FMECA method with the STPA method, so it is not necessary to go in further detail to see the advantages and limitations of the method.

The FMECA demonstrates that it is very straight forward to add further detail concerning the components in the different subsystems, but it did not occur to me to add the *local system* that IM team and IMV uses to make decisions and process data from sensor platforms. This was considered in the STPA but is not included in the FMECA analysis. Based on this a FMECA worksheets are made, and is given in Figure 4.2, 4.3 and 4.4.



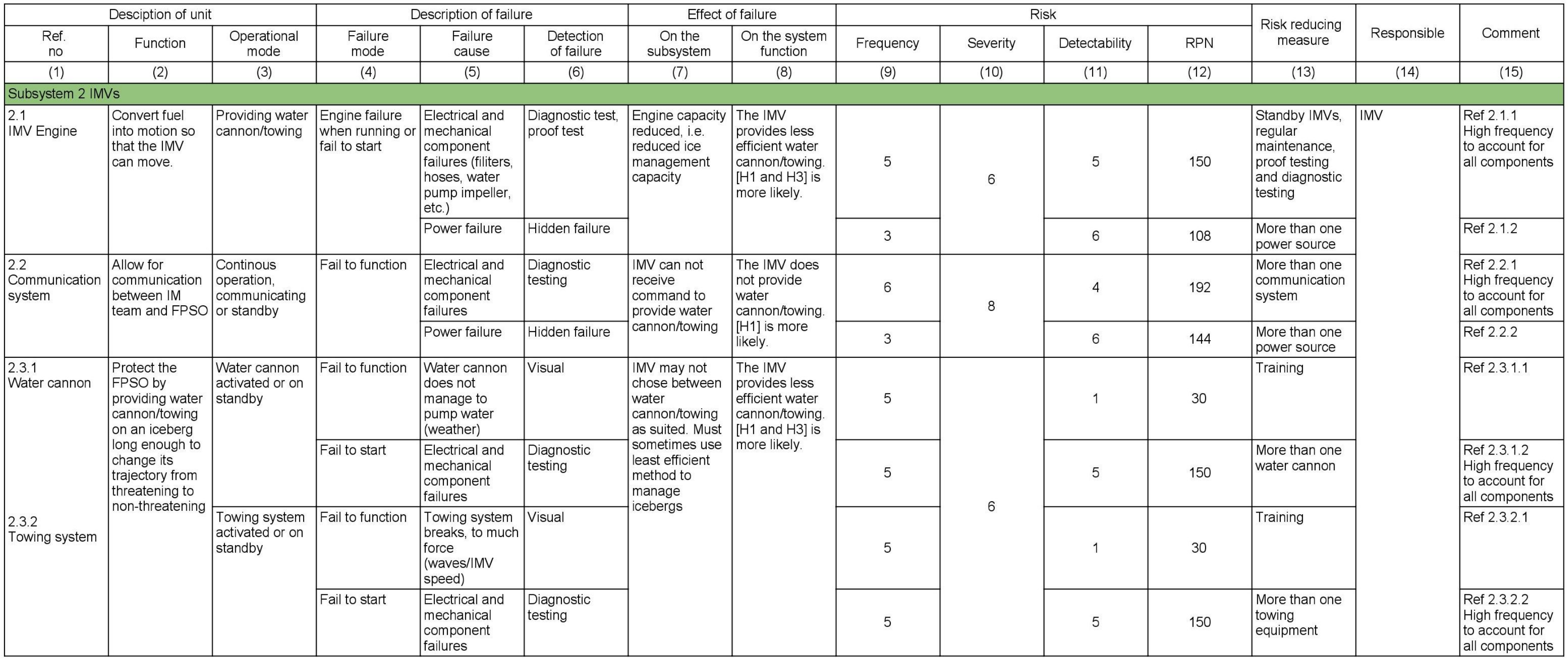
Desciption of unit			Description of failure			Effect of failure		Risk				Risk reducing measure	Responsible	Comment
Ref. no	Function	Operational mode	Failure mode	Failure cause	Detection of failure	On the subsystem	On the system function	Frequency	Severity	Detectability	RPN			
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)	(13)	(14)	(15)
Subsystem 1 FPSO														
1.1 Disconnection mechanism	Allow for the FPSO to disconnect and evade when threatening icebergs approaches	Disconnecting and evacuating	Failure during disconnection	Stresses during disconnection (component failures)	Proof testing	FPSO can not disconnect and evacuate when commanded by IM team	The FPSO does not disconnect and evacuate when a threatening iceberg that exceeds certain kinetic energy drifts towards the FPSO [H1]	1	10	8	80	Fail-safe disconnection mechanism	FPSO	Ref 1.1.1
		Standby, waiting for command	Fail to start	Stuck due to frost, corrosion, etc.	Visual control, proof testing			3		3	90	Heating on critical components		Ref 1.1.2
				Electrical and mechanical component failures	Diagnostic test, proof test			6		5	300	Fail-safe disconnection mechanism		Ref 1.1.3 High frequency to account for all components
				Power failure	Hidden failure			3		5	150	More than one power source		Ref 1.1.4
1.2 Communication system	Allow for communication between IM team and FPSO	Continous operation, communicating or standby	Fail to function	Electrical and mechanical component failures	Diagnostic test, proof test	FPSO can not receive command to disconnect and evacuate		6		5	300	More than one communication system		Ref 1.2.1 High frequency to account for all components
				Power failure	Hidden failure			3		5	150	More than one power source		Ref 1.2.2

Figure 4.2: FMECA worksheet subsystem 1 FPSO



Desciption of unit			Description of failure			Effect of failure		Risk				Risk reducing measure	Responsible	Comment
Ref. no	Function	Operational mode	Failure mode	Failure cause	Detection of failure	On the subsystem	On the system function	Frequency	Severity	Detectability	RPN			
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)	(13)	(14)	(15)
Subsystem 3 Observation														
3.1 Sensor platform	Gather information about approaching icebergs, and send relevant information to IM team, IMV and FPSO	Continous operation and collection of data	Failt to function, data not collected or transmitted	Electrical and mechanical component failures	Diagnostic testing	Observation system with its three sensor platforms do not have fewer pieces of information	IM team, IMV and FPSO do not have necessary information. [H1, H2, H3 and H4] is more likely	4	6	4	96	Do not rely on data from all sensor platforms. More conservative, disconnect sooner with less information	IM team	Ref 3.1.1 High frequency to account for all components
			Failt to function, data improperly collected or transmitted	Data not transmitted or collected nominally due to weather conditions	Diagnostic testing		IM team, IMV and FPSO do not have all necessary information. [H1, H2, H3 and H4] is more likely	6	4	2	72	Do not rely on data from all sensor platforms		Ref 3.1.2 Lower severity since some information is available

Figure 4.3: FMECA worksheet subsystem 3 Observation



Desciption of unit			Description of failure			Effect of failure		Risk				Risk reducing measure	Responsible	Comment
Ref. no	Function	Operational mode	Failure mode	Failure cause	Detection of failure	On the subsystem	On the system function	Frequency	Severity	Detectability	RPN			
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)	(13)	(14)	(15)
Subsystem 2 IMVs														
2.1 IMV Engine	Convert fuel into motion so that the IMV can move.	Providing water cannon/towing	Engine failure when running or fail to start	Electrical and mechanical component failures (filiters, hoses, water pump impeller, etc.)	Diagnostic test, proof test	Engine capacity reduced, i.e. reduced ice management capacity	The IMV provides less efficient water cannon/towing. [H1 and H3] is more likely.	5	6	5	150	Standby IMVs, regular maintenance, proof testing and diagnostic testing	IMV	Ref 2.1.1 High frequency to account for all components
				Power failure	Hidden failure			3		6	108	More than one power source		Ref 2.1.2
2.2 Communication system	Allow for communication between IM team and FPSO	Continous operation, communicating or standby	Fail to function	Electrical and mechanical component failures	Diagnostic testing	IMV can not receive command to provide water cannon/towing	The IMV does not provide water cannon/towing. [H1] is more likely.	6	8	4	192	More than one communication system		Ref 2.2.1 High frequency to account for all components
				Power failure	Hidden failure			3		6	144	More than one power source		Ref 2.2.2
2.3.1 Water cannon	Protect the FPSO by providing water cannon/towing on an iceberg long enough to change its trajectory from threatening to non-threatening	Water cannon activated or on standby	Fail to function	Water cannon does not manage to pump water (weather)	Visual	IMV may not chose between water cannon/towing as suited. Must sometimes use least efficient method to manage icebergs	The IMV provides less efficient water cannon/towing. [H1 and H3] is more likely.	5	6	1	30	Training		Ref 2.3.1.1
			Fail to start	Electrical and mechanical component failures	Diagnostic testing			5		5	150	More than one water cannon		Ref 2.3.1.2 High frequency to account for all components
2.3.2 Towing system		Towing system activated or on standby	Fail to function	Towing system breaks, to much force (waves/IMV speed)	Visual			5		1	30	Training		Ref 2.3.2.1
			Fail to start	Electrical and mechanical component failures	Diagnostic testing			5		5	150	More than one towing equipment		Ref 2.3.2.2 High frequency to account for all components

Figure 4.4: FMECA worksheet subsystem 2 IMVs

Table 4.1: Risk Matrix

Frequency/ Consequence	Very unlikely	Remote	Occasional	Probable	Frequent
Catastrophic	2.2.2	2.2.1	1.1.3, 1.2.1		
Critical	1.1.1, 1.1.2	1.1.4, 1.2.2	2.1.2, 2.3.1.2, 2.3.2.2		
Major	3.1.1	2.1.2			
Minor	2.3.1.1, 2.3.2.1	3.1.2			

Table 4.2: Ranking of RPNs

Reference	1.1.3	1.2.1	2.2.1	1.1.4	1.2.2	2.1.1	2.3.1.2	2.3.2.2
RPN	300	300	192	150	150	150	150	150
Reference	2.2.2	2.1.2	3.1.1	1.1.2	1.1.1	3.1.2	2.3.1.1	2.3.2.1
RPN	144	108	96	90	80	72	30	30

As the FMECA worksheets are completed, it is straight forward to see which references that have the highest RPN as shown in Table 4.2 and place these in a risk matrix as shown in 4.1. Here we can easily see which parts of the system identified by the FMECA that should be prioritised, and evaluate these up against the actual cost of to determine which risk-reducing measures that should be implemented. If the analysis were not on such a high-level, a lot of details about component failures in the different subsystems would have been revealed as well. All critical failures identified by the FMECA, and all failures with an RPN of 150 and higher, are related to electrical and mechanical component failures.

New technology introduces new types of hazards. Introduction of digital technology is an example affecting most sectors, automated systems and complex relationships with humans introduces to new types of human errors, the complex interaction between components and software design errors. Traditional hazard identification methods such as FMECA are not adequate to analyse modern complex sociotechnical systems, as it is best suited to identify component failures etc. The need for a new method for hazard identification are given in Chapter 5 *STPA*.

Chapter 5

System-Theoretic Process Analysis (STPA)

This chapter is mainly based on the works done by Professor Nancy G. Leveson.

1. Her book *Engineering a Safer World: Systems Thinking Applied to Safety* (Leveson, 2012) which describes the need for a new accident causation model such as STAMP (Systems-Theoretic Accident Model and Processes), and among other concepts and an older version of STPA (System-Theoretic Process Analysis).

2. The *STPA Handbook* (Leveson and Thomas, 2018) for the newest version of STPA to date.

This chapter is merely a summary. For a better and more in-depth understanding of the theory described in this chapter, the literature mentioned above is highly recommended. To describe STAMP and STPA precisely, it is essential to have a clear and mutual understanding of what is meant using different terms, in Appendix C different definitions are listed. An earlier version of this chapter was given in my project thesis (Nesse, 2019).

5.1 Modern Complex Sociotechnical Systems

Technology is in continuous advancement, and companies that do not innovate are in danger of becoming obsolete. New products and systems must reach the market much faster than before, which leads to less time for testing. Radical innovations render past experiences more or less obsolete. Priorities throughout design processes must be made with less information, and it is more expensive to step wrong than ever before. New technology introduces new types of hazards. Introduction of digital technology is an example affecting most sectors, automated systems and complex relationships with humans presents new kinds of human errors, complex component interactions and software design errors.

Traditional hazard identification methods such as FMECA are suggested in Section 7.1 to not be adequate to analyse modern complex sociotechnical systems. In his review of accident modelling approaches for complex sociotechnical systems Qureshi (2007) highlights the first version of STAMP (Leveson, 2004) and the hierarchical model of the sociotechnical system (Rasmussen, 1997), which STAMP is built on, as two notable systemic modelling approaches. Since this, the STAMP model has been refined, but the method's purpose is still the same; to meet the challenges of handling risk in ever-increasing complex systems.

Leveson argued that a new basis for safety engineering was needed as summarised in Table 5.1 to fully comprehend modern complex sociotechnical systems. Based on these new assumptions, Leveson was determined that new types of hazard analysis and risk assessments were necessary. A new model would have to acknowledge the complex role of software and humans in modern sociotechnical systems, consider processes and not just events and conditions that lead to accidents, understand what shapes human behaviour and decision making and be capable of identifying system design errors and dysfunctional system interactions.

Table 5.1: The basis for a new foundation for safety engineering. Taken from (Leveson, 2012)

Old Assumption	**New Assumption**
Safety is increased by increasing system or component reliability; if components do not fail, then accidents will not occur.	High reliability is neither necessary nor sufficient for safety.
Accidents are caused by chains of directly related events. We can understand accidents and assess risk by looking at the chains of events leading to the loss.	Accidents are complex processes involving the entire sociotechnical system. Traditional event-chain models cannot describe this process adequately.
Probabilistic risk analysis based on event chains is the best way to assess and communicate safety and risk information.	Risk and safety may be the understood and communicated in ways other than probabilistic risk analysis.
Most accidents are caused by operator error. Rewarding safe behaviour and punishing unsafe behaviour will eliminate or reduce accidents significantly.	Operator error is a product of the environment in which it occurs. To reduce operator "error" we must change the environment in which the operator works.
Highly reliable software is safe.	Highly reliable software is not necessarily safe. Increasing software reliability will have only minimal impact on safety.
Major accidents occur from the chance simultaneous occurrence of random events.	Systems will tend to migrate toward states of higher risk. Such migration is predictable and can be prevented by appropriate system design or detected during operations using leading indicators of increasing risk.
Assigning blame is necessary to learn from and prevent accidents or incidents.	Blame is the enemy of safety. Focus should be on understanding how the system behaviour as a whole contributed to the loss and not on who or that to blame for it.

5.2 STPA Foundation – STAMP

STAMP is the foundation of which STPA and CAST (Causal Analysis based on Systems Theory) is built. Based on the new assumptions in Table 5.1 and goals set by Leveson for a new accident model STAMP was developed. Generally, accidents are viewed as a control problem and not a failure problem as in reliability engineering. However, hazards due to component failures are included. In STAMP the focus in system safety changes from preventing failures to implementing safety constraints. The goal is to have adequate control so that the safety constraints are followed. The three main concepts of STAMP are *1) Safety constraints*, *2) Hierarchical control structures* and *3) Process models.*

Safety Constraints

Instead of decomposing the system based on events and components, the fundamental element of STAMP is the constraint. Accidents occur due to lack of control. We use constraints on how parts of a system can act, and interact with other parts of the system. Safety constraints are imposed to prevent accidents and hazards, e.g. to make sure that a boiler does not exceed a given temperature, or that an automated vehicle does not speed. When accidents occur, it is because we did not manage to control the temperature of the boiler, or the speed of the vehicle, i.e. the safety constraint was violated due to lack of control.

Hierarchical Control Structures

In STAMP systems are modelled as hierarchical control structures. Modern systems may consist of very large organisations, and there might be hundreds, or even thousands of people, involved in a project. Leveson argued that a new holistic approach to safety, based on control and enforcing safety constraints in the entire sociotechnical system is needed to ensure safety. Figure 5.1 shows an excerpt of a hierarchical control structure, and the whole organisation and legislators could have been included in this control.

To successfully have a holistic approach, system-level constraints are essential. Public opinion or politicians might call for certain criteria for oil and gas in the Arctic, which might lead to ISO (International organisation for Standardisation) developing standards such as *ISO 19906:2010, Petroleum and natural gas industries – Arctic offshore structures.* Leveson argues that system-level constraints must be identified, and responsibility for enforcing them must be divided up and allocated to appropriate groups. In such standards, one may do just that.

Each level in the hierarchy imposes constraints on the level below. Lower levels may perform actions within these constraints, and if the constraints are well designed, the system will remain safe. The arrows going down are the constraints given from a higher to a lower level in the hierarchy, also called control action, and the arrows going up is the feedback which enables

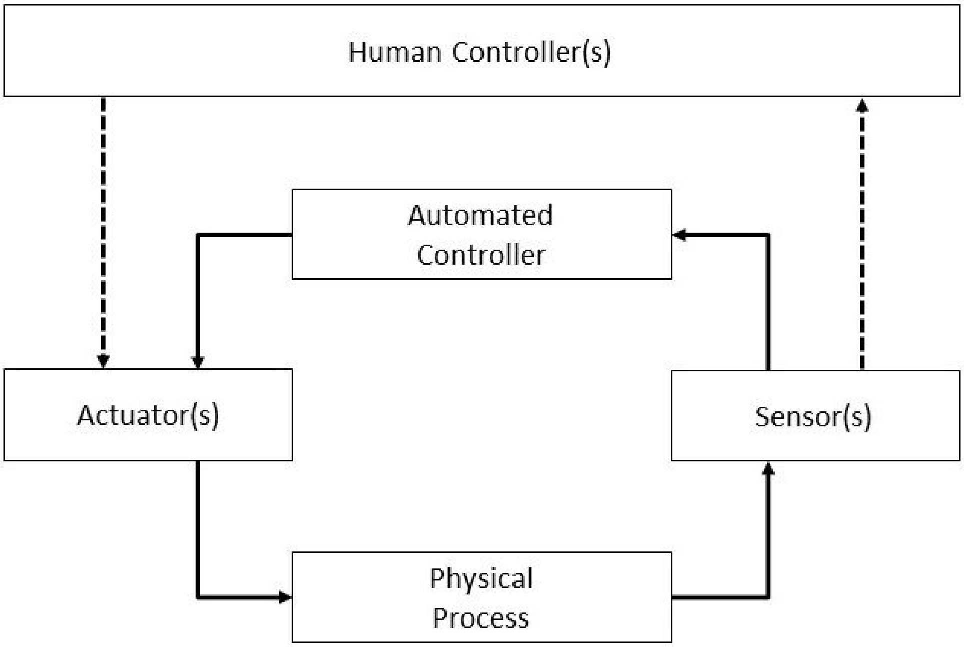


Figure 5.1: Excerpt of a sociotechnical control, adapted from (Leveson, 2012)

control. Feedback might show that the constraints imposed, e.g. by the standards are not efficient, perhaps they are not being followed, maybe they are being followed but not working, and might need to be adapted.

Process Models

Process models are the final central concept of STAMP in addition to safety constraints and hierarchical control structures. In STAMP systems consist of controllers, actuators (control actions), sensors (feedback loops) and controlled processes as shown in 5.2. An important aspect in STAMP is that controllers can be both automated and human, i.e. the process models should not only be physically described in automated controllers, but human process models must also be considered. The mental model that shapes human behaviour and decision-making of a human controller must also be considered to be a process model (Teikari, 2014). Leveson argues that process models play an important role in understanding why accidents occur and why humans provide inadequate control over safety-critical systems and in designing safer systems.

Accidents in STAMP occur due to lack of control. To control a process such as the one in Figure 5.2, four conditions adapted from Leveson (2012), must be in place:

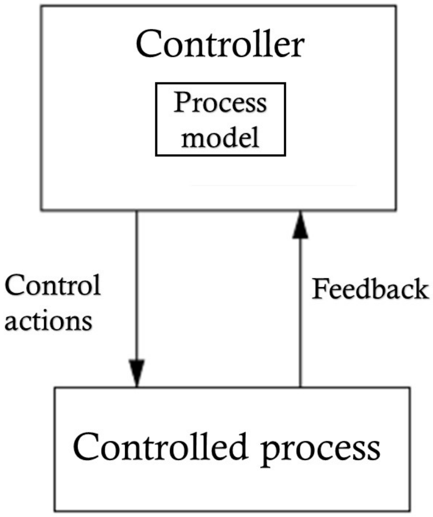


Figure 5.2: Simple process model, adapted from (Leveson, 2012)

- *Goal condition*: The controller must have a defined goal to navigate after, which in STAMP is the safety constraint.
- *Action Condition*: The controller execute control actions using actuators in order to adjust the system so it does not violate safety constraints.
- *Model Condition*: The controller must have a model of the system, in order to know which control actions to impose.
- *Observability Condition*: The controller must receive feedback from sensors that observes the real system or other pieces of information, to verify the model

Accidents occur when one or more of these conditions are not in place. The controller needs to know how different parts of the system interacts, the current state of the system, and how to change the system. The process model is rarely a perfect copy of the real system, and textbooks on basic control theory such as Balchen et al. (2004) describes many issues that can lead to instability, delayed feedback, etc. When the process model is incorrect, our control actions might be inadequate, leading to instability in the system and accidents. It takes time to see the effects of the control actions, and it takes time to update the process model with feedback from sensors. We might end up initiate incorrect or unsafe control actions, or not initiate them at all. We might initiate control actions too early or too late, or even activate the actuators too long or too short so that they do not have the intended effect. For an accident to occur, the safety constraints must be violated in one or more ways, also described in the STPA process for how to identify UCAs.

5.3 STPA Overview

STPA is a proactive hazard identification method built on STAMP. The main objective is to identify unsafe control actions and derive safety constraints. Since STAMP applies to any emergent property, STPA may also be used for any system property. STPA is an efficient tool to find possible causes to accidents and may be used to identify methods to eliminate or control these hazards. Section 5.2 describes the foundation of STPA.

The STPA method was revised by Leveson and Thomas (2018), and there is not much literature applying the newest version of STPA yet. However, this does not mean that previous work has been in vain. STPA is still interesting for many sectors and domains. "Application areas have included aviation, air traffic control, space, defence, the automotive industry, railways, chemicals, oil and gas, medical devices, health-care, and workplace safety, with a growing interest coming from new areas such as the pharmaceutical industry and the finance and insurance sectors. Ongoing developments aim at extending the application field of STPA to include security (Björnsdóttir, 2017)."

STPA is also a top-down approach and may be used throughout the whole life-cycle of a system. STPA is particularly useful in assisting system design and development, as it can be created on a system-level, and add more details as throughout the project as more information becomes available. Another interesting part of STAMP and STPA is that traditional hazard analysis may be integrated into these analyses.

Similarly to STAMP, the system is viewed as a control structure. Human minds manage complexity through abstraction and hierarchy. Therefore it is rather practical to have a top-down process where we start at a high abstract (system-level). The control structure shows all our system interactions, control actions and feedback. The goal of STPA is to classify unsafe or inadequate control actions, and analyse why these are flawed and dysfunctional system interactions.

How do the control actions themselves lead to hazards? In STPA, we deduce the control structure into more detail (or refine it for preliminary analysis), adding detail creating process models for each relevant controller. The control actions are also analysed to see how they might contribute to hazards, and we determine how they might occur, and recommendations are given to mitigate these flaws. In the process, we refine accidents and unacceptable losses, function hazards and function-level constraints and requirements. More details on the STPA process is given in Section 5.5.

5.4 STPA Advantages and Limitations

For STPA, that is built on STAMP, the many advantages and limitations are similar. Table 5.2 shows the advantages and limitations of STPA, many of which also apply to STAMP.

Table 5.2: Advantages and limitations STPA

Advantages	**Limitations**
STPA works on very complex systems because it works top-down rather than bottom up, and may be used even if there is limited knowledge about the system	Systems are getting so complex that it is beyond our capability to successfully create effective system safety constraints and predict all interactions.
STPA considers more causal factors than traditional approaches such as software, humans, organisation, safety culture in accidents and other types of losses without having to threat them differently or separately.	STPA are by no means the only way to identify new causes to accidents and hazards. A very skilled team may take into account all causes with a traditional approach as basis.
Theoretically more flaws could be found, as STPA and STAMP accounts for more factors. “Unknown unknowns” that were previously only found in operations can be identified	STPA may be rather time consuming, especially if the system is not very complex. For simple systems traditional methods still more than good enough.
STPA does not require extensive domain experience of the system analysed, as guidance on how to identify unsafe control actions are provided	Broad experience on the STPA method itself is required. The analysis can be time-consuming, especially if analysts are inexperienced
STPA provides documentation of system functionality that is often missing or difficult to find in large, complex systems. Traceability is also rather straight-forward, making it easier refine the analysis as more detailed design becomes available	STPA may need to take use of other risk assessment approaches when a quantitative results are needed to decide between tradeoffs

5.5 STPA Process

There are several possible uses of STPA, but most steps are similar for all applications. The *STPA Handbook* describes the STPA process by the use of four steps. 1) Define the purpose of the analysis, 2) Model the control structure, 3) Identify unsafe control actions and 4) Identify loss scenarios.

Step 1 and 2 are in practice identical with what the four steps I described as the STAMP process in my specialisation project Nesse (2019), here named step 1. Step 1 is equal to all applications of STPA. Step 3 and 4 in the *STPA Handbook* correspond to step 2 and 3 here. The last step is the only one that varies depending on the application of the STPA analysis. Here I have also added a fourth step of refining the analysis and the fifth step about documentation and implementation of the results.

Step 1: Build or Refine a Control Structure

It is a good idea to make use of domain experts in the first step of STPA, creating or refining the control structure. If a control structure already is in place, this should be refined to match the purpose of the STPA analysis. This first step is the whole STAMP process and is needed to determine why accidents occurred (CAST) and to determine how accidents can be avoided (STPA). To create a control structure, this must be done:

Identify system-level accidents and unacceptable losses. The first step is to find all these, and possible sources might be laws, standards or regulations governing our domain, goals set by management, etc. These might be ranked according to the level of severity to be used in trade-offs among goals later on. This may be listed, as shown in Table 6.1 in the case study. There is no correct or wrong amount of accidents and unacceptable losses in a list such as this.

Identify system-level hazards: To continue with the second step system boundaries must be defined, so that the list of system-level hazards are relevant. Hazards should not refer to individual components of the system, but the overall system and system state. Also, the hazards should refer to factors that can be controlled or managed by the system, and this can be organised in a list, as shown in Table 6.2 in the case study. Since system-level hazards are high-level, there should not be too many of them. If there is more than 10, one is probably not classifying hazards correctly.

Identify the system-level constraints and requirements: After the system-level hazards have been identified, the next step is to specify the safety requirements and the constraints that are needed to prevent hazards from taking place. This may be organised in a list such as Table 6.3 in the case study.

Develop the hierarchical control structure and list responsibilities: After identifying system-level accidents and unacceptable losses, hazards, requirements and constraints the control structure should be built, as shown in Figure 6.1 in the case study. It is important to note that there is not one correct hierarchical control structure, but it is important to include which controllers are responsible for implementing what requirements. Control actions are the tools used to enforce the requirements, and feedback loops are necessary to control that the controllers are maintaining the process models as intended. A separate list could be made listing all the responsibilities, such as the one shown in Table 6.4.

For the first high-level construction of a control structure, we do not go into all details, and more information is likely to be added in revisions. Arrows going down are the constraints that a higher level may impose on a lower level (control actions), and the arrows going up are is different sorts of information given from a lower level to a higher level to enable control (feedback). Labels of control actions and feedback should be as specific as possible and contain functional information that is sent. All controlled physical processes should be controlled by at least one controller, and responsibilities should be reviewed wherever there is overlap (conflicts) or boundaries (risk of neglecting responsibilities).

The control structure may be different depending on the type of system analysed. Finishing up the control structure one should check that all control actions and feedback needed to satisfy responsibilities are included, which sometimes is not available in the early stages of design. To complete an STPA, the following steps are also required:

Step 2: Identify Unsafe Control Actions and Constraints

This step will be the same for all applications of the STPA analysis. Using the information from the first step, causal factors should be classified, and one should deduce reasons for flawed control and dysfunctional interactions. Here we attempt to identify all unsafe control actions that may lead to the system-level hazards and system-level losses defined in the first step. These unsafe control actions may be used to investigate necessary functional requirements and constraints further.

There are several causes of accidents. For each control action, we must evaluate whether or not some of them can be unsafe in specific contexts:

1. The controller provides an unsafe control action. Four types of unsafe control actions are possible:
   (a) A control action necessary for safety is not provided
   (b) An unsafe control action is provided, which leads to hazard
   (c) A control action necessary for safety is provided too late, too soon, or out of sequence
   (d) A control action necessary for safety is stopped too soon or applied too long
2. Appropriate control actions were provided but not followed

The UCAs may then be listed as shown in Table 6.6 or Table 6.7 in the case study. Here we see how each control action may be unsafe with respect to the list above. A UCA should not be confused with the causes of a UCA, nor should the UCA context be confused with the UCA outcomes. All UCAs should be related to a system-level hazard, and if they are not, some system-level hazards have probably not yet been identified. When we have deduced all the unsafe control actions, this is used to identify controller constraints corresponding to each UCA, as shown in Table 6.8 in the STPA case study. After completing the second step, we have everything we need to identify loss scenarios.

Step 3: Identify Loss Scenarios and Countermeasures

From the second step, we have identified UCAs and controller constraints, and in this step, we should define the loss scenarios. The *STPA Handbook* describes two types of loss scenarios:

1. Why would UCAs occur?
2. Why would control actions be improperly executed or not executed?

The first question is related to the feedback loop of the process model (upward arrows). Scenarios that deduce why UCAs could occur could start with going backwards and determining the causes the control action to act or not act. Failures could be related to the (physical) controller (e.g. component failure or lack of power), inadequate control algorithms (e.g. flawed algorithms or implementation of these), unsafe control input or inadequate process models (e.g. incorrect feedback, wrong interpretation of feedback or delays in feedback).

The second question is related to the control action part of the process model. Scenarios that deduce why control actions may be improperly, or not executed at all, can also be caused by UCAs. When deducing such scenarios, factors that affect the controlled path is of importance (downward arrows). Reasons to that control actions are not executed may be, e.g. that the actuators do not receive the information to perform a control action, or that the signal is received, but the actuator for different reasons fail to respond. Control actions may be improperly executed when information sent by the controller or received by the actuator is misinterpreted, or even if a signal that is not transmitted is registered.

One of the changes made to STPA in the *STPA Handbook* is the model to deduce causal scenarios/loss scenarios, and it is referred to the handbook for a more detailed description how to use this model. The most eye-catching difference is that automated and human controllers have been separated, and proves to be useful in causal scenario generation. This change is a testament to the significance of human behaviour. Analysts using this model (by the book) are forced (or helped) to consider factors that shape human behaviour, which may be very difficult to do without a structured way to do so.

Step 4: Refine Step 1-3 if Necessary

Step 4 is just another iteration of step 1–3. For an instance where STPA is used in a design process, step 4 (i.e. refine step 1–3) should be done for every step of the process shown in Figure 5.3. For each step, more information becomes available, and we should refine STPA analysis, including all steps. This is how STPA may be used to give recommendations in the development of a project.

This process of refining the steps should not only be done in these cases. When we go further into the details of the analysis, we can create specific control loops in more detail, making subhazards etc., and we should make sure that everything we did on the system-level still is valid. It might also be smart to involve a team of experts to review what the analyst has done. Domain expertise is not necessary for the analyst to perform the STPA analysis, but input from those with that expertise will be beneficial.

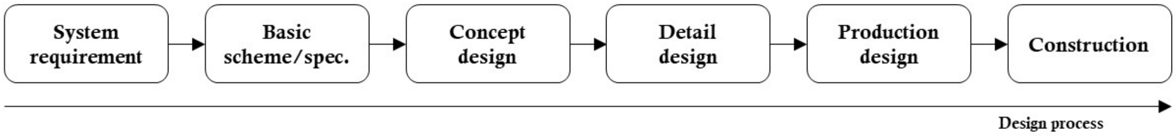


Figure 5.3: Standard design process, STPA should be refined for each step

As previously mentioned, STPA has a broad area of application. Steps 1–3 should also be refined, e.g. when a manufacturing process is to be changed, or when operations changes. There might also be smart to check from time to time whether or not the STPA analysis is adequate. Over time at least human controllers tend to adapt their behaviour, and we might discover that the system constraints no longer are sufficient (i.e. that they never were).

Step 5: Documentation and Implementation of Results

For each step of, e.g. the design process, the results should be implemented before proceeding to the next phase. Recommendations should be made in the development of a design. Documentation should be available so that, e.g. changes in manufacturing, operation, etc. can be included in the STPA analysis. For such cases, the analysis must be refined, and step 4 (i.e. refine step 1–3) should be executed for the new conditions. One of the advantages of STPA concerning complex systems is related to traceability. The process of labelling hazards, losses, UCAs may prove useful when changes to the design are made, and older STPA analysis needs to be revisited for revision.

Chapter 6

Case Study: STPA in Ice Management

In this chapter, I will perform an STPA analysis, as described in Chapter 5. The purpose of this analysis is to protect an FPSO (Floating Production, Storage and Offloading) from a collision with icebergs to ensure steady production, and prevent the defined losses defined in Table 6.1. System boundaries are set to include the FPSO, IMVs (Ice Management Vessels), sensor platforms for ice monitoring (Observation) and the area being monitored. Weather forecasts are external.

This case study has some limitations, as described in Subsection 1.5. It is assumed that the FPSO is located in an area not infested by sea ice and that the only threatening ice feature is icebergs. The literature study has focused on ice management in general and STPA in particular. The objective of conducting this case study is to learn more about the STPA methods applicability to similar problems, and not to conduct a complete in-depth study. The problem is to complex to do so in a master thesis adequately. The case study is held to a high-level.

6.1 Step 1: Build or Refine a Control Structure

To conduct an STPA analysis, we need to build a high-level control diagram. As described in 5, we first need to identify losses, system-level hazards and system-level constraints. It is a good idea to make use of domain experts in the first step of STPA, creating or refining the STAMP model. Since the case study is performed on a high-level, discussions made with my supervisors were considered to be sufficient.

Identify System-Level Losses

In Table 6.1 losses have been limited to five general losses L.1, L.2, L.3, L.4 and L.5. These are defined to protect human beings such as employees, the environment, equipment used for both production and ice management, production and the IMVs limited time resources.

Table 6.1: System-level losses

Loss ID	Description
L.1	Loss of life or injury to people
L.2	Environmental loss
L.3	Loss of equipment or damage to equipment (FPSO, IMVs, sensors)
L.4	Loss of production
L.5	Loss of time or waste of ice management capacity

The first four losses were identified immediately. However, the final loss, L.5, were added during the process of creating UCAs. It seemed to be trivial to avoid L.1 to L.4 with unlimited ice management capacity, and unnecessary to manage non-threatening icebergs as well. It is costly to have IMVs protecting the FPSO and to ensure a more realistic case it had to be a goal to minimise or optimise then needed ice management capacity, or at least not to waste it. Another concern was that it would be unsafe to have IMVs occupied with non-threatening icebergs instead of threatening icebergs. Therefore adding L.5 could also help to increase the likelihood of avoiding L.1 to L.4.

Identify System-Level Hazards

In Table 6.2 four system-level hazards have been identified. To ensure stable production, it is important that the FPSO does not evade needlessly, and it is important that the FPSO evades in good time when a threatening iceberg does approach.
<Hazard> = <System> & <Unsafe Condition> & <Link to Losses>.

Table 6.2: System-level hazards and corresponding losses

Hazard ID	Description	Loss ID
H.1	A threatening iceberg that exceeds certain kinetic energy drifts into the FPSO, and the FPSO does not disconnect and evade	L.1, L.2, L.3, L.4
H.2	The FPSO disconnect and evade when there is no threatening iceberg that exceeds certain kinetic energy and no other emergency requiring disconnection	L.4
H.3	The IMVs use water cannon or towing on non-threatening icebergs	L.5
H.4	The IMVs use water cannon or towing in dangerous weather	L.1, L.3, L.5

The process of identifying system-level hazards was more challenging than that of losses. It is tempting to define more hazards and more detailed hazards. However, as described in Chapter

5, creating detailed hazards at this stage of the STPA makes it easier to overlook relevant UCAs and loss scenarios. Since the whole case study is conducted on a high-level, sub-hazards are not identified at a later stage.

I ended up with three high-level hazards H.1 to H.3, but while identifying loss scenarios, I realised that there were scenarios that could lead to loss of life or injury to people (L.1) and loss of equipment or damage to equipment (L.3) without these three hazards being relevant. Use of IMVs and water cannon/towing in dangerous weather conditions can lead to L.1 and L.3, and since the use of water cannon/towing often is inefficient, it also leads to loss of time or waste of ice management capacity (L.5). A fourth hazard H.4 were included.

Identify System-Level Safety Constraints

In Table 6.3 five system-level safety constraints have been identified, which are linked to the system-level hazards. To prevent losses, IMVs must manage all threatening icebergs, and the FPSO must only evade when threatening icebergs are approaching the FPSO. Also, the IMVs must not manage icebergs in dangerous weather conditions. The focus in this master thesis is on ice management, so other hazards such as storms, drifting vessels, etc. in SC.3 that also could require the FPSO to disconnect and evade is not considered. The fifth safety constraint was added as a consequence of adding H.4.
<Safety Constraint> = <System> & <Condition to Enforce> & <Link to Hazards>.

Table 6.3: System-level safety constraints and corresponding hazards

Safety Constraints	Description	Hazard ID
SC.1	The IMVs must prevent threatening icebergs from drifting into the FPSO	H.1
SC.2	The FPSO must disconnect and evade when a threatening iceberg cannot be managed by IMVs	H.1
SC.3	The FPSO must never disconnect and evade when all icebergs are non-threatening	H.2
SC.4	The IMVs must never use towing or water cannon on non-threatening icebergs	H.3
SC.5	The IMVs must never use towing or water cannon in dangerous weather	H.4

Develop or Refine the Hierarchical Control Structure and List Responsibilities

With the information obtained when defining the system boundaries, identifying losses, system-level hazards and system-level constraints, a preliminary version of the high-level control diagram in Figure 6.1 was made. In the later stages of the analysis, it would be possible to add more detail to the control diagram and create more control diagrams. Sub-hazards and sub-constraints could also be made in later stages to ensure that all is thought of when we are planning to prevent all losses in Table 6.1. However, this STPA has been limited to high-level analysis.

In Table 6.4 responsibilities for the IM team, IMVs and FPSO have been listed. The responsibilities R.1a and R.1b are related to the control action *water cannon/towing*, similarly R.2a and R.2b are related to the control action *disconnect and evacuate*. Only the ice management (IM) team commands control actions, but the IMVs and FPSO have a responsibility to act as well. Table 6.5 shows the derived feedback based on the responsibilities, and Figure 6.1 have been updated accordingly after several iterations.

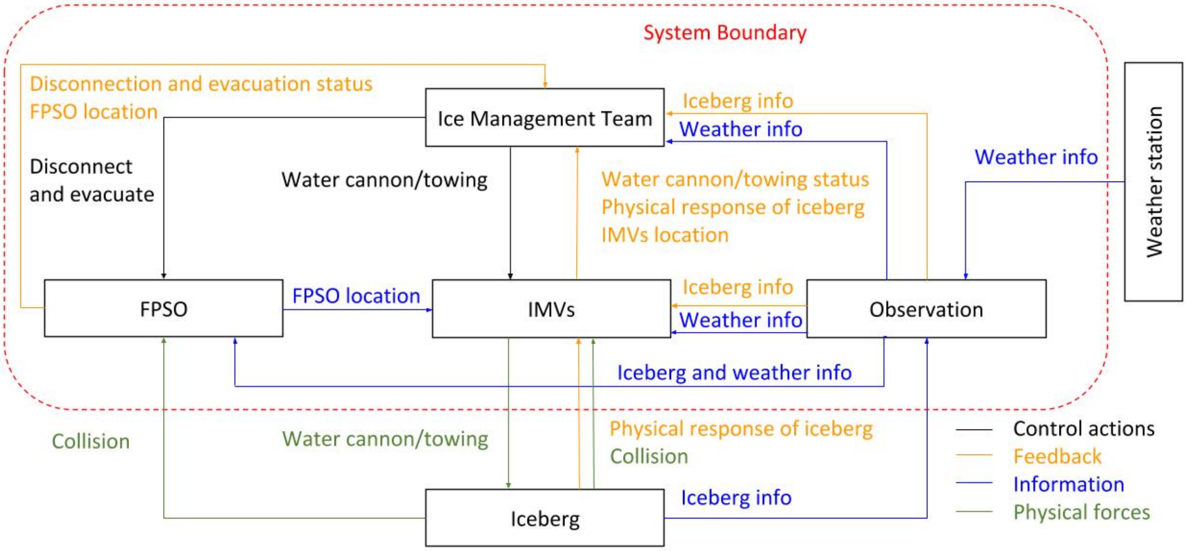


Figure 6.1: High-Level Control Diagram

In addition to the IM team and icebergs, the system consists of three parts – the FPSO, IMVs and Observation (sensor platforms for monitoring icebergs). It as assumed that the sensor platforms are autonomous, and themselves collect the data, or that someone outside the system boundaries does so. Different parts of the data about icebergs are sent to different parts of the system, as shown in Table 6.5, even though the figure may suggest that the same iceberg information is sent to all parts of the system. Weather conditions are also monitored outside the system boundaries, but available to both IM team, FPSO, IMVs and Observation.

Feedback is here understood as a reaction (or a result) of a control action, and *information* is just information not related to a control action (e.g. weather condition). Therefore, e.g. the location of FPSO is considered to be feedback to the IM team, but only information to the IMV. Similarly, data about the icebergs are considered to be information to the FPSO, but feedback to both the IM team and IMV. Weather conditions could arguably be feedback instead of information to both the IM team and IMV in some cases since it could imply dangerous weather conditions and that the IMV should not provide water cannon/towing. However, most of the time weather conditions are just information, so it is shown like that in the figure.

Table 6.4: Responsibilities and corresponding system-level safety constraints

Responsibilities	Description	Safety Constraints
R.1a R.1b	**IM team:** Request IMV to provide water cannon/towing when needed and conditions are safe **IMV:** Provide water cannon/towing when requested by IM team and conditions are safe	SC.1, SC.4, SC.5
R.2a R.2b	**IM team:** Request FPSO to disconnect and evacuate when needed **FPSO:** Disconnect and evacuate when requested by IM team	SC.2, SC.3

6.2 Step 2: Identify Unsafe Control Actions and Constraints

As shown in Chapter 5, there are several ways a control action can be unsafe. The process of identifying UCAs have been challenging. At first, over 20 UCAs were discovered, but this has been reduced to 11 final UCAs as many have been removed or merged with other UCAs.

During the process of identifying loss scenarios, some of these UCAs appeared to overlap with other UCAs, while some UCAs were inverse duplicates. I.e. in Figure 6.1 there are only two control actions, where the first control action is the IM team requesting the FPSO to disconnection and evacuate, and the second control action being the IM team requesting IMVs to use water cannon/towing. I have made one table listing UCAs for each control action. However, loss scenarios are not only related to the request being sent or not by the IM team, but also whether or not the FPSO and IMVs act and provide the control action when requested (or act when they are not requested to do so etc.). It took some time, but I realised that this was not two different UCAs, but rather one UCA with more loss scenarios.

Many UCAs were merged into more general UCAs, but to identify loss scenarios, my initial mistake of identifying too many UCAs became helpful. I thought of each UCA as two different

Table 6.5: Feedback derived from responsibilities

Responsibilities	**Process Model**	**Feedback**
R.1a [SC.1, SC.4, SC.5]	*IM team:* Request IMV to provide water cannon/towing when needed and conditions are safe	- Weather conditions - Present location icebergs - Size of all icebergs - Trajectory of all icebergs - Speed of all icebergs - Present location of IMVs - Water cannon/towing status - Present location of FPSO
R.1b [SC.1, SC.4, SC.5]	*IMV:* Provide water cannon/towing when requested by IM team and conditions are safe	- Weather conditions - Present location of all threatening icebergs - Size of said icebergs - Trajectory said icebergs - Speed of said icebergs - Present location of FPSO
R.2a [SC.2, SC.3]	*IM team:* Request FPSO to disconnect and evacuate when needed	Feedback R.2a = R.1a
R.2b [SC.2, SC.3]	*FPSO:* Disconnect and evacuate when requested by IM team	- Weather conditions - Present location of all threatening icebergs - Speed of said icebergs

UCAs when identifying loss scenarios. Take UCA.1 as an example *Water cannon/towing is not provided when a threatening iceberg is approaching the FPS [H.1].* Here it was helpful to first identify the loss scenarios to when the control action was not provided because the IM team never sent the request to use water cannon/towing, but also for when the IMVs never provided the water cannon/towing even though the IM team requested it. All loss scenarios should have been identified anyways, but it was helpful to systematically first identify loss scenarios because of the IM team, and then loss scenarios because of the IMVs. STPA is not a straight forward method to use and requires a lot of training. It is not a given that I, as a newcomer to the STPA method would have identified as many loss scenarios for each UCA if I did not systematically work through them as I just described. This is one of the disadvantages of the STPA method.

Table 6.6: Unsafe Control Actions [R.1a and R.1b]

Control Action	**Not providing causes hazard**	**Providing causes hazard**	**Too early, too late, out of order**	**Applied too long or stopped too soon**
IM team: Request IMV to provide water cannon/towing when needed and conditions are safe [R.1a]	UCA.1: Water cannon/towing is not provided when a threatening iceberg is approaching the FPSO [H.1]	UCA.2: Water cannon/towing is provided on a less critical iceberg instead of a more critical iceberg [H.1, H.3] UCA.5: Water cannon/towing is provided in dangerous weather conditions [H.1, H.4] UCA.7: The least efficient method of water cannon/towing is used to manage an iceberg [H.1, H.3]	UCA.3: Water cannon/towing is provided too late, both iceberg or IMV may collide with FPSO [H.1]	UCA.4: Water cannon/towing is provided too long, potentially not enough time for other icebergs [H.1, H.3] UCA.6: Water cannon/towing is stopped too soon. Iceberg still threatening [H.1]

This finally resulted in 11 UCAs. In Table 6.6 we have identified 7 unsafe control actions UCA.1 to UCA.7 related to the control action *water cannon/towing*, i.e. responsibility R.1a and R.1b. In Table 6.7 we have identified 4 unsafe control actions UCA.8 to UCA.11 related to the control action *disconnect and evacuate*, i.e. responsibility R.2a and R.2b. For this case study, what happens during the evacuation of the FPSO is not included, i.e. the direction of evacuation, protection of FPSO after disconnection, etc. It is assumed that the evacuation is successful if the FPSO disconnects when it is supposed to.

Table 6.7: Unsafe Control Actions [R.2a and R.2b]

Control Action	**Not providing causes hazard**	**Providing causes hazard**	**Too early, too late, out of order**	**Applied too long or stopped too soon**
IM team: Request FPSO to disconnect and evacuate when needed and [R.2a]	UCA.8: Disconnection and evacuation is not provided when a threatening iceberg is approaching the FPSO [H.1]	UCA.9: Disconnection and evacuation is provided when a threatening iceberg is not approaching the FPSO [H.2]	UCA.10: Disconnection and evacuation is provided too early, when it is needed [H.2] UCA.11: Disconnection and evacuation is provided too late [H.1]	N/A

In Table 6.8 we have identified controller constraints (CCs) that are linked to the given UCAs. All controller constraints are accounted for in the later step of identifying loss scenarios and countermeasures (CMs), but there was no logical way to use the controller constraints in the process of identifying countermeasures. However, it was reassuring to see that the identified countermeasures were in compliance with the controller constraints.

Table 6.8: Controller Constraints

Unsafe Control Actions	**Controller Constraints**
UCA.1: Water cannon/towing is not provided when a threatening iceberg is approaching the FPSO [H.1]	CC.1: Water cannon/towing must be requested by IM team when it is needed CC.2: Water cannon/towing must be provided by IMV when commanded by IM team
UCA.2: Water cannon/towing is provided on a less critical iceberg instead of a more critical iceberg [H.1, H.3]	CC.3: Water cannon/towing must be requested by IM team for the most critical iceberg CC.4: Water cannon/towing must be provided by IMV on the most critical iceberg when commanded by IM team
UCA.3: Water cannon/towing is provided too late, both iceberg or IMV may collide with FPSO [H.1]	CC.5: Water cannon/towing must not be provided too late by IMV

UCA.4: Water cannon/towing is provided too long, potentially not enough time for other icebergs [H.1, H.3]	CC.6: Water cannon/towing must be stopped by IMV when the iceberg is non-threatening
UCA.5: Water cannon/towing is provided in dangerous weather conditions [H.1, H.4]	CC.7: Water cannon/towing must not be requested by IM team in dangerous weather conditions CC.8: Water cannon/towing must not be provided by IMV in dangerous weather conditions if commanded by IM team
UCA.6: Water cannon/towing is stopped too soon. Iceberg still threatening [H.1]	CC.9: Water cannon/towing must not be stopped by IMV when the iceberg is threatening, unless IM team requests water cannon/towing on a more critical iceberg
UCA.7: The least efficient method of water cannon/towing is used to manage an iceberg [H.1, H.3]	CC.10: Water cannon/towing must always be chosen so that the most efficient method is used, unless it is unsafe to use one method.
UCA.8: Disconnection and evacuation is not provided when a threatening iceberg is approaching the FPSO [H.1]	CC.11: Disconnection and evacuation must be requested by IM team when it is needed CC.12: Disconnection and evacuation must be provided by FPSO when commanded by IM team
UCA.9: Disconnection and evacuation is provided when a threatening iceberg is not approaching the FPSO [H.2]	CC.13: Disconnection and evacuation must not be requested by IM team when it is not needed CC.14: Disconnection and evacuation must not be provided by FPSO unless it is requested by IM team
UCA.10: Disconnection and evacuation is provided too early, when it is needed [H.2]	CC.15: Disconnection and evacuation must be requested by IM team late enough to not unnecessarily loose production CC.16: Disconnection and evacuation must not be provided by FPSO earlier than requested
UCA.11: Disconnection and evacuation is provided too late [H.1]	CC.17: Disconnection and evacuation must be requested by IM team early enough to be able to conduct it safely CC.18: Disconnection and evacuation must not be provided by FPSO later than requested

6.3 Step 3: Identify Loss Scenarios and Countermeasures

Loss scenarios have been identified for all UCAs, as described in Chapter 5. As mentioned in Section 6.2 some UCAs were removed during the process if identifying loss scenarios. For each of the UCAs between 16 and 30 loss scenarios were identified, a total of 243, which are summarised in Table 6.11. An excerpt of the loss scenarios and countermeasures related to UCA.1 are presented in Table 6.10 as an example. All loss scenarios are presented in Appendix D.

At first loss scenarios were only named *LS.1-UCA.1, LS.2-UCA.1, ..., LS.30-UCA.1,* which seemed systematic enough in the spreadsheet where I had all UCAs and loss scenarios. Every UCA had its column, where each row represented a separate cause of each loss scenario. When I organised all these loss scenarios in tables for each UCA, systematic information about the causes of each loss was lost. It seemed impossible to go over all the loss scenarios and control them after I had moved them over to tables. To ensure that the STPA and the loss scenarios may be refined in the future, loss scenarios needed to be referenced in more detail. As described in Chapter 5, the *STPA Handbook* gives several suggestions of causes of loss scenarios, so I have assigned a letter to some possible causes of loss scenarios:

A. Failure related to controller (physical): Physical failure of the controller itself

B. Failure related to controller (physical): Power failure of the controller itself

C. Inadequate control algorithm: Flawed implementation of the specified control algorithm

D. Inadequate control algorithm: The specific control algorithm is flawed

E. Inadequate control algorithm: The specific control algorithm becomes inadequate over time due to changes or degradation

F. Inadequate process model: Controller receives incorrect feedback/information

G. Inadequate process model: Controller receives correct feedback/information but interprets it incorrectly or ignores it

H. Inadequate process model: Controller does not receive feedback/information when needed (delayed or never received)

I. Failure related to actuator: Not executed

J. Failure related to actuator: Improperly executed

This list is in no way complete, but it is adequate to go through and control the loss scenarios deduced in this master thesis. E.g. *Unsafe control input: UCA received from another controller* were not relevant for my loss scenarios, so it is not listed above. Similarly, *Inadequate process model: Necessary controller feedback /information does not exist* are not included either, as feedback such as this one has been added instead. Loss scenarios are referenced as appropriately as possible, but one can argue that some of the loss scenarios would be better suited to a different letter. My main focus has been to identify all relevant loss scenarios. But it would be impossible to check if the losses make sense or not without such a reference.

Reference A *Failure related to controller (physical): Physical failure of the controller itself* includes several component failures on each subsystem, that are not actuators or sensors, e.g. communication systems. Reference B *Failure related to controller (physical): Power failure of the controller itself* several loss scenarios perhaps could be better suited under reference H *Inadequate process model: Controller does not receive feedback/information when needed (delayed or never received)*, but they are placed under reference B since communication systems etc. are by me considered to be part of the controller itself.

Reference C *Inadequate control algorithm: Flawed implementation of the specified control algorithm* and reference D *Inadequate control algorithm: The specific control algorithm is flawed* are easy to mix when creating loss scenarios, so some losses might arguably be interchanged, but that is up for discussion. The most important thing is that all loss scenarios are identified.

Reference E *Inadequate control algorithm: The specific control algorithm becomes inadequate over time due to changes or degradation* and reference F *Inadequate process model: Controller receives incorrect feedback/information* do have some similar loss scenarios, as the result of E often is incorrect feedback/information. Also, F and H may be similar, and some overlapping loss scenarios were also removed during the process of writing countermeasures.

A weakness in the formulation of loss scenarios is that they are not entirely written out. The first loss scenario for each UCA are, but not the rest. I found that the final sentence *"As a result [...]"* were more or less similar for all loss scenarios for a given UCA. This is true for most loss scenarios, but some UCAs are linked to two and not only one system-level hazard. When this is the case, I did not write out all the sentences, but I focused on referencing the correct system-level hazard instead. Writing out all these sentences would generate approximately 5'000 extra words and 10-15 additional pages tables in Appendix D, without providing any more useful information, so I decided not to do so.

The STPA method identifies a lot of hazards, and similarly, many countermeasures. 243 unique loss scenarios were identified for the 11 UCAs, approximately 22 loss scenarios per UCA. I realised that this would lead to hundreds of countermeasures, and without a method to sort these, it would be very difficult to evaluate which risk-reducing measures to prioritise. While creating countermeasures for each loss scenario, I attempted to create some main categories, which became the 8 categories:

- CM1: Redundancy

- CM2: Maintenance
- CM3: Risk aversion
- CM4: Constraint
- CM5: Training
- CM6: Procedures
- CM7: Equipment modification
- CM8: Adaptation

For each of these 8 categories of countermeasures, several specific countermeasures were made during the process of creating countermeasures. These were made as general as possible, to enable me to reuse countermeasures for other loss scenarios where applicable. 50 unique countermeasures were identified. However, most of these unique countermeasures are relevant for reducing the probability for more than one loss scenario.

In total, 551 countermeasures were listed, but this number could have been much higher particularly if all countermeasures that were relevant to a loss scenario were repeated every time, and also if even more time were dedicated to this part of the STPA process. I found that a weakness with this was that it was easier to write up a countermeasure that was fresh in my memory, that I had just used. Also, for the last half of loss scenarios, fewer countermeasures are identified per loss scenario, but this might be because they already are identified, and my focus was not on repeatedly listing all countermeasures.

This method of listing countermeasures may be structured, but it is very difficult to be consistent. E.g. loss scenarios LS.13.F-UCA.1 and LS.23.H-UCA.1 are almost identical and are related to the fact that in some cases, IM team or IMV may not receive all necessary information from sensor platforms during lousy weather conditions. However, the same countermeasures were not linked to both of the loss scenarios. Also, it may be commented that I went through UCA for UCA, from category A to J, systematically. Countermeasures could be repeated several times for many more loss scenarios, but since I had already included them elsewhere, it was challenging to be consistent.

However, most aspect of identifying countermeasures is to identify all that is relevant. I believe that I was likely to identify new countermeasures where they were needed because when the specified countermeasures already identified did not fit, I had to create a new unique CM. Some nuances might have been lost when creating general formulations, but it proved to be very helpful when attempting to sum up the loss scenarios and countermeasures and attempt to see which risk-reducing measures are important. All unique countermeasures are shown in Table 6.9.

Table 6.9: Specific countermeasures and categories

CM Category	Description
Redundancy	
CM1.1	Two communication systems for all subsystems
CM1.2	Two times needed engine capacity
CM1.3	Two water cannons/towing systems
CM1.4	Two navigation systems
CM1.5	Two disconnection mechanisms
Maintenance	
CM2.1	More frequent preventive maintenance (engine)
CM2.2	More frequent preventive maintenance (sensor platforms)
CM2.3	More frequent preventive maintenance (water cannon/towing)
CM2.4	More frequent preventive maintenance (disconnection mechanism)
Risk aversion	
CM3.1	Standby IMV to fill in during maintenance (engine)
CM3.2	Standby IMV to fill in immediately during failure
CM3.3	Invest in additional IMV
CM3.4	Invest in additional sensor platform
Constraint	
CM4.1	Always have one IMV between FPSO and approaching icebergs
CM4.2	Always command disconnection and evacuation if it is uncertain that IMV in CM4.1 will succeed in providing water cannon/towing
CM4.3	Always command disconnection and evacuation if IMV in CM4.1 have several approaching threatening iceberg in close proximity
CM4.4	Always update procedures after maintenance/change in equipment
CM4.5	Never command/proceed water cannon/towing in dangerous weather conditions
Training	
CM5.1	IM team/IMV training in detecting/tracking icebergs
CM5.2	IMV training in navigating only after coordinates
CM5.3	IMV training in water cannon/towing
CM5.4	FPSO training in how to disconnect and evacuate

Procedures	
CM6.1	Immediate read-back of coordinates/prioritisation/etc
CM6.2	Periodically control of data sources/control deviation
CM6.3	IMV must always check with IM team if they have observed an iceberg when IMV detects an iceberg
CM6.4	IM team must always send command to manage an iceberg (or add it to prioritisation) when local system detects a threatening iceberg
CM6.5	IMV must follow IM team command, and say if command defied
CM6.6	IMV must check for status of iceberg threat and prioritisation with IM starting/stopping water cannon/towing
CM6.7	IM team must always check with IMV for status of water cannon/towing if usage of time is longer than expected
CM6.8	IM team/IMV/FPSO human operator must always wear secondary communication system if not by primary communication system
CM6.9	IM team must lower threshold to command FPSO to disconnect when anomalies (e.g. reduced IM capacity, uncertainties, failures etc.)
CM6.10	IMV must inform IM team of reduced IM capacity/efficiency, so that IM team temporary lower threshold to disconnect/evade FPSO
CM6.11	IM team must always evaluate if IMV must leave iceberg immediately, when prioritisation changes according to local system
CM6.12	IM team must prepare to command disconnection/evacuation if dangerous weather conditions and inform IMV
CM6.13	FPSO must always check with IM team after preparation and before actual disconnection if it still is necessary
CM6.14	IM team must command IMV to stop water cannon/towing if it is obvious that an iceberg no longer is threatening
CM6.15	IM team/IMV/FPSO must always report near-accidents, so that procedures may be updated
CM6.16	IMV must always consider all data and experience when deciding between water cannon/towing, and stick to the choice
CM6.17	FPSO must follow IM team command, and say if command defied
CM6.18	IM team must command to disconnection and evacuation when local system detects that all threatening icebergs can't be managed

Equipment modification	
CM7.1	IM team local system must give a signal (sound/light) that IM team human operator actively must turn off/register when detecting threatening iceberg. If it is not registered signal is sent to the whole IM team for registration
CM7.2	IM team/IMV/FPSO communication system can not be turned off
CM7.3	IMV water cannon/towing add heating to avoid frost problems (or use towing equipment that withstands frost)
CM7.4	IMV towing system must have quick-disconnect to quickly dispose of iceberg
CM7.5	FPSO disconnection mechanism must function without power
CM7.6	FPSO disconnection mechanism add heating to avoid frost problems (or use mechanism that is not affected by frost)
CM7.7	IMV local system must give a signal (sound/light) that IMV human operator actively must turn off/register when command is received. If it is not registered signal is sent to the whole IMV for registration
CM7.8	FPSO local system must give a signal (sound/light) that FPSO human operator actively must turn off/register when command is received. If it is not registered signal is sent to the whole FPSO for registration
Adaptation	
CM8.1	Allow for this loss scenario to occur (e.g. fail-safe)
CM8.2	Allow for IMV to help search for threatening icebergs

When all loss scenarios and countermeasures were completed, they had to be presented clearly and transparently. Table 6.10 shows how all loss scenarios and related countermeasures are listed in Appendix D. There Table D.1-D.11 which contains all 243 loss scenarios and 551 countermeasures related to the 11 identified UCAs are listed. This chapter provides a summary of the results in Section 6.5.

Table 6.10: Excerpt Table D.1, loss scenarios and countermeasures

UCA.1: Water cannon/towing is not provided when a threatening iceberg is approaching the FPSO [H.1]	
Loss scenarios	**Suggested countermeasures**
LS.A.1-UCA.1: The IM team's communication system has failed, so the IM team are not able to request water cannon/towing. As result, a threatening iceberg that exceeds certain kinetic energy drifts towards the FPSO, and may collide if FPSO does not disconnect [H1]	CM1.1 CM6.9
LS.A.2-UCA.1: The IMV receives command from IM team to use water cannon/towing on an iceberg, but one out of two engines fails so the IMV are unable to catch up with the iceberg. As result, [...] [H1]	CM1.2 CM2.1 CM3.1, CM3.2, CM3.3 CM6.10
LS.B.3-UCA.1: The IM team's communication system does not function because of power failure, so the IM team are not able to request water cannon/towing. As result, [...] [H1]	CM1.1 CM6.9
Etc...	Etc...

6.4 Step 4: Refine Step 1–3 if Necessary

For this master thesis, the STPA analysis is not refined and studied in more detail. This means that I have kept the analysis on a high-level, and I have not created more than system-level losses, hazards and safety constraints. More complicated control structures of each subsystem could also have been made, as this is considered to be out of scope.

6.5 Step 5: Documentation and Implementation of Results

The results are documented in this chapter and may be reused and built on as we move from preliminary analysis to more detailed planning/realisation of the project in the case study. All

243 loss scenarios and 551 countermeasures identified in Table D.1-D.11, which are summarised in Table 6.11 and Table 6.12. A graphical representation is also given for the loss scenarios and countermeasures divided on the UCAs in Figure 6.2 and divided on references A–J in Figure 6.3.

Table 6.11: Loss scenarios broken down by UCA and reference

Ref	**UCA.1**	**UCA.2**	**UCA.3**	**UCA.4**	**UCA.5**	**UCA.6**	**UCA.7**	**UCA.8**	**UCA.9**	**UCA.10**	**UCA.11**	**Sum**
A	2	1	2	0	2	1	1	1	2	2	1	15
B	2	2	2	1	2	1	1	2	0	1	2	16
C	2	2	3	1	1	0	2	2	2	1	6	22
D	3	4	4	2	3	1	1	2	2	2	4	28
E	2	3	6	3	1	4	4	1	3	5	3	35
F	3	3	1	4	1	4	1	3	4	1	1	26
G	8	7	4	2	2	2	2	8	1	2	7	45
H	4	6	6	1	2	1	2	5	2	1	5	35
I	3	0	0	0	0	0	1	2	0	0	0	6
J	0	1	2	2	5	2	1	0	0	1	1	15
Sum	**29**	**29**	**30**	**16**	**19**	**16**	**16**	**26**	**16**	**16**	**30**	**243**

Table 6.12: Countermeasures broken down by UCA and reference

Ref	**UCA.1**	**UCA.2**	**UCA.3**	**UCA.4**	**UCA.5**	**UCA.6**	**UCA.7**	**UCA.8**	**UCA.9**	**UCA.10**	**UCA.11**	**Sum**
A	8	2	9	0	4	3	3	1	3	3	1	37
B	4	7	3	1	3	3	3	3	0	1	2	30
C	7	5	7	1	3	0	4	3	3	1	13	47
D	5	13	14	4	7	1	2	3	3	2	9	63
E	9	13	27	6	1	8	12	1	6	8	4	95
F	11	9	5	7	1	8	3	7	9	1	3	64
G	18	14	8	4	3	4	3	27	2	2	12	97
H	9	14	18	1	5	1	7	10	3	2	7	77
I	6	0	0	0	0	0	1	4	0	0	0	11
J	0	2	4	6	10	4	1	0	0	1	2	30
Sum	**77**	**79**	**95**	**30**	**37**	**32**	**39**	**59**	**29**	**21**	**53**	**551**

As we see in Figure 6.2 with loss scenarios and countermeasures sorted per UCA, a lot more countermeasures were identified for the first couple of UCAs, this might be because I started finding countermeasures from UCA.1 to UCA.11 and that my focus was not on listing all relevant countermeasures for all UCAs, but instead identifying all necessary countermeasures. Another peak is shown for UCA.8, which is interesting because this is the first UCA related to the FPSO. The number of loss scenarios is evenly distributed, with from 16 to 30 loss scenarios per UCA.

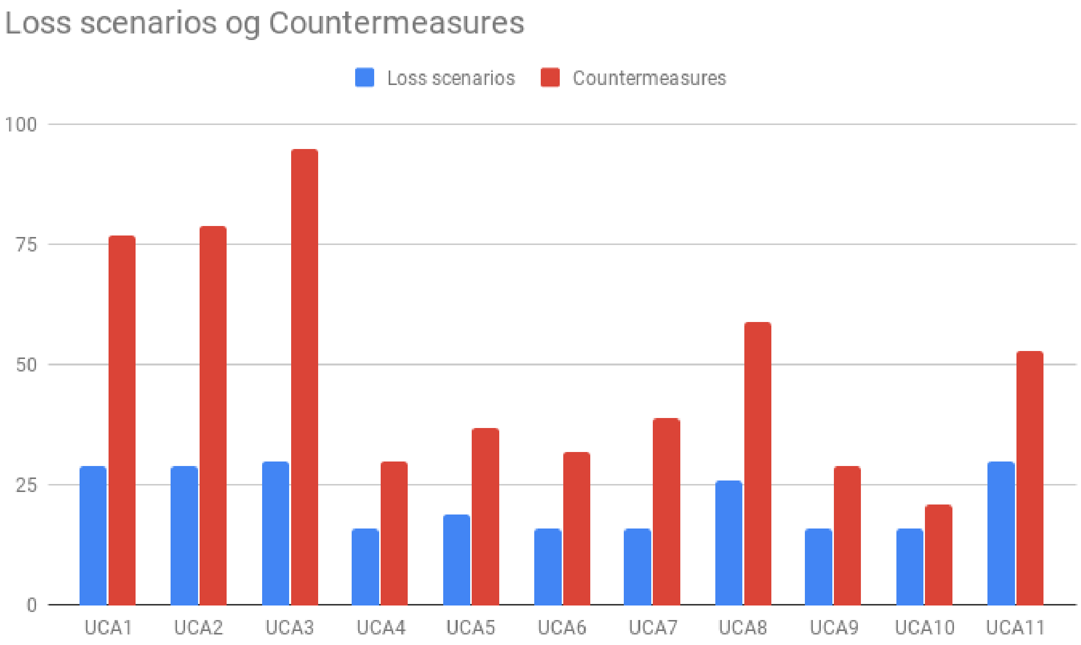


Figure 6.2: Loss scenarios and countermeasures per UCA

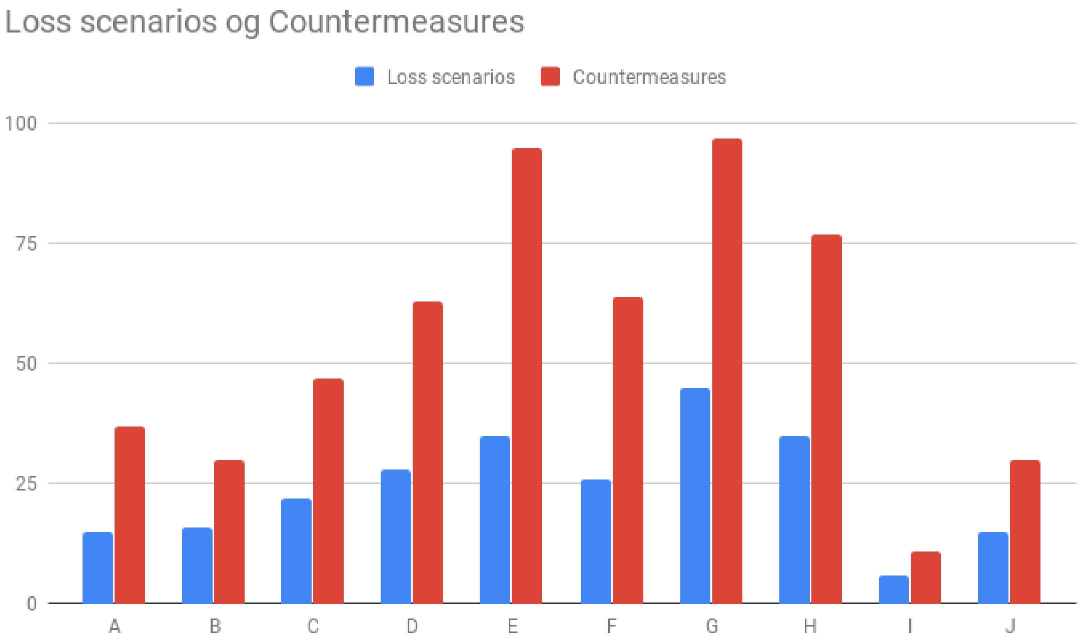


Figure 6.3: Loss scenarios and countermeasures per reference

The same result is not apparent in Figure 6.3 with loss scenarios and countermeasures sorted per reference A–J, there seem to be a lot more loss scenarios, related to the references about *inadequate control algorithm* and *Inadequate process model*, rather than component failures etc. which are more likely to be found in reference A, B, I and J. Similarly, a lot more countermeasures are also found for the same references, and not just proportionally to number of loss scenarios. These loss scenarios are related to weaknesses in procedures, i.e. how information/feedback are sent and received.

Table 6.13: Quantity of countermeasures per specific countermeasure and category

CM1 [34]	CM1.1 [19]	CM1.2 [6]	CM1.3 [4]	CM1.4 [1]	CM1.5 [4]
CM2 [30]	CM2.1 [7]	CM2.2 [12]	CM2.3 [6]	CM2.4 [5]	
CM3 [16]	CM3.1 [2]	CM3.2 [2]	CM3.3 [1]	CM3.4 [11]	
CM4 [79]	CM4.1 [29]	CM4.2 [9]	CM4.3 [8]	CM4.4 [19]	CM4.5 [14]
CM5 [36]	CM5.1 [8]	CM5.2 [1]	CM5.3 [22]	CM5.4 [5]	
CM6 [313]	CM6.1 [48]	CM6.2 [19]	CM6.3 [3]	CM6.4 [15]	CM6.5 [15]
	CM6.6 [30]	CM6.7 [39]	CM6.8 [13]	CM6.9 [10]	CM6.10 [16]
	CM6.11 [2]	CM6.12 [16]	CM6.13 [25]	CM6.14 [8]	CM6.15 [27]
	CM6.16 [8]	CM6.17 [11]	CM6.18 [8]		
CM7 [32]	CM7.1 [9]	CM7.2 [2]	CM7.3 [1]	CM7.4 [1]	CM7.5 [2]
	CM7.6 [1]	CM7.7 [8]	CM7.8 [8]		
CM8 [11]	CM8.1 [3]	CM8.2 [8]			

[1-5]	[6-15]	[16-25]	[26-50]

Table 6.13 shows how many countermeasures were found per specific countermeasure and category. 18 of the 50 specified countermeasures, CM6.1–CM6.18, are related to *procedures*. I.e. 313 of the 551 countermeasures are related to procedures. The second most frequent countermeasure as related to *constraints* (79), followed by *training* (36), *redundancy* (34), *equipment modification* (32), *maintenance* (30), *risk aversion* (16) and *adaptation* (11). Almost all countermeasures are of importance when it comes to ensuring successful ice management. Hazards, UCAs, loss scenarios, countermeasures etc. are not ranked in STPA, but with this table, at least a visualisation of the countermeasures frequency is given. However, this may be more misleading than helpful.

My contribution to STPA from this analysis has been to add references to both loss scenarios and countermeasures. This is useful to ensure a more systematic approach and to ease both documentation, control and refining results in further analyses.

Chapter 7

Comparison of STPA and FMECA Cases

In Chapter 4 and Chapter 6 FMECA and STPA cases are given respectively. Both cases are given at an equivalent high-level on the same problem, early phase planning of a marine operation in the Arctic. The overarching goal is to protect an FPSO from a collision with icebergs. In this chapter, I will first compare STPA to traditional hazard analysis methods such as FMECA, and secondly, I will compare the results of the two case studies. Lastly, I will discuss which approach is better for threat identification in ice management applications.

7.1 STPA Compared to Traditional Hazard Analysis Methods

Studies have been made to compare traditional hazard analysis methods and STPA, but most comparisons were made before Leveson and Thomas (2018) revised the STPA method. However, I find these comparisons to be valid, as the fundamentals of STPA rest unchanged. FMEA/FMECA, PHA, and qualitative FTA only require some system information. In contrast, the information needed to do an STPA analysis generally is much more extensive. However, the joint research project Ishimatsu et al. (2010) between MIT and JAXA/JAMSS comparing FTA and STPA points out that one strength of STPA is that detailed information about the component design is not necessary, which enables the use of STPA in earlier phases. One major limitation of approaches such as FTA and FMECA is that "much of the effort goes into proving that existing designs are safe rather than building designs that are safe from the beginning."

To successfully conduct an analysis using FMEA/FMECA, PHA, FTA, or STPA, a higher level of expertise in the method is required to use the STPA method compared to the other methods, respectively. STPA is a rather new method, and naturally, there are not as many experts on STPA compared to traditional hazard analysis methods, which are more straight-forward to use. However, Teikari (2014) argues that methods such as STPA and HAZOP offer more guidance than FMECA in terms of identifying failure modes and causes to these. To successfully conduct an STPA, the analyst must know the STPA method very well, but domain expertise on the system analysed is not as critical.

An evaluation of the applicability, understandability, effectiveness, ease of use and efficiency of FTA, FMEA/FMECA and STPA in terms of identifying software safety requirements of safety-critical software was made by Abdulkhaleq and Wagner (2015). This study found that there was no significant difference in the applicability, understandability and ease of use of the three methods, but that STPA was more applicable when compared to FMEA/FMECA. STPA was the least efficient method, i.e. more time-consuming. However, STPA was more effective than both FMEA/FMECA and FTA, i.e. more thorough finding more faults. For safety-critical systems, the latter is arguably more important than the time perspective.

Case studies like Sulaman et al. (2017) on a forward collision avoidance system argue that further research should look into extensions and combinations of hazard analysis techniques that have different focuses. Neither FMEA/FMECA or STPA found all hazards single-handedly. The traditional hazard analysis methods may not be suitable for analysing systems that are software-intensive or have complex interactions between components, humans, etc. A new method is necessary to analyse modern complex sociotechnical systems efficiently, as discussed in Chapter 5. The traditional methods were not developed with these factors that appear more and more frequently in newer systems in mind, but they might still be a useful supplement in the pursuit of an optimal hazard identification method.

7.2 Discussion and Comparison of Results STPA and FMECA

For the STPA case study, many loss scenarios and countermeasures were identified, almost overwhelmingly many. Since I have done this analysis manually without any dedicated tools, I found that it was necessary to deviate from how the method is described both by Leveson and Thomas (2018) in the *STPA handbook* and by myself in Chapter 5. To keep track of accumulating loss scenarios and countermeasures, it was necessary to deviate from the STPA steps and reference these. Both to be able to keep track of them and to allow for quality control of the findings.

The categories made for countermeasures are more debatable. Some categories could be merged afterwards, or a list of categories could have been given by the *STPA handbook* to ensure that all types of necessary countermeasures are included. As briefly mentioned in Section 6.3, categories were just made whilst identifying countermeasures relevant to each loss scenario. The total number of countermeasures could have been much higher, particularly if all countermeasures relevant to a loss scenario were repeated every time.

Given the limitations of the master thesis and the case study, I would say that all relevant UCAs are found. The same can not be said for loss scenarios and countermeasures. At a certain point, a hard line had to be drawn, both to ensure that the analysis was conducted at the proper intended high-level, and to be able to finish and complete the analysis. The references added to loss scenarios are not controversial what so ever, as they reflect suggested causes to loss scenarios from the *STPA handbook*. 243 unique loss scenarios were identified for the 11 UCAs, on average, 22 loss scenarios per UCA. 50 unique countermeasures were identified, where many were relevant for several loss scenarios. In total, 551 countermeasures were identified, on average, 50 per UCA, i.e. more than two per loss scenario.

STPA does not rank the severity of different loss scenarios. Therefore it was useful to systematically list loss scenarios and countermeasures, as the sheer number of countermeasures might indicate where the focus should be. However, this may be dangerous too. It is tempting to omit countermeasures that are less frequent, but those may be just as important. The most significant advantage of this systematic approach is to be able to control and revise the analysis and ensure that all identified loss scenarios and countermeasures are evaluated when deciding which risk-reducing measures to prioritise.

Table 3.1 shows advantages and limitations of the FMECA technique, and Table 5.2 shows advantages and limitations of STPA. These tables are general and have not been developed with ice management in mind. The FMECA did not identify all hazardous scenarios that the STPA analysis identified. Similarly, some of the hardware failures were not identified in the same detail using STPA. STPA identifies a lot of hazards, but these are not ranked, so it is more difficult to assess whether or not a loss scenario is critical or not and to prioritise countermeasures to reduce risk efficiently. There are several hazards identified by the STPA regarding hazards due to decisions made by human operators, that I did not think of using the FMECA method. The STPA method would be a good supplement to the FMECA for problems regarding ice management to ensure that all aspects of the analysis are considered.

The FMECA analysis proved very efficient in identifying failures related to hardware. It would be straight-forward to go into more detail on each subsystem to the component level and identifying critical failures. STPA identified almost all hardware failures too, but it was much more challenging to find the same hazards that FMECA does. STPA would have proven inefficient in finding all component failure hazards if the analysis were not on such a high-level, and there is no method to rank these failures, which is an integrated part of the FMECA analysis. This is an argument to combine STPA with FMECA or other hazard analysis methods. Without some method to convert all the qualitative information obtained from the STPA analysis into quantitative data that may be used to rank risks and make prioritisation based on the actual cost of reducing risk, and consequences of not doing so, it is difficult to mitigate risk using only STPA when resources are limited efficiently. This is consistent with the previous studies comparing STPA and FMECA in Section 7.1.

Both the STPA and FMECA identified many failures due to component failure, and both methods suggested more frequent maintenance or different sorts of testing to avoid these. Both methods also recommended building in some redundancy. In the STPA analysis, these countermeasures are organised under the specific countermeasures *redundancy* and *maintenance*, and they were all also identified by the FMECA method. However, the STPA method cannot easily rank these failures or determine which ones are critical. This is straight forward with FMECA. All of the critical RPNs, as shown in Table 4.1 was related to this type of failure mode.

In the STPA, all countermeasures were not structurally repeated for all loss scenarios, so the quantitative summary also gives a wrong picture of the frequency. However, the indication that STPA detects many countermeasures related to procedures and inadequate algorithms and process models are apparent. Almost as many faults related to hardware are listed for the STPA as for the FMECA, but this is just because the analysis is done on a very high-level. It would be challenging to go into more detail on component failures in STPA, and it would not be possible to make a quantitative evaluation of component errors anyways, and they would not be ranked. One of the difficulties using STPA is that it is a very tedious process to discover all UCAs and loss scenarios. If I had not derived "too many", I might have risked not identifying as many loss scenarios as I did. The STPA method is not straight forward and clear as the FMECA method is. This is one of the disadvantages of STPA.

I completed the STPA analysis before I began the FMECA analysis, so this might have been an advantage when working with the FMECA. I had a better understanding of the system as a whole, and I had already thought a lot about hazardous scenarios when commencing the FMECA. Because of this, it was easier to perform the FMECA than usually. It might have been the other way around if I started with the FMECA, and then did the STPA analysis, but is it hard to say. I still believe that it is correct that the FMECA is a much easier and more straightforward method than STPA. However, STPA has some advantages that FMECA does not have.

Albeit, there are very many countermeasures that the FMECA did not identify. Most of the 551 countermeasures identified by STPA are essential to ensure successful ice management, and only 64 of these are related to *redundancy* and *maintenance*, which also FMECA identified. Other failures identified by the FMECA method that were not component failures, were power failures, fail to function and in one instance, not receiving data due to weather conditions. The latter probably would not be identified if I had not already found it using the STPA method. It is challenging to identify failure modes and causes without domain expertise. However, many of the hazards identified by the STPA method are very important and were not identified by the FMECA method. In this case study, the FMECA did not identify failures related to what I named the "local system" that both IM team and IMV use to process data, to get information about trajectory and criticality of icebergs, and track these. This system provides valuable decision-making help for the human operators, that may lead to many hazards if the decision making help is flawed in some way, or if the information is misunderstood. The FMECA could be used to rank failures in this system if it were combined with STPA, and the hazards were identified.

Several countermeasures identified by STPA are of importance to ice management, such as *equipment modification*, *procedures* and *constraints*. These are also difficult identifying using FMECA but could, of course, be identified spending much time with domain experts. counter-measures such as those related to *risk aversion* and *training* are to some extent trivial, and could of course also be identified using FMECA. However, when one is familiar with the STPA method, it is easier to identify more causal factors using STPA than a more traditional approach such as FMECA. Studying the results from the case studies, it is apparent that causal factors related to software, humans, organisation, safety culture, etc. are more straight-forward to identify with STPA. STPA have proved useful for threat identification in ice management systems, while the same may not be said for a traditional method such as FMECA. That said, none of the methods is adequate by themselves.

7.3 Possibility to combine STPA with Traditional Hazard Analysis Methods and BBNs

Looking at Section 7.1 and 7.2 it seems apparent that STPA and traditional hazard analysis methods should be complementary, but it is not as trivial to determine how STPA could or should be combined with other methods.

Traditional hazard analysis methods are better than STPA to find quantitative results, but are not necessarily good at accounting for uncertainty. Chapter 2 on *Ice Management* shows that there are uncertainty linked to many parameters such as expert judgement, weather states, ice states, etc. Bayesian reliability analysis is a probabilistic method that has shown to be be useful when uncertainty is an important factor. This method is not introduced in this master thesis, but was introduced in my specialisation project Nesse (2019).

Bayesian approaches may be used on both statistical uncertainty, i.e. when results vary due to effects that appear to be random or at least very difficult to predict, and systematic uncertainty, i.e. when results vary due to effects that we could interpret but we in fact do not due to simplifications or imperfections in our models. Bayesian methods are efficient tools to incorporate engineering information or other prior information into a formal statistical analysis (Rausand and Høyland, 2004).

One application of Bayesian reliability is called Bayesian belief networks (BBNs), which are a quantitative approach used to used to model uncertainty. One application of BBN are Arctic shipping accident scenario analysis (Afenyo et al., 2017). The examples are as numerous as the areas of application of BBNs such as Fu et al. (2016), Khan et al. (2018) and Farid et al. (2014) describes some applications of BBN to marine operations in harsh Arctic environments. The latter, the Hybrid Bayesian belief network for risk modelling of Arctic marine operations, by Farid et al. (2014) is a combination of Bayesian belief networks (BBNs) and Fault tree analysis (FTA). He aimed to "describe and model the uncertainties involved and to quantitatively asses the risk of an ice management operation as a barrier whose failure can threaten the safety of the protected structure or vessel." This can be used to see which risk influencing factors (RIFs) is most cost-effective to invest in to maximise reliability. STPA could be combined with such a method to ensure that all threats are identified and considered.

Different methods to identify hazards may be combined or blended. The purpose of blending is to take advantage of the strengths of each method while compensating for their weaknesses. In a blended method, the fundamental elements of two or more methods are identified, and a new, single, methodology is formed from these elements. It is crucial to understand how these elements fit together so that the methods can be blended. Blending requires an in-depth knowledge of how the methods operate and the fundamental concepts underlying them Seligmann et al. (2012).

Table 7.1: Function and component-driven classification of well-known HAZID methods. Adapted from Seligmann et al. (2012)

Method	Component-driven	Function-driven
FMEA/FMECA	x	
Fault Tree Analysis	x	
HAZOP		x
Preliminary Hazard Analysis	x	
STPA		x

In Table 7.1, where I have added STPA as well, shows some whether or not methods are component- or function-driven. Component-driven methods are often better suited for quantitative analysis, while others are more qualitative. To take advantage of the strengths of STPA, and eliminate some of its weaknesses, it would be smart to combine or blend it with a more component-driven method, such as FMECA or FTA.

For this master thesis, I cannot check whether or not combining STPA with methods such as FMECA or FTA will be successful or not, but I believe that there would be some benefits to this. One example of how to combine STPA with FMECA is shown in Chapter 6. Secondly, for a more detailed analysis at least, all flaws related to hardware and components could be part of a normal FMECA, as shown in Chapter 4. And lastly, to take advantage of all the identified loss scenarios and countermeasures from the STPA analysis, these could be integrated into a new analysis where the goal is to rank the necessity and cost of all countermeasures to efficiently be able to determine the most efficient method to reduce risk. To do this, one would need to:

1. rank the severity/consequence of each loss scenario, with respect to the worst outcome

2. rank the frequency of this loss scenario to occur

3. rank the resources necessary of implementing a countermeasure

These numbers could be multiplied similarly as RPNs are found in an FMECA. It would need some work to figure out exactly how this could be done in a meaningful way. Perhaps countermeasures would need to be formulated in a particular fashion, and maybe the sheer number of countermeasures could have some significance as well (to ensure that countermeasures regarding procedures are appropriately weighted). Combining or blending STPA with traditional hazard analysis methods, e.g. in a variation such as the one mentioned above, could be an essential step towards optimal threat identification in ice management systems, and should be considered for further work.

Chapter 8

Conclusions, Discussion, and Recommendations for Further Work

8.1 Summary and Conclusions

For the past century, the Arctic has been attracting brave researchers and adventurers, but inaccessible for most. Advancements in technology and changes in the climate are rapidly changing this, making the Arctic region more accessible. Section 1.1 shows that annual mean ice thickness in the Arctic has decreased by approximately two thirds since the 70s and that the ice also tends to shrink in extent, and by the 2030s we might have periods of the year with no sea ice at all. This may affect global trade patterns, as the usage of the Northern Sea Route through the Arctic will reduce the time in transit considerably for some routes from Europe to Asia. A sixth of the world's undiscovered hydrocarbons and other minerals may be found north of the Arctic circle. However, to exploit these resources and opportunities, marine operations must handle harsh weather and ice conditions. To safely do this, ice management is necessary.

Ice management is defined in Section 2.2 as the sum of all activities where the objective is to reduce or avoid actions from any ice features. This definition includes, but is not limited to surveillance and monitoring of ice features, threat identification and evaluation of ice features and physical management of ice features. For this master thesis, marine operations have been limited to regions where ice management of icebergs are in focus. It is made clear that efficient ice management is necessary to ensure safe marine operations. Chapter 2 also showed that ice management systems arguably are complex modern systems as described in Section 5.1. Ice management systems are software-intensive, and many component and system interactions must be investigated during threat identification. Ice management operations today are dependent on the crew's ability and experience, and developments in tools used for decision-making attempts to reduce our dependability on capable crews. Modern complex sociotechnical systems introduce new types of hazards.

The hypothesis in my specialisation project Nesse (2019) was that traditional hazard analysis methods were not sufficient for identifying hazards in ice management. The results were promising, so this has been followed up in this master thesis through two case studies. Traditional hazard analysis methods are not adequate for threat identification of complex modern sociotechnical systems, and the applicability of STPA has been further investigated.

The first objective of this master thesis was to establish fundamental knowledge on ice management and STPA. I have scratched the surface of state of the art research relevant to ice management and summarised challenges which remains to be solved in Section 2.7. Efficient ice management operations also depend on reliable monitoring and surveillance of ice, which in itself is challenging to accomplish. Sensors and sensor platforms of the future are autonomous, software intensive, and do themselves potentially introduce new threats such as complex interactions, flawed algorithms, failure to send and receive information, and more may lead to unsafe control actions potentially leading to accidents. Tools used to simulate marine operations and identify and evaluate threats and offer decision support to crew are described briefly. An encompassing overview of all simulation tools could be proven useful but was far too labour-intensive to conduct. It was, however, found that the phenomena we are trying to simulate are very complex, and it is difficult to make good predictions because of the complexity of ice interaction. Complex models are used to translate data into useful decision support, and may themselves lead to accidents because of flawed algorithms, suggesting unsafe actions when incomplete information is received, and more. Physical management of ice features is critical to ensure safe operations, but may itself lead to hazardous situations and accidents such as collisions. In Section 2.6 on *Data sources and expert judgement* it is shown that ice management often are subject to lack of information, and use of expert judgements are important to account for uncertainties. I have not managed to find much information on how threat identification is made by companies performing marine operations, which would be very helpful when conducting my case studies. The objective of establishing fundamental knowledge on ice management have been partially accomplished.

In addition to ice management, fundamental knowledge on STPA and the STPA process have been established. This proved to be an easier task and pretty straight forward. The hypothesis in my specialisation project Nesse (2019) was that traditional hazard analysis methods were not sufficient for identifying hazards in ice management. The results were promising, so this has been followed up in this master thesis. In Section 5.1, the characteristics of modern sociotechnical systems are established, and it is shown that a completely new way of thinking might be necessary in terms of threat identification. STAMP is based on systems theory and a sociotechnical framework, and an overview is presented in Section 5.2. STPA is built on STAMP, and is presented in Section 5.3 followed by advantages and limitations in Section 5.4. The STPA process is given in Section 5.5. STPA manages to take into account new causes to accidents and hazards such as software, human, organisational and complex system and component interactions. These causes are becoming increasingly more important as systems are becoming more complex. STPA is efficient because it is a top-down approach, and does not rely on extensive information on detailed design to perform preliminary analysis. The objective of establishing fundamental knowledge on STPA has been accomplished.

The second objective of this master thesis was to conduct a case study related to ice management of icebergs using FMECA and STPA and to compare the two case studies, and identify the advantages and limitations of the two methods. Fundamental knowledge of STPA was established as part of the first objective. FMECA is well known, but a brief overview of FMECA was given in Chapter 3. The case studies using FMECA and STPA are given in Chapter 4 and 6 respectively. Both case studies were done on a high-level, and more detailed analysis would be beneficial comparing the two case studies, which is done as part of the final objective. The objective to conduct two case studies has been accomplished.

The final objective was to evaluate whether or not STPA should be applied to ice management, if it should be used in combination with other methods, or if it is not suited whatsoever. In Section 7.1 I investigate literature comparing STPA to traditional hazard analysis methods, and in Section 7.2 I compare the results of the two methods, with respect to the advantages and limitations that I have found in my literature study describing the methods, and what others have found comparing the methods. The traditional hazard analysis methods are not suitable for analysing systems that are software-intensive, have complex interactions, etc. A new method is necessary to efficiently analyse modern complex sociotechnical, which ice management systems are. Also, in Section 7.3, I further discuss whether or not STPA may be combined or blended with other methods to take advantage of the strengths of the STPA method and to eliminate its weaknesses.

It is concluded in this master thesis that STPA should be used for ice management, as many hazards are difficult to identify using traditional hazard analysis methods. However, it is more difficult to see how the STPA method is best exploited. It is necessary to do a more complex case study of STPA in parallel with industry partners to compare results with what is identified in a real situation. STPA does not require extensive domain experience of the system analysed, which have proven useful in my master thesis. To determine how STPA best is blended or combined with other traditional hazard analysis methods, it still is needed to investigate this further. The suggestions I give are merely speculations on what may work and not. My contribution to STPA from this master thesis has been to investigate whether or not STPA should be applied to ice management and to add references to both loss scenarios and countermeasures. This is useful to ensure a more systematic approach and to ease both documentation, control and refining results in further analyses. I have also suggested to combine STPA with FMECA, and potentially with BBNs, which should be investigated in further work.

8.2 Discussion

Chapter 7 *Comparison of STPA and FMECA Cases* discusses and compares the results found in the case studies. Here the conclusions of the master thesis as a whole are discussed.

Chapter 2 showed that ice management systems arguably are complex modern systems as described in Section 5.1. Ice management systems are software-intensive, and many component and system interactions must be investigated during threat identification. Ice management operations are dependent on the crew's ability and experience, and developments in tools used for decision-making attempting to reduce how dependent we are on capable crews. Simultaneously, the conclusions show that the very same developments aimed at improving ice management might lead to new hazardous situations. I am not in any way saying that this advancement is not good, but it is an indication of that new approaches to threat identification methods in the domain of ice management is necessary.

Efforts have been put into becoming familiar with ice management. However, STPA does not require domain experience, and I do not think that the case study would have suffered much if I did not learn as much about ice management. However, for a more complex or in-depth STPA analysis, of a real situation, my newly attained knowledge of ice management would have come to better use. In such an analysis, it would be necessary to discuss several aspects with domain experts, which would be difficult to do without extensive knowledge of ice management. I am not very familiar with the process of threat identification in normal marine operations, but I do have some understanding of how it is done in the oil and gas sector. In my literature study, some applications of STPA to oil and gas were found, but this is not how it is typically done. I would expect that increased precautions are made, using traditional hazard analysis methods.

My best guess is that they do it in a similar way that they do in operations in other regions of the world, i.e. areas not infested with sea ice or any other ice features, with the same tools and methods, but in some way attempt to integrate the new ice loads and hazards that are important in harsh Arctic environments into these models. In the oil industry that has, or are planning to operate in the Arctic, I would guess that SIL (safety integrity levels) are used to determine whether or not they are satisfied with the performance required for a safety instrumented function they have introduced. However, this does still not tell me much about their methods of identifying hazards, but it would be found while investigating this further and is suggested as further work.

The established results on ice management, however, are not useless. The lessons learned on ice management have been useful in attempting to suggest to which parts of ice management STPA may be used for. I have realised that many hazards should be measured and ranked quantitatively, which is difficult to do using only STPA. However, many causes of accidents in modern sociotechnical systems also appear in ice management. It is useful to apply STPA to ice management, but not only on its own. Nor will the traditional hazard analysis methods be sufficient when it comes to complex sociotechnical systems, which ice management operations arguably are, so everything points in the direction of which STPA may be applied to ice management. However, further work is necessary to do more than speculate on what parts of ice management STPA is best suited for, and with which traditional hazard analysis methods STPA should be combined or blended with.

There is little data on accidents in the Arctic, some of which are due to few marine operations in the Arctic. There is a good reason to assume that operations in the Arctic are often well planned and executed with large safety margins. However, improvements in ice management are interesting to ensure the safety of projects as they are today, and may extend the reach of marine operations further into regions with harsh Arctic environments and still be able to ensure safe operations.

A general limitation of the findings on STPA is that there is not very much literature that has not been written without help or support from Professor Leveson or people affiliated with her. However, the methods have been applied to a wide range of sectors and domains, and interest in the model is increasing. Some possible applications of STPA are that the outputs may be used to "drive the system architecture, create executable requirements, identify design recommendations or mitigations and safeguards needed, define test cases and create test plans, drive new design actions, evaluate design, and design more effective safety management systems".

The main objective of this master thesis was to investigate whether or not STPA proved to be useful for applications within ice management. It is concluded in this master thesis that STPA should be used for ice management, as many hazards are difficult to identify using traditional hazard analysis methods. However, it is more difficult to see how the STPA method is best exploited. One clear thing is that a new method is necessary to analyse modern complex sociotechnical systems which ice management is. An apparent limitation of STPA is that it may not be used independently to create probabilistic estimations of threats, and it might be difficult to decide which improvements that should be prioritised with respect to risk mitigation. However, STPA is compatible with such traditional hazard analysis methods. The traditional methods were not developed with these factors that appear more and more frequently in newer systems in mind, but they still will be a useful supplement in the pursuit of an optimal hazard identification method. STPA must be combined or blended with at least one of these methods to identify and evaluate threats in ice management adequately.

8.3 Recommendations for Further Work

The literature on ice management describes many areas that should be subject to improvement, with respect to surveillance and monitoring, threat identification and evaluation and physical ice management of ice features. My recommendations for further work are with regard to hazard identification in ice management processes. The recommendations may be classified as:

- ***Short-term:*** Building on this master thesis, more work should also be done to establish how companies realising marine operations in harsh Arctic environments approach hazard identification. Efforts should also be made creating more complex academic case studies with different applications to ice management systems, and comparing these with identified results in real situations. These case studies should be more detailed, as this master thesis was done on a high-level. This could be used to verify or challenge the suggestions made in this master thesis about the best areas of application of STPA in ice management.

- ***Medium-term:*** In a short-term to medium-term perspective, it should be investigated whether or not the suggestions of how to combine STPA with other methods have merit or not. Also, if academic case studies show promising results, case studies should be made in cooperation with industry partners in parallel with their conventional approaches to hazard identification. This could be used to investigate how STPA performs in combination with other hazard analysis methods in ice management.

- ***Long-term:*** In a long-term perspective, given that the above-mentioned further work leads to promising results, efforts should be made to develop best practice further and make available examples that may be used for everyone interested in marine operations in harsh Arctic environments. Standards such as ISO 19906:2010 *Petroleum and natural gas industries – Arctic offshore structures* could be updated with findings.

Appendix A

Abbreviations

ACCP Alaska Center for Climate Assessment and Policy

ACEX Arctic Coring Expedition

ALARP As low as reasonably practicable

AMAP Arctic Monitoring and Assessment Programme

AOOS Alaska Ocean Observing System

ARCUS Arctic Research Consortium of the U.S.

ARP Aerospace Recommended Practice

ASPeCT Antarctic Sea Ice Processes & Climate

BBN Bayesian belief network

BS British Standards

CAST Causal analysis using STAMP

CIS Canadian Ice Services

DP Dynamic Positioned

EVITRs Equivalent-Volume Ice Thickness Ranges

FMEA Failure Mode and Effects Analysis

FMECA Failure Mode, Effects and Criticality Analysis

FFTA Fuzzy FTA

FPSO Floating Production, Storage and Offloading

FTA Fault tree analysis

F-VIM Fussel-Vesely importance measure

HAZOP Hazard and operability study

ICEMON Sea ice monitoring in the polar regions

ICEWATCH Real-time sea ice monitoring of the Northern Sea Route

IEC International Electrotechnical Commission

IMV Ice Management Vessel

ISIS Ice Services Integrated System

ISO International Organization for Standardization

JAMSS Japan Manned Space Systems Corporation

JAXA Japan Aerospace Exploration Agency

KMOU Korea Maritime and Ocean University

KRISO Korea Research Institute of Ships and Ocean Engineering

MIL-STD Military Standard

MIT Massachusetts Institute of Technology

NASA National Aeronautics & Space Administration

NSIDC National Snow and Ice Data Center

NSR Northern Sea Route

NTNU Norwegian University of Science and Technology

NWP Northwest Passage

PC Polar Class

PHA Preliminary hazard analysis

RAMS Reliability, Availability, Maintainability, and Safety

RBD Reliability block diagram

RPN Risk priority number

SAE Society of Automotive Engineers

SIBIS Simulation of Interaction between Broken Ice and Structures

SIL Safety integrity level

SNAP Scenarios Network for Alaska and Arctic Planning

STAMP Systems-Theoretic Accident Model and Processes

STPA System Theoretic Process Analysis

UAV Unmanned aerial vehicles

USV Unmanned surface vehicles

WHOI Woods Hole Oceanographic Institution

WMO World Meteorological Organization

Appendix B

Ice Management terminology

Ice management introduces many terms unknown to most readers of this master thesis. Usually, the use of terminology is consistent, but to ensure that what I have meant is understood correctly and to make reading easier, a list of terms is provided in this appendix.

Several glossaries are made available by National Aeronautics & Space Administration (NASA) Earth Observatory, Woods Hole Oceanographic Institution (WHOI), National Snow and Ice Data Center (NSIDC), Antarctic Sea Ice Processes & Climate (ASPeCt), Arctic Research Consortium of the U.S. (ARCUS) and more. Atlas (2019), a data source funded by AOOS, ACCAP and SNAP provides a useful adaption of these glossaries. The list below is based on this adaptation:

☞ **Anchor ice**: Submerged sea ice attached or anchored to the bottom, irrespective of the nature of its formation.

☞ **Compact pack ice**: Pack ice in which sea ice concentration is 10/10 (100%) and no water is visible.

☞ **Concentration**: See sea ice concentration.

☞ **Consolidated pack ice**: Pack ice in which sea ice concentration is 10/10 (100%) and floes are frozen together.

☞ **Drift ice**: Sea ice that moves because of winds, currents, or other forces.

☞ **Fast ice**: Sea Ice that is anchored to the shore, ocean bottom, an ice wall, an ice front, or between shoals or grounded icebergs. Fast ice is defined by the fact that it does not move with winds or currents. May be formed in situ from sea water or by pack ice freezing to the shore, and may extend a few meters or several hundred km from the coast. If it is thicker than about 2 meters above sea level, it is called an ice shelf.

☞ **Fast ice boundary**: Boundary between fast ice and pack ice.

☞ **Fast ice edge**: Boundary between fast ice and open water.

☞ **First-year ice**: Sea ice of not more than one winter's growth, developing from young ice, with a thickness of 30 cm to 2 m.

☞ **Floe**: Any relatively flat piece of sea ice 20 m or more across. Floes are subdivided according to horizontal extent: SMALL (20–10 m across); MEDIUM (100–500 m across); BIG (500 m–2 km across); VAST (2–10.8 km across); GIANT (> 10.8 km across).

☞ **Ice management**: The sum of all activities where the objective is to reduce or avoid actions from any kind of ice features.

☞ **Ice thickness**: See sea ice thickness.

☞ **Iceberg**: A massive piece of ice greatly varying in shape, showing more than 5 meters above the sea surface, which has broken away from a glacier, and which may be afloat or aground. Icebergs may be described as tabular, dome shaped, pinnacled, drydock, glacier or weathered, blocky, tilted blocky, or drydock icebergs. For reports to the International Ice Patrol they are described with respect to size as small, medium, or large icebergs.

☞ **Icefoot**: A narrow fringe of sea ice attached to the coast, unmoved by tides and remaining after the fast ice has broken free.

☞ **Lead**: A long, linear area of open water that ranges from a few meters to over a kilometre in width, and tens of km long, which develops as sea ice pulls apart.

☞ **Marginal ice zone**: Transition zone between the ice edge (often defined by the 15% contour of ice concentration) and the boundary of ice having a concentration > 80%.

☞ **Multi-year ice**: Old sea ice 3 m or more thick that has survived at least two summers' melt. Hummocks are even smoother than in second-year ice, and the ice is almost salt free. The colour, where snow free, is usually blue. The melt pattern consists of large interconnecting irregular puddles and a well developed drainage system.

☞ **Navigable** : Characterisation given to a waterway that is passable by ship, even with the presence of sea ice. Vessel capability determines navigability of sea ice.

☞ **Open lead**: A lead that connects two open bodies of water; ships can traverse between them through this lead. It also refers to a lead where open water is found, or a lead that has not completely frozen.

☞ **Open pack ice**: Pack ice in which the concentration is 4/10 to 6/10 (40–60%) with many leads and polynyas, and floes generally not in contact with one another.

☞ **Open water**: A large area of freely navigable water in which floes may be present in concentration under 1/10 (10%). If no sea ice is present, the area may be considered open water even if icebergs are present.

☞ **Pack ice**: Sea ice that not attached to the shoreline and that drifts in response to winds, currents, and other forces. Some prefer the generic term drift ice, and reserve pack ice to mean drift ice that is closely packed.

☞ **Pancake ice**: Predominantly circular pieces of sea ice from 30 cm – 3 m in diameter and up to 10 cm thick, with raised rims due to the pieces striking against each other.

☞ **Permanent ice zone**: A region that is covered in sea ice year-round. Most of the sea ice in the permanent ice zone is multi-year ice, but younger ice and open water may still be present. The permanent ice zone is what remains in summer after all melting has occurred (also known as the summer minimum extent).

☞ **Polynya**: A wide area of open water in an area of pack ice. A polynya differs from a lead in that leads are long and narrow.

☞ **Remote sensing**: Viewing something from a distance. Satellites and other instruments are used to collect a variety of remote sensing data:

- *visible light*: light that our eyes can detect
- *infrared light*: longer wavelengths than those of visible light (can be thought of as heat)
- *passive microwave*: measures objects that emit even longer wavelengths than infrared

- *active microwave*: satellite sensors that emit microwaves toward Earth's surface and "read" the energy returned to the sensor.

☞ **Sea ice**: Any form of ice found at sea that has originated from the freezing of seawater.

☞ **Sea ice area**: Ice extent minus the open water area within the ice edge.

☞ **Sea ice concentration**: Amount of sea ice covering an area. Written as the ratio of sea ice to water, either a fraction (8/10) or percentage (80%) of sea ice coverage. <30% sea ice concentration = navigable by ship. >90% is considered solid ice.

- *very open drift* 1–2/10 (10–20%)
- *open to very open drift* 3–4/10 (30–40%)
- *open drift* 5–6/10 (50–60%)
- *close pack* 7–8/10 (70–80%)
- *very close pack* 9/10 (90%)
- *compact* 10/10 (100%)

☞ **Sea ice extent**: Total area covered by some amount of sea ice at a given time, including open water between floes. Normally sea ice is considered to be "present" sea ice concentration is >15%. Thus, sea ice extent is the area of sea covered by at least 15% ice for a specific date.

☞ **Sea ice maximum extent**: Day of the year when the sea ice covers the largest area of the Arctic (or Antarctic).

☞ **Sea ice minimum extent**: Day of the year when the sea ice covers the smallest area of the Arctic (or Antarctic).

☞ **Sea ice thickness**: Average thickness from sea ice surface-to-underside of a specified sea ice extent. Can be measured directly by coring or drilling, but satellites allow for faster collection of thickness data.

☞ **Second-year ice**: Sea ice that has not melted in the first summer of its existence. By the end of the second winter, it attains an ice thickness of 2 m or more and rises higher out of the water than first-year ice.

☞ **Shore lead** : A stretch of navigable water between pack ice and the shore. Vessel capability determines navigability of sea ice.

☞ **Summer minimum extent**: The permanent ice zone that remains in summer after all melting has occurred.

☞ **Very close pack ice**: Pack ice where sea ice concentration >9/10 (90%), and floes are tightly packed to frozen together. Very little, if any, seawater is visible.

Appendix C

STPA and STAMP terminology

To describe STPA and STAMP precisely it is essential to have a clear and mutual understanding of what is meant using different terms, so definitions of the most important terms as they are used in Leveson (2012) and Leveson and Thomas (2018) are mentioned here:

☞ **Accident**: An undesired and unplanned event that results in a loss (including loss of human life or injury, property damage, environmental pollution, and so on).

☞ **Control structure**: A system model that is composed of feedback control loops. An effective control structure will enforce constraints on the behaviour of the overall system.

☞ **Controller constraint**: a controller constraint specifies the controller behaviours that need to be satisfied to prevent UCAs.

☞ **Hazard**: A system state or set of conditions that, together with a particular set of worst-case environment conditions, will lead to an accident (loss).
<Hazard specification> = <System>&<Unsafe Condition>&<Link to Losses (Loss or Accident ID>

☞ **Loss**: involves something of value to stakeholders. Losses may include loss of human life or human injury, property damage, environmental pollution, loss of mission, loss of reputation, loss or leak of sensitive information, or any other loss that is unacceptable to the stakeholders.

☞ **Loss scenario**: describes the causal factors that can lead to the unsafe control actions and to hazards.

☞ **Safety constraints**: are imposed on systems to prevent hazards and accidents
<Safety constraint> = <System>&<Condition to Enforce>&<Link to Hazards (Hazard ID)>

☞ **System**: is a set of components that act together as a whole to achieve some common goal, objective, or end. A system may contain subsystems and may also be part of a larger system.

☞ **System-level constraint**: specifies system conditions or behaviours that need to be satisfied to prevent hazards (and ultimately prevent losses).

☞ **Unsafe control action (UCA)**: a control action that, in a particular context and worst-case environment, will lead to a hazard.
<UCA> = <Source>&<Type>&<Control Action>&<Context>&<Link to Hazards (Hazard ID)>

Appendix D

STPA Case Study

The STPA case study identified many loss scenarios, and Table D.1-D.11 contains all 243 loss scenarios and 551 countermeasures related to the 11 identified UCAs.

Table D.1: Loss scenarios UCA.1 and countermeasures

UCA.1: Water cannon/towing is not provided when a threatening iceberg is approaching the FPSO [H.1]	
Loss scenarios	**Suggested countermeasures**
LS.A.1-UCA.1: The IM team's communication system has failed, so the IM team are not able to request water cannon/towing. As result, a threatening iceberg that exceeds certain kinetic energy drifts towards the FPSO, and may collide if FPSO does not disconnect [H1]	CM1.1 CM6.9
LS.A.2-UCA.1: The IMV receives command from IM team to use water cannon/towing on an iceberg, but one out of two engines fails so the IMV are unable to catch up with the iceberg. As result, [...] [H1]	CM1.2 CM2.1 CM3.1, CM3.2, CM3.3 CM6.10
LS.B.3-UCA.1: The IM team's communication system does not function because of power failure, so the IM team are not able to request water cannon/towing. As result, [...] [H1]	CM1.1 CM6.9
LS.B.4-UCA.1: The IMV receives command from IM team to use water cannon/towing on an iceberg, but then suffers from a power failure so the IMV are unable to provide water cannon/towing. As a result, [...] [H1]	CM1.1 CM6.10

LS.C.5-UCA.1: The IM team does not detect a threatening iceberg, and as a consequence the IMV is never commanded to start water cannon/towing. As a result, [...] [H1]	CM3.4 CM4.1 CM5.1 CM8.2
LS.C.6-UCA.1: The IMV receives command from IM team to use water cannon/towing, but the IMV human operator passes on the wrong coordinates and the iceberg is not located. As a result, [...] [H1]	CM4.1 CM5.1 CM6.1
LS.D.7-UCA.1: The IM team detects a threatening iceberg, but human operators in IM team assumes that someone else sends command to IMV to use water cannon/towing. As a result, [...] [H1]	CM6.1
LS.D.8-UCA.1: The IMV receives command from IM team to use water cannon/towing, but it is not specified where the iceberg is located or how urgent it is, so the iceberg is never managed as it is assumed that further information will be sent when they must act. As a result, [...] [H1]	CM6.1
LS.D.9-UCA.1: The IMV receives command from IM team to use water cannon/towing on an iceberg, but fail to find the specific iceberg. As result, [...] [H1]	CM4.1 CM5.1 CM6.1
LS.E.10-UCA.1: The IM team's local system (to locate/evaluate icebergs) becomes more inaccurate over time, and eventually it is so inaccurate that all threatening icebergs are not detected. The IM team does not request water cannon/towing. As a result, [...] [H1]	CM4.1 CM5.1 CM6.2 CM8.2
LS.E.11-UCA.1: The IMV local system (to locate icebergs) becomes more inaccurate over time, and eventually it is inaccurate enough for the IMV to fail to locate the iceberg. As a result, [...] [H1]	CM2.2 CM4.1 CM5.1 CM6.2

LS.F.12-UCA.1: The IM team's local system (to locate/evaluate icebergs) does not detect an iceberg that is threatening, because one of the sensors in the sensor platform have failed. The IM team does not request water cannon/towing. As a result, [...] [H1]	CM2.2 CM3.4 CM4.1 CM5.1 CM6.2 CM8.2
LS.F.13-UCA.1: The IM team's local system (to locate/evaluate icebergs) does not detect an iceberg that is threatening, because one of the sensors in the sensor platform does not manage to attain data due to weather conditions. The IM team does not request water cannon/towing. As a result, [...] [H1]	CM4.1 CM5.1 CM6.9 CM8.2
LS.F.14-UCA.1: The IMV sees an iceberg on the local system (to locate icebergs), but does not receive command from IM team to use water cannon/towing, and assumes that it is a non-threatening iceberg and decides to not manage iceberg. As a result, [...] [H1]	CM6.3
LS.G.15-UCA.1: The IM team's local system (to locate/evaluate icebergs) detects a threatening iceberg, but the IM team human operator disagrees that the iceberg needs to be managed, and ignores the information. As a result, [...] [H1]	CM6.4
LS.G.16-UCA.1: The IM team's local system (to locate/evaluate icebergs) detects a threatening iceberg, but IM team human operator wrongly assumes that IMV are already occupied with an iceberg, so the command is not sent. As a result, [...] [H1]	CM6.4
LS.G.17-UCA.1: The IM team's local system (to locate/evaluate icebergs) detects a threatening iceberg, but the IM team human operator are occupied with other tasks and fails to command IMV to use water cannon/towing. As a result, [...] [H1]	CM7.1

LS.G.18-UCA.1: The IMV receives command from IM team to use water cannon/towing, but does not see the iceberg on the local system (to locate icebergs), and decides to not proceed to locate and manage iceberg. As a result, [...] [H1]	CM6.1, CM6.5, CM6.7
LS.G.19-UCA.1: The IMV receives command from IM team to manage an iceberg/different iceberg, but the human operator wrongly assumes that the new command can wait, and continues to manage a different iceberg first instead of leaving it immediately. When available to manage a new iceberg the human operator have forgotten the new command. As a result, [...] [H1]	CM6.1, CM6.5, CM6.6, CM6.7
LS.G.20-UCA.1: The IMV receives command from IM team to use water cannon/towing, but the human operator are occupied with other tasks and fails to inform the rest of IMV to locate iceberg and commence water cannon/towing. As a result, [...] [H1]	CM6.1, CM6.7
LS.G.21-UCA.1: The IMV receives command from IM team to use water cannon/towing, but the human operator disagrees that the iceberg in the command needs to be managed, and ignores the command. As a result, [...] [H1]	CM6.1, CM6.5, CM6.7
LS.G.22-UCA.1: The IMV receives command from IM team to use water cannon/towing on an iceberg, but are already occupied with a different iceberg so the command is ignored. As a result, [...] [H1]	CM6.1, CM6.5, CM6.7
LS.H.23-UCA.1: The IMV does not receive command from IM team because human operator are not with the communication system when the message is sent, and the command is only sent once. As a result, [...] [H1]	CM6.1, CM6.8

LS.H.24-UCA.1: The IMV does not receive command from IM team because human operator are busy with other tasks when the message is sent and does not perceive the command, and the command is only sent once. As a result, [...] [H1]	CM6.1, CM6.8
LS.H.25-UCA.1: The IMV does not receive command from IM team because human operator have turned off/not turned on the communication system. As a result, [...] [H1]	CM6.1, CM6.8 CM7.2
LS.H.26-UCA.1: The IMV does not receive command from IM team because the communication system has failed. As a result, [...] [H1]	CM6.1, CM6.8
LS.I.27-UCA.1: Water cannon/towing simultaneous component failure. As a result, [...] [H1]	CM1.3 CM2.3 CM6.10
LS.I.28-UCA.1: Water cannon/towing simultaneous malfunction due to frost problems. As a result, [...] [H1]	CM6.10 CM7.3
LS.I.29-UCA.1: Water cannon/towing are not efficient (negligible effect) due to wind direction. As a result, [...] [H1]	CM6.10

Table D.1 shows 29 loss scenarios and 77 suggested countermeasures identified for UCA.1.

Table D.2: Loss scenarios UCA.2 and countermeasures

UCA.2: Water cannon/towing is provided on a less critical iceberg instead of a more critical iceberg [H.1, H.3]	
Loss scenarios	**Suggested countermeasures**
LS.A.1-UCA.2: The IM team's communication system is flawed, and location to the wrong iceberg is given. As result, a threatening iceberg that exceeds certain kinetic energy drifts towards the FPSO, and may collide if FPSO does not disconnect [H1] and resources have been wasted [H3]	CM1.1 CM6.1
LS.B.2-UCA.2: The IM team's communication system does not function because of power failure. IM team sends request in an alternative way, but it is not sent correctly, and IMV locates wrong iceberg. As a result, [...] [H1, H3]	CM1.1 CM6.1, CM6.6
LS.B.3-UCA.2: The IMV receives command from IM team to use water cannon/towing, but the local system (to locate icebergs) then suffers from a power failure. Without this system the IMV (often) locates the wrong iceberg and starts water cannon/towing. As a result, [...] [H1, H3]	CM1.4 CM5.2 CM6.1, CM6.6
LS.C.4-UCA.2: The IM team detects several icebergs, and requests water cannon/towing on these, but not in a prioritised order. As a result, [...] [H1, H3]	CM6.1, CM6.4
LS.C.5-UCA.2: The IMV receives command from IM team to use water cannon/towing, but the IMV human operator passes on the wrong coordinates and the wrong iceberg located. As a result, [...] [H1, H3]	CM6.1, CM6.6, CM6.7
LS.D.6-UCA.2: The IM team detects a several icebergs, but human operators in IM team are not able to determine which icebergs are most critical, and request IMV to use water cannon/towing in an arbitrary order. As a result, [...] [H1, H3]	CM6.4, CM6.6, CM6.9

LS.D.7-UCA.2: The IMV receives command from IM team to use water cannon/towing on the iceberg with most kinetic energy, and IMV follows the order. However, a different iceberg with less kinetic energy is very close and in fact the most critical iceberg. As a result, [...] [H1, H3]	CM4.1, CM4.2, CM4.3
LS.D.8-UCA.2: The IMV receives command from IM team to use water cannon/towing on a set of icebergs in prioritised order, but the order changes after some time due to changes in weather, and the IMV does not receive an updated list. As a result, [...] [H1, H3]	CM6.4, CM6.6, CM6.7, CM6.11
LS.D.9-UCA.2: The IMV receives command from IM team to use water cannon/towing, but locates wrong iceberg and start to use water cannon/towing on a less critical iceberg. As result, [...] [H1, H3]	CM6.1, CM6.6, CM6.7
LS.E.10-UCA.2: The IM team's local system (to locate/evaluate icebergs) becomes more inaccurate over time due to new sensor platforms, and eventually it is so inaccurate that it is ineffective in determining which icebergs are most critical. As a result, [...] [H1, H3]	CM4.1, CM4.4 CM6.2
LS.E.11-UCA.2: The IM team's local system (to locate/evaluate icebergs) becomes more inaccurate over time due to degrading sensor platforms, and eventually it is so inaccurate that it is ineffective in determining which icebergs are most critical. As a result, [...] [H1, H3]	CM2.2 CM4.1 CM6.2
LS.E.12-UCA.2: The IMV local system (to locate icebergs) becomes more inaccurate over time, and eventually it is inaccurate enough for the IMV to locate the wrong iceberg. As a result, [...] [H1, H3]	CM2.2 CM4.1 CM6.1, CM6.2, CM6.6, CM6.7, CM6.9

LS.F.13-UCA.2: The IM team's local system (to locate/evaluate icebergs) wrongly detects an iceberg and identifies it as threatening, because one of the sensors in the sensor platform have failed. As a result, [...] [H1, H3]	CM2.2 CM3.4 CM6.9
LS.F.14-UCA.2: The IM team's local system (to locate/evaluate icebergs) wrongly detects an iceberg and identifies it as threatening, because one of the sensors in the sensor platform does not manage to attain data due to weather conditions. As a result, [...] [H1, H3]	CM6.4, CM6.9 CM8.2
LS.F.15-UCA.2: The IMV receives command from IM team to use water cannon/towing on an iceberg, but it is in fact not the most critical iceberg (with respect to kinetic energy). As a result, [...] [H1, H3]	CM4.1 CM6.4, CM6.6
LS.G.16-UCA.2: The IM team's local system (to locate/evaluate icebergs) detects a threatening iceberg, but the IM team human operator wrongly assumes that the IMV are not already managing an iceberg. IM team sends command to use water cannon/towing, and the IMV leaves a more critical iceberg. As a result, [...] [H1, H3]	CM6.1, CM6.4
LS.G.17-UCA.2: The IM team's local system (to locate/evaluate icebergs) detects changes in how threatening icebergs are, but the IM team human operator disagrees, and ignores the information. As a result, [...] [H1, H3]	CM6.4
LS.G.18-UCA.2: The IM team's local system (to locate/evaluate icebergs) detects a threatening iceberg, but IM team human operator wrongly assumes that IMV are occupied with a more critical iceberg, so the command is not sent. As a result, [...] [H1, H3]	CM6.4

LS.G.19-UCA.2: The IMV receives command from IM team to use water cannon/towing on a set of icebergs in prioritised order, but the IMV human operator does not follow the prioritisation because it is more convenient to manage the icebergs in a different order. As a result, [...] [H1, H3]	CM6.5, CM6.7
LS.G.20-UCA.2: The IMV receives command from IM team to use water cannon/towing on a set of icebergs in prioritised order, but the IMV human operator disagrees with the recommended prioritised order, and does not listen to the IM team. As a result, [...] [H1, H3]	CM6.1, CM6.5, CM6.7
LS.G.21-UCA.2: The IMV receives command from IM team to use water cannon/towing on a set of icebergs in prioritised order, but the IMV human operator misunderstands the prioritised order, and manages at least one iceberg in the wrong order. As a result, [...] [H1, H3]	CM6.1, CM6.5, CM6.7
LS.G.22-UCA.2: The IMV receives command from IM team to use water cannon/towing on an iceberg, but are already occupied with a different iceberg so the command is ignored. As a result, [...] [H1, H3]	CM6.5, CM6.7
LS.H.23-UCA.2: The IM team's local system (to locate/evaluate icebergs) detects changes in how threatening icebergs are, but the IM team human operator are occupied with other tasks and fails to command IMV to change prioritisation. As a result, [...] [H1, H3]	CM4.1 CM7.1
LS.H.24-UCA.2: The IM team's local system (to locate/evaluate icebergs) does not detect changes in how threatening icebergs are, because one of the sensors in the sensor platform does not manage to send data due to weather conditions. As a result, [...] [H1, H3]	CM4.1 CM7.1 CM8.2

LS.H.25-UCA.2: The IMV does not receive command from IM team to change prioritisation because human operator are not with the communication system when the message is sent, and the command is only sent once. As a result, [...] [H1, H3]	CM6.8 CM7.7
LS.H.26-UCA.2: The IMV does not receive command from IM team to change prioritisation because human operator are busy with other tasks when the message is sent and does not perceive the command, and the command is only sent once. As a result, [...] [H1, H3]	CM6.8 CM7.7
LS.H.27-UCA.2: The IMV does not receive command from IM team to change prioritisation because human operator have turned off/not turned on the communication system. As a result, [...] [H1, H3]	CM1.1 CM6.8 CM7.7
LS.H.28-UCA.2: The IMV does not receive command from IM team to change prioritisation because the communication system has failed. As a result, [...] [H1, H3]	CM1.1 CM6.8
LS.J.29-UCA.2: IMV receives command from IM team to use water cannon/towing, but the towing equipment is stuck to an iceberg. As a result, [...] [H1, H3]	CM6.10 CM7.4

Table D.2 shows 29 loss scenarios and 79 suggested countermeasures identified for UCA.2.

Table D.3: Loss scenarios UCA.3 and countermeasures

UCA.3: Water cannon/towing is provided too late, both iceberg or IMV may collide with FPSO [H.1]	
Loss scenarios	**Suggested countermeasures**
LS.A.1-UCA.3: The IM team's communication system is flawed, and an imprecise location of the iceberg is given. The IMV does not locate it immediately. As result, a threatening iceberg that exceeds certain kinetic energy drifts towards the FPSO, and may collide if FPSO does not disconnect [H1]	CM1.1 CM6.1, CM6.6, CM6.10
LS.A.2-UCA.3: The IMV receives command from IM team to use water cannon/towing on an iceberg, but one out of two engines fails so the IMV arrives to late at the iceberg. As result, [...] [H1]	CM1.2 CM2.1 CM3.1, CM3.2 CM6.10
LS.B.3-UCA.3: The IM team's communication system does not function because of power failure. IM team sends request in an alternative way, but it is not sent correctly, and IMV takes longer time to locate iceberg. As a result, [...] [H1]	CM1.1 CM6.1
LS.B.4-UCA.3: The IMV receives command from IM team to use water cannon/towing, but the local system (to locate icebergs) then suffers from a power failure. Without this system the IMV spends longer time to locate the iceberg and start water cannon/towing. As a result, [...] [H1]	CM6.14
LS.C.5-UCA.3: The IM team detects a threatening iceberg, and requests water cannon/towing on this, but underestimates the distance between IMV and iceberg. As a result, [...] [H1]	CM6.2, CM6.7, CM6.15
LS.C.6-UCA.3: The IM team detects a threatening iceberg, and requests water cannon/towing on this, but underestimates the time needed to manage this iceberg. As a result, [...] [H1]	CM6.2, CM6.7, CM6.15
LS.C.7-UCA.3: The IMV does not have adequate procedures for how to commence water cannon/towing. As a result, [...] [H1]	CM5.3

LS.D.8-UCA.3: The IM team gives command to use water cannon/towing on a set of icebergs in a prioritised order, but it is not enough time to manage all icebergs adequately. As a result, [...] [H1]	CM4.3 CM6.1, CM6.4, CM6.6, CM6.7
LS.D.9-UCA.3: The IM team gives command to use water cannon/towing on a set of icebergs in a prioritised order, but the order changes due to changes in weather, and the IMV does not have time to manage all icebergs adequately. As a result, [...] [H1]	CM6.4, CM6.6, CM6.7, CM6.11
LS.D.10-UCA.3: The IMV receives command to use water cannon/towing on an iceberg, but does not respond immediately. As a result, [...] [H1]	CM6.1 CM7.7
LS.D.11-UCA.3: The IMV receives command from IM team to use water cannon/towing, but struggles to locate the correct iceberg immediately. As result, [...] [H1]	CM6.1, CM6.6 CM7.7
LS.E.12-UCA.3: The IM team's local system (to locate/evaluate icebergs) becomes more inaccurate over time due to degrading sensor platforms, and eventually it is so inaccurate that it is ineffective in determining how much time is needed to manage an iceberg. As a result, [...] [H1]	CM2.2 CM4.4 CM6.2, CM6.7
LS.E.13-UCA.3: The IM team's local system (to locate/evaluate icebergs) becomes more inaccurate over time because it does not account for reduced speed of IMVs, and eventually the system underestimates how much time is needed to manage icebergs. As a result, [...] [H1]	CM1.2 CM2.1 CM4.4 CM6.2, CM6.7
LS.E.14-UCA.3: The IM team's local system (to locate/evaluate icebergs) becomes more inaccurate over time because it does not account for reduced force of water cannon, and eventually the system underestimates how much time is needed to manage icebergs. As a result, [...] [H1]	CM1.3 CM2.3 CM4.4 CM6.2, CM6.7

LS.E.15-UCA.3: The IMV engine becomes less efficient over time (loss of horsepower) and does not navigate as fast as it used to do. Therefore, the IMV started using water cannon/towing too late. As a result, [...] [H1]	CM1.2 CM2.1 CM4.4 CM6.2, CM6.7
LS.E.16-UCA.3: The IMV water cannon becomes less efficient over time (loss of pressure), and needs more time that originally to manage an iceberg. This is not accounted for, and therefore the IMV started using water cannon/towing too late. As a result, [...] [H1]	CM1.3 CM2.3 CM4.4 CM6.2, CM6.7
LS.E.17-UCA.3: The IMV human operators are changed out over time, leaving a less experienced team. Over time, the team is less qualified and spends more time to manage icebergs than planned for. Therefore, the IMV started using water cannon/towing too late. As a result, [...] [H1]	CM5.1, CM5.3 CM6.7
LS.F.18-UCA.3: The IMV receives command from IM team to use water cannon/towing on an iceberg, but the iceberg is much closer than they are told, so the IMV human operator plans to arrive at the iceberg too late. As a result, [...] [H1]	CM4.1, CM4.2 CM6.1, CM6.7, CM6.15
LS.G.19-UCA.3: The IM team's local system (to locate/evaluate icebergs) detects changes in how threatening icebergs are, but the IM team human operator disagrees, and ignores the information. The human operator changes his mind after a while, but it is too late. As a result, [...] [H1]	CM6.4
LS.G.20-UCA.3: The IM team's local system (to locate/evaluate icebergs) detects a threatening iceberg, but IM team human operator wrongly assumes that IMV are occupied with a more critical iceberg, so the command is not sent immediately. When the command is sent it is too late. As a result, [...] [H1]	CM6.4

LS.G.21-UCA.3: The IMV receives command from IM team to use water cannon/towing, but the human operator are occupied with other tasks and does not have time to immediately commence the procedure to locate iceberg/start water cannon/towing. As a result, [...] [H1]	CM6.1, CM6.5, CM6.7
LS.G.22-UCA.3: The IMV receives command from IM team to use water cannon/towing, but the human operator wrongly assumes that they can proceed with ongoing tasks before locating iceberg and commencing water cannon/towing. As a result, [...] [H1]	CM6.1, CM6.5, CM6.7
LS.H.23-UCA.3: The IM team's local system (to locate/evaluate icebergs) detects that a previous non-threatening iceberg now are threatening, but the IM team human operator are occupied with other tasks and fails to command IMV to use water cannon/towing on this iceberg immediately. The command is sent too late. As a result, [...] [H1]	CM4.1 CM7.1 CM8.2
LS.H.24-UCA.3: The IM team's local system (to locate/evaluate icebergs) wrongly detects an iceberg and identifies it as non-threatening, because one of the sensors in the sensor platform have failed. Correct information that the iceberg is threatening arrives too late. As a result, [...] [H1]	CM2.2 CM4.1 CM6.3 CM7.1 CM8.2
LS.H.25-UCA.3: The IM team's local system (to locate/evaluate icebergs) wrongly detects an iceberg and identifies it as non-threatening, because one of the sensors in the sensor platform does not manage to attain data due to weather conditions. Correct information that the iceberg is threatening arrives too late. As a result, [...] [H1]	CM3.4 CM4.1

LS.H.26-UCA.3: The IMV does not receive command from IM team to use water cannon/towing, but detects the iceberg on local system (to locate icebergs). However, this occurs too late. As a result, [...] [H1]	CM6.1, CM6.3, CM6.4 CM7.7
LS.H.27-UCA.3: The IMV does not receive command from IM team the first time it is sent because human operator are not with the communication system when the message is sent. As a result, [...] [H1]	CM6.1 CM7.7
LS.H.28-UCA.3: The IMV does not receive command from IM team the first time it is sent because human operator are busy with other tasks when the message is sent. As a result, [...] [H1]	CM6.1 CM7.7
LS.J.29-UCA.3: The IMV receives command from IM team to use water cannon/towing on iceberg and successfully locates iceberg, but water cannon/towing does not start immediately because of problems with actuators. As a result, [...] [H1]	CM1.3 CM2.3 CM6.10
LS.J.30-UCA.3: The IMV receives command from IM team to use water cannon/towing on iceberg and successfully locates iceberg, but water cannon/towing does not start immediately because of inexperience of the human operators. As a result, [...] [H1]	CM5.3

Table D.3 shows 30 loss scenarios and 95 suggested countermeasures identified for UCA.3.

Table D.4: Loss scenarios UCA.4 and countermeasures

UCA.4: Water cannon/towing is provided too long, potentially not enough time for other icebergs [H.1, H.3]	
Loss scenarios	**Suggested countermeasures**
LS.B.1-UCA.4: The IMVs local system (to calculate future location of iceberg) suffers from power failure, and IMV human operator keeps on using water cannon/towing to ensure that the new trajectory is safe. As result, a threatening iceberg that exceeds certain kinetic energy drifts towards the FPSO, and may collide if FPSO does not disconnect [H1] and resources have been wasted [H3]	CM6.14
LS.C.2-UCA.4: The IMV does not have adequate procedures for how to stop water cannon/towing. As a result, [...] [H1, H3]	CM5.3
LS.D.3-UCA.4: The IMV receives command to use water cannon/towing, but does not have a way to determine when water cannon/towing have been used long enough. Therefore icebergs are managed longer than necessary. As result, [...] [H1, H3]	CM6.6, CM6.14
LS.D.4-UCA.4: The IMV does not have a adequate local system (to locate/evaluate icebergs) to determine when water cannon/towing may be stopped. Therefore icebergs are managed longer than necessary. As a result, [...] [H1, H3]	CM6.6, CM6.14
LS.E.5-UCA.4: The IM team's local system (to locate/evaluate icebergs) becomes more precise over time due to replacement and/or upgrade of sensor platforms. Eventually it underestimates how good the information sent is, and icebergs are managed more efficiently than before. The IMV does not trust that the iceberg is non-threatening at once, and continues water cannon/towing longer than necessary. As a result, [...] [H1, H3]	CM4.4, CM6.7

LS.E.6-UCA.4: The IM team's local system (to locate/evaluate icebergs) does not take into account that the IMVs have been upgraded and have increased speed. The icebergs are managed more efficiently than before. The IMV does not trust that the iceberg is non-threatening at once, and continues water cannon/towing longer than necessary. As a result, [...] [H1, H3]	CM4.4, CM6.7
LS.E.7-UCA.4: The IM team's local system (to locate/evaluate icebergs) does not take into account that the water cannons have been upgraded. The icebergs are managed more efficiently than before. The IMV does not trust that the iceberg is non-threatening at once, and continues water cannon/towing longer than necessary. As a result, [...] [H1, H3]	CM4.4, CM6.7
LS.F.8-UCA.4: The IMV's local system (to locate/evaluate icebergs) wrongly indicates that water cannon/towing must proceed. As a result, [...] [H1, H3]	CM6.7
LS.F.9-UCA.4: The IMV's local system (to locate/evaluate icebergs) indicates that water cannon/towing may stop, but the IM team wrongly commands the IMV to continue and the IMV human operator listens to the command. As a result, [...] [H1, H3]	CM6.5 CM8.1
LS.F.10-UCA.4: The IM team's local system (to locate/evaluate icebergs) does not take into account the good weather conditions, and the IMV spends shorter time to tow an iceberg than during normal conditions. The IMV is requested to stop towing later than necessary. As a result, [...] [H1, H3]	CM6.6, CM6.16

LS.F.11-UCA.4: The IM team's local system (to locate/evaluate icebergs) does not take into account the good weather conditions, and the IMV spends shorter time to use water cannon on an iceberg than during normal conditions. The IMV is requested to stop using water cannon later than necessary. As a result, [...] [H1, H3]	CM6.6, CM6.16
LS.G.12-UCA.4: The IMV understands feedback and understand that the iceberg is adequately managed, but does not stop to use water cannon/towing to be on the safe side. As a result, [...] [H1, H3]	CM6.5, CM6.7
LS.G.13-UCA.4: The IMV human operator misinterprets information from local system (to calculate future location of iceberg), and manages the iceberg to long when it is not necessary. As a result, [...] [H1, H3]	CM6.5, CM6.7
LS.H.14-UCA.4: The IMV human operator does not receive command from IM team that water cannon/towing may be stopped, and proceeds even though it is not necessary. As a result, [...] [H1, H3]	CM6.14
LS.J.15-UCA.4: The IMV human operator improperly aims water cannon at iceberg. Must use water cannon for a longer period of time than intended. As a result, [...] [H1, H3]	CM5.3 CM6.6, CM6.10
LS.J.16-UCA.4: The IMV human operator improperly attaches towing equipment, so the IMV must navigate slower than theoretically possible. As a result, [...] [H1, H3]	CM5.3 CM6.6, CM6.10

Table D.4 shows 16 loss scenarios and 30 suggested countermeasures identified for UCA.4.

Table D.5: Loss scenarios UCA.5 and countermeasures

UCA.5: Water cannon/towing is provided in dangerous weather conditions [H.1, H.4]	
Loss scenarios	**Suggested countermeasures**
LS.A.1-UCA.5: The IMV local system (to locate icebergs) malfunction due to component failure, so the IMV human operator does not have necessary information to determine if it is safe to use water cannon/towing. Water cannon/towing us used during dangerous weather conditions. As result, a threatening iceberg that exceeds certain kinetic energy drifts towards the FPSO, and may collide if FPSO does not disconnect [H1] and the IMV and its crew inflicted with unnecessary risk [H4]	CM4.5
LS.A.2-UCA.5: The IMV are using water cannon/towing in safe weather conditions. The local system and communication system are linked together and malfunctions due to component failure, and the IMV can not detect that the weather conditions are changing. As a result, [...] [H1, H4]	CM1.1 CM4.5 CM6.12
LS.B.3-UCA.5: The IMV local system (to locate icebergs) suffers from power failure, so the IMV human operator does not have necessary information to determine if it is safe to use water cannon/towing. Water cannon/towing us used during dangerous weather conditions. As result, [...] [H1, H4]	CM4.5 CM6.12
LS.B.4-UCA.5: The IMV are using water cannon/towing in safe weather conditions. The local system and communication system suffers from power failure, and the IMV can not detect that the weather conditions are changing. As a result, [...] [H1, H4]	CM6.12

LS.C.5-UCA.5: The IM team detects a threatening iceberg and commands IMV to use water cannon/towing instead of commanding FPSO to disconnect and evade when the IM team knows the weather conditions are dangerous. The IMV follows the command even though they know it is dangerous. As a result, [...] [H1, H4]	CM4.5 CM6.12, CM6.15
LS.D.6-UCA.5: The IM team detects a threatening iceberg and commands IMV to use water cannon/towing instead of commanding FPSO to disconnect and evade. The procedures are not conservative enough, and say that the weather conditions are safe when they in fact are dangerous. As a result, [...] [H1, H4]	CM4.5 CM6.12, CM6.15
LS.D.7-UCA.5: The IM team has commanded IMV to use water cannon/towing, and does not withdraw the command when weather conditions are becoming dangerous. As a result, [...] [H1, H4]	CM4.5 CM6.12
LS.D.8-UCA.5: The IMV has received a command to use water cannon/towing from IM team, and IMV human operator does not abandon mission when weather conditions are becoming dangerous. As a result, [...] [H1, H4]	CM4.5 CM6.12
LS.E.9-UCA.5: The IMVs in the fleet are changed out, and does not have the same ice class as previous IMVs. This is not taken into account in the procedures, and the new IMVs are commanded to use water cannon/towing in weather conditions that are dangerous for these IMVs. As a result, [...] [H1, H4]	CM4.4
LS.F.10-UCA.5: The IMV local system (to locate icebergs) and also weather information receives flawed information, because one of the sensors in the sensor platform does not manage to attain data due to weather conditions. As a result, [...] [H1, H4]	CM6.12

LS.G.11-UCA.5: The IMV receive all necessary information, but interprets it incorrectly and assumes that the weather conditions are good. As a result, [...] [H1, H4]	CM6.12
LS.G.12-UCA.5: The IMV receive all necessary information, and understands that the weather conditions are dangerous, but the IMV human operator are overconfident and takes the risk to use water cannon/towing. As a result, [...] [H1, H4]	CM4.5 CM6.12
LS.H.13-UCA.5: The IMV local system (to locate icebergs) and also weather information receives this too late, because one of the sensors in the sensor platform does not manage to send data immediately due to weather conditions. Decision to use water cannon/towing must be made without all the information, and sometimes the least efficient method is selected. As a result, [...] [H1, H4]	CM4.5 CM5.3 CM6.12
LS.H.14-UCA.5: The IMV local system (to locate icebergs) and also weather information never receives this, because one of the sensors in the sensor platform does not manage to send data immediately because it is broken. Decision to use water cannon/towing must be made without all the information, and sometimes the least efficient method is selected. As a result, [...] [H1, H4]	CM2.2 CM5.3
LS.J.15-UCA.5: The IMV provides water cannon/towing in dangerous weather, and the IMV human operators on deck are injured because of the harsh weather. As a result, [...] [H1, H4]	CM4.5 CM6.12
LS.J.16-UCA.5: The IMV provides water cannon/towing in dangerous weather, and the IMV human operators are thrown off deck because of the harsh weather. As a result, [...] [H1, H4]	CM4.5 CM6.12
LS.J.17-UCA.5: The IMV provides towing in high waves, and the towing equipment breaks. The iceberg are not managed. As a result, [...] [H1, H4]	CM4.5 CM6.12

LS.J.18-UCA.5: The IMV provides towing in high waves, and it is not efficient because of the harsh weather. The iceberg are not managed. As a result, [...] [H1, H4]	CM4.5 CM6.12
LS.J.19-UCA.5: The IMV provides water cannon in high waves and strong winds, and the pump takes in air when the IMV is above water in harsh weather. The water cannon equipment breaks. The iceberg are not managed. As a result, [...] [H1, H4]	CM4.5 CM6.12

Table D.5 shows 19 loss scenarios and 37 suggested countermeasures identified for UCA.5.

Table D.6: Loss scenarios UCA.6 and countermeasures

UCA.6: Water cannon/towing is stopped too soon. Iceberg still threatening [H.1]	
Loss scenarios	**Suggested countermeasures**
LS.A.1-UCA.6: The IMV engine suffers from component failure when using water cannon/towing, and water cannon/towing is stopped too early. As result, a threatening iceberg that exceeds certain kinetic energy drifts towards the FPSO, and may collide if FPSO does not disconnect [H.1]	CM1.2 CM2.1 CM6.10
LS.B.2-UCA.6: The IMV engine suffers from power failure when using water cannon/towing, and water cannon/towing is stopped too early. As result, [...] [H1]	CM1.2 CM6.7, CM6.10
LS.D.3-UCA.6: The IMV does not have a adequate local system (to locate/evaluate icebergs) to determine when water cannon/towing may be stopped. Therefore icebergs sometimes are not managed long enough. As a result, [...] [H1]	CM6.6
LS.E.4-UCA.6: The IM team's local system (to locate/evaluate icebergs) becomes more inaccurate over time because it does not account for reduced speed of IMVs, and eventually the system underestimates how much time is needed to manage icebergs. The IM team commands IMV to stop using water cannon/towing too soon. As a result, [...] [H1]	CM2.1 CM6.2
LS.E.5-UCA.6: The IM team's local system (to locate/evaluate icebergs) becomes more inaccurate over time because it does not account for reduced force of water cannon, and eventually the system underestimates how much time is needed to manage icebergs. The IM team commands IMV to stop using water cannon/towing too soon. As a result, [...] [H1]	CM2.3 CM6.2

LS.E.6-UCA.6: The IMV engine becomes less efficient over time (loss of horsepower) and does not navigate as fast as it used to do. This is not accounted for, and therefore the IMV local system (to locate/evaluate icebergs) are not conservative enough. As a result, [...] [H1]	CM2.1 CM6.2
LS.E.7-UCA.6: The IMV water cannon becomes less efficient over time (loss of pressure), and needs more time that originally to manage an iceberg. This is not accounted for, and therefore the IMV local system (to locate/evaluate icebergs) are not conservative enough. As a result, [...] [H1]	CM2.3 CM6.2
LS.F.8-UCA.6: The IM team's local system (to locate/evaluate icebergs) does not take into account the poor weather conditions, and the IMV spends longer time to tow an iceberg than during normal conditions. The IMV is requested to stop towing too soon. As a result, [...] [H1]	CM6.9 CM6.15
LS.F.9-UCA.6: The IM team's local system (to locate/evaluate icebergs) does not take into account the poor weather conditions, and the IMV spends longer time to use water cannon on an iceberg than during normal conditions. The IMV is requested to stop using water cannon too soon. As a result, [...] [H1]	CM6.9 CM6.15
LS.F.10-UCA.6: The IMV's local system (to locate/evaluate icebergs) indicates that water cannon/towing may stop, but the IM team wrongly commands the IMV to stop water cannon/towing and the IMV human operator listens to the command. As a result, [...] [H1]	CM6.9 CM6.15
LS.F.11-UCA.6: The IMV's local system (to locate/evaluate icebergs) wrongly indicates that water cannon/towing must stop. As a result, [...] [H1]	CM6.6 CM6.15

LS.G.12-UCA.6: The IMV understands feedback and understand that the iceberg is not adequately managed, but stops using water cannon/towing because it may be enough. As a result, [...] [H1]	CM6.5, CM6.6
LS.G.13-UCA.6: The IMV human operator misinterprets information from local system (to calculate future location of iceberg), and stops managing the iceberg too early. As a result, [...] [H1]	CM6.5, CM6.6
LS.H.14-UCA6: The IMV human operator stops water cannon/towing on iceberg, but is not requested by IM team to continue even though IM team knows that it still too early. As a result, [...] [H1]	CM6.6
LS.J.15-UCA.6: The IMV human operator improperly aims water cannon at iceberg, but think that it is properly aimed. Must use water cannon for a longer period of time than they the IMV human operator thinks. Water cannon is stopped too soon. As a result, [...] [H1]	CM5.3 CM6.6
LS.J.16-UCA.6: The IMV human operator improperly attaches towing equipment, but think that it is properly attached. Must tow iceberg for a longer period of time than the IMV human operator thinks. Towing is stopped too soon. As a result, [...] [H1]	CM5.3 CM6.6

Table D.6 shows 16 loss scenarios and 32 suggested countermeasures identified for UCA.6.

Table D.7: Loss scenarios UCA.7 and countermeasures

UCA.7: The least efficient method of water cannon/towing is used to manage an iceberg [H.1, H.3]	
Loss scenarios	**Suggested countermeasures**
LS.A.1-UCA.7: The IMV local system (to locate icebergs) malfunction due to component failure, so the IMV human operator does not have necessary information to determine if water cannon or towing should be used. May use the least efficient method. As result, a threatening iceberg that exceeds certain kinetic energy drifts towards the FPSO, and may collide if FPSO does not disconnect [H1] and resources have been wasted [H3]	CM5.3 CM6.7, CM6.10
LS.B.2-UCA.7: The IMV local system (to locate icebergs) suffers from power failure, so the IMV human operator does not have necessary information to determine if water cannon or towing should be used. May use the least efficient method. As result, [...] [H1, H3]	CM5.3 CM6.7, CM6.10
LS.C.3-UCA.7: The IMV human operator determines which method is most efficient, but does not decide to use that method. As a result, [...] [H1, H3]	CM5.3 CM6.16
LS.C.4-UCA.7: The IMV human operator determines which method is most efficient under normal conditions, but does not take into account the weather conditions that does affect which method is most efficient. As a result, [...] [H1, H3]	CM5.3 CM6.16
LS.D.5-UCA.7: The IMV local system (to locate icebergs) also used to determine which method of water cannon or towing to use is not capable to take into account the weather conditions, so when weather conditions are changing the least efficient method of water cannon/towing are often used. As result, [...] [H1, H3]	CM5.3 CM6.16

LS.E.6-UCA.7: The IMV procedure to decide which method to use of water cannon/towing does not take into account that the towing equipment can withstand less force after some time, but the IMVs navigate slow enough. The towing method is overestimated. As a result, [...] [H1, H3]	CM5.3 CM6.2, CM6.6, CM6.16
LS.E.7-UCA.7: The IMV procedure to decide which method to use of water cannon/towing does not take into account that the towing equipment have been upgraded/replaced, and can withstand more force. The IMVs navigate in the same tempo as before. The towing method is underestimated. As a result, [...] [H1, H3]	CM4.4 CM6.14
LS.E.8-UCA.7: The IMV procedure to decide which method to use of water cannon/towing does not take into account that the water cannon loses capacity over time, and are less efficient. The water cannon method is overestimated. As a result, [...] [H1, H3]	CM4.4 CM5.3 CM6.6
LS.E.9-UCA.7: The IMV procedure to decide which method to use of water cannon/towing does not take into account that the water cannon have been upgraded/replaced, and have a higher capacity. The water cannon method is underestimated. As a result, [...] [H1, H3]	CM4.4 CM6.14, CM6.16
LS.F.10-UCA.7: The IMV local system (to locate icebergs) and also decide which method to use receives flawed information, because one of the sensors in the sensor platform does not manage to attain data due to weather conditions. As a result, [...] [H1, H3]	CM3.4 CM6.6, CM6.14
LS.G.11-UCA.7: The IMV receive all necessary information, but interprets it incorrectly and chooses the least efficient method of water cannon and towing. As a result, [...] [H1, H3]	CM5.3 CM6.7

LS.G.12-UCA.7: The IMV receives all necessary information, and one of the two methods are clearly most efficient, but the equipment for the other method is already prepared, so the least efficient method is used. As a result, [...] [H1, H3]	CM6.16
LS.H.13-UCA.7: The IMV local system (to locate icebergs) and also decide which method to use receives information too late, because one of the sensors in the sensor platform does not manage to send data immediately due to weather conditions. Decision to use water cannon/towing must be made without all the information, and sometimes the least efficient method is selected. As a result, [...] [H1, H3]	CM3.4 CM5.3 CM6.7
LS.H.14-UCA.7: The IMV local system (to locate icebergs) and also decide which method to use never receives information, because one of the sensors in the sensor platform does not manage to send data immediately because it is broken. Decision to use water cannon/towing must be made without all the information, and sometimes the least efficient method is selected. As a result, [...] [H1, H3]	CM2.2 CM3.4 CM5.3 CM6.7
LS.I.15-UCA.7: The IMV receives all necessary information, and one of the two methods are clearly most efficient, but the equipment that method does not function properly, so the least efficient method must be used. As a result, [...] [H1, H3]	CM5.3
LS.J.16-UCA.7: The IMV receives all necessary information, and one of the two methods are clearly most efficient, if it is properly executed. The IMV human operators are not well trained using this method, so the other method would be more efficient in practice. In practice the least efficient method is used. As a result, [...] [H1, H3]	CM5.3

Table D.7 shows 16 loss scenarios and 39 suggested countermeasures identified for UCA.7.

Table D.8: Loss scenarios UCA.8 and countermeasures

UCA.8: Disconnection and evacuation is not provided when a threatening iceberg is approaching the FPSO [H.1]	
Loss scenarios	**Suggested countermeasures**
LS.A.1-UCA.8: The IM team's communication system has failed, so the IM team are not able to request disconnection and evacuation. As result, a threatening iceberg that exceeds certain kinetic energy drifts towards the FPSO, and may collide if FPSO does not disconnect [H1]	CM1.1
LS.B.2-UCA.8: The IM team's communication system does not function because of power failure, so the IM team are not able to request FPSO to disconnect and evade. As result, [...] [H1]	CM1.1 CM7.5
LS.B.3-UCA.8: The FPSO receives command from IM team to disconnect and evade, but then suffers from a power failure so the FPSO are unable to disconnect and evade. As a result, [...] [H1]	CM7.5
LS.C.4-UCA.8: The IM team does not detect a threatening iceberg, and as a consequence the FPSO is never commanded to disconnect and evade. As a result, [...] [H1]	CM3.4 CM4.1
LS.C.5-UCA.8: The FPSO receives command from IM team to disconnect and evade, but the FPSO human operator does not follow procedure and does not disconnect. As a result, [...] [H1]	CM6.17
LS.D.6-UCA.8: The IM team detects a threatening iceberg, but human operators in IM team assumes that someone else sends command to FPSO to disconnect and evade. As a result, [...] [H1]	CM6.1
LS.D.7-UCA.8: The FPSO receives command from IM team to disconnect and evade, but due to bad procedures and little training the task is not completed. As a result, [...] [H1]	CM5.4 CM6.1

LS.E.8-UCA.8: The IM team's local system (to locate/evaluate icebergs) becomes more inaccurate over time, and eventually it is so inaccurate that all threatening icebergs are not detected. The IM team does not request disconnection and evacuation. As a result, [...] [H1]	CM6.2
LS.F.9-UCA.8: The IM team's local system (to locate/evaluate icebergs) does not detect an iceberg that is threatening, because one of the sensors in the sensor platform have failed. The IM team does not request disconnection and evacuation. As a result, [...] [H1]	CM2.2 CM3.4 CM4.1
LS.F.10-UCA.8: The IM team's local system (to locate/evaluate icebergs) does not detect an iceberg that is threatening, because one of the sensors in the sensor platform does not manage to attain data due to weather conditions. The IM team does not request disconnection and evacuation. As a result, [...] [H1]	CM4.1
LS.F.11-UCA.8: The FPSO does not have a method to monitor icebergs, and does not receive command from IM team to disconnect and evade when a threatening iceberg is approaching. Assumes that everything is safe. As a result, [...] [H1]	CM4.1 CM6.15, CM6.18
LS.G.12-UCA.8: The IM team's local system (to locate/evaluate icebergs) detects a threatening iceberg, but the IM team human operator disagrees that the FPSO needs to disconnect and evade, and ignores the information. As a result, [...] [H1]	CM4.1, CM4.2 CM6.18 CM7.1
LS.G.13-UCA.8: The IM team's local system (to locate/evaluate icebergs) detects a threatening iceberg, but IM team human operator wrongly assumes that the FPSO have already disconnected and evacuated, so the command is not sent. As a result, [...] [H1]	CM4.1, CM4.2 CM6.13, CM6.18 CM7.1

LS.G.14-UCA.8: The IM team's local system (to locate/evaluate icebergs) detects a threatening iceberg, but the IM team human operator are occupied with other tasks and fails to command FPSO to disconnect and evade. As a result, [...] [H1]	CM4.1, CM4.2 CM6.18 CM7.1
LS.G.15-UCA.8: The FPSO receives command from IM team to disconnect and evade, but the human operator wrongly assumes that it is not urgent, and continues operating. When current operation are done the human operator have forgotten the new command. As a result, [...] [H1]	CM6.1, CM6.17
LS.G.16-UCA.8: The FPSO receives command from IM team to disconnect and evade, but the human operator are occupied with other tasks and fails to inform the rest of FPSO to commence disconnection and evacuation. As a result, [...] [H1]	CM6.1, CM6.17 CM7.8
LS.G.17-UCA.8: The FPSO receives command from IM team to disconnect and evade, but the human operator disagrees that the iceberg in the command is threatening (will not collide), and ignores the command. As a result, [...] [H1]	CM6.1, CM6.17 CM7.8
LS.G.18-UCA.8: The FPSO receives command from IM team to disconnect and evade, but the human operator disagrees that the iceberg in the command is threatening (FPSO withstand collision), and ignores the command. As a result, [...] [H1]	CM6.1, CM6.17 CM7.8
LS.G.19-UCA.8: The FPSO receives command from IM team to disconnect and evade, but are occupied with a critical task (e.g. drilling) so the command is ignored. As a result, [...] [H1]	CM6.1, CM6.17 CM7.8

LS.H.20-UCA.8: The IM team's local system (to locate/evaluate icebergs) does not detect an iceberg that is threatening, because one of the sensors in the sensor platform does not manage to send data due to weather conditions. The IM team does not request disconnection and evacuation. As a result, [...] [H1]	CM4.1 CM6.15
LS.H.21-UCA.8: The FPSO does not receive command from IM team because human operator are not with the communication system when the message is sent, and the command is only sent once. As a result, [...] [H1]	CM6.8 CM7.8
LS.H.22-UCA.8: The FPSO does not receive command from IM team because human operator are busy with other tasks when the message is sent and does not perceive the command, and the command is only sent once. As a result, [...] [H1]	CM6.8 CM7.8
LS.H.23-UCA.8: The FPSO does not receive command from IM team because human operator have turned off/not turned on the communication system. As a result, [...] [H1]	CM6.8 CM7.2
LS.H.24-UCA.8: The FPSO does not receive command from IM team because the communication system has failed. As a result, [...] [H1]	CM1.1 CM6.8
LS.I.25-UCA.8: Disconnection and evacuation not possible due to component failure in the disconnection mechanism. As a result, [...] [H1]	CM1.5 CM2.4
LS.I.26-UCA.8: Disconnection and evacuation not possible due to frost problems with the disconnection mechanism. As a result, [...] [H1]	CM1.5 CM7.6

Table D.8 shows 26 loss scenarios and 59 suggested countermeasures identified for UCA.8.

Table D.9: Loss scenarios UCA.9 and countermeasures

UCA.9: Disconnection and evacuation is provided when a threatening iceberg is not approaching the FPSO [H.2]	
Loss scenarios	**Suggested countermeasures**
LS.A.1-UCA.9: The IM team's communication system is flawed and command to disconnect and evade is sent automatically when it is not needed. As a result, the FPSO disconnect and evade when there is no threatening iceberg that exceeds certain kinetic energy and we have loss of production [H2]	CM1.1 CM6.13
LS.A.2-UCA.9: The FPSO disconnection mechanism automatically disconnects itself when it is not needed. As a result, [...] [H2]	CM2.4
LS.C.3-UCA.9: The IM team detects an approaching iceberg, but commands FPSO to disconnect and evade even though the iceberg is non-threatening. As a result, [...] [H2]	CM6.15
LS.C.4-UCA.9: The FPSO decides to disconnect without being specifically told by IM team. As a result, [...] [H2]	CM6.13, CM6.17
LS.D.5-UCA.9: The IM team detects an approaching iceberg that in reality is non-threatening, but the specifications are conservative and ranks the iceberg to be threatening, so the IM team commands FPSO to disconnect and evade. As a result, [...] [H2]	CM6.15
LS.D.6-UCA.9: The FPSO receives command from IM team prepare to disconnect and evade in some hours, but the FPSO disconnects and evades early, and it was not necessary because the iceberg ended up being non-threatening. As a result, [...] [H2]	CM6.13, CM6.15

LS.E.7-UCA.9: The IM team's local system (to locate/evaluate icebergs) becomes more precise over time due to replacement and/or upgrade of sensor platforms. Eventually it underestimates how good the information sent is, and icebergs are managed more efficiently than before. Command to disconnect and evade are sent too soon (could wait and see that disconnection is unnecessary). As a result, [...] [H2]	CM4.4 CM6.13
LS.E.8-UCA.9: The IM team's local system (to locate/evaluate icebergs) does not take into account that the IMVs have been upgraded and have increased speed. The icebergs are managed more efficiently than before. Command to disconnect and evade are sent too soon (could wait and see that disconnection is unnecessary). As a result, [...] [H2]	CM4.4 CM6.13
LS.E.9-UCA.9: The IM team's local system (to locate/evaluate icebergs) does not take into account that the water cannons have been upgraded. The icebergs are managed more efficiently than before. Command to disconnect and evade are sent too soon (could wait and see that disconnection is unnecessary). As a result, [...] [H2]	CM4.4 CM6.13
LS.F.10-UCA.9: The IM team's local system (to locate/evaluate icebergs) wrongly detects an iceberg and identifies it as threatening, because one of the sensors in the sensor platform have failed. Command to disconnect and evade are sent. As a result, [...] [H2]	CM2.2 CM6.13, CM6.15
LS.F.11-UCA.9: The IM team's local system (to locate/evaluate icebergs) wrongly detects an iceberg and identifies it as threatening, because one of the sensors in the sensor platform does not manage to attain data due to weather conditions. Command to disconnect and evade are sent. As a result, [...] [H2]	CM6.13, CM6.15

LS.F.12-UCA.9: The FPSO wrongly receives a command to disconnect and evade, and does not double check whether or not it is correct, and disconnects and evades. As a result, [...] [H2]	CM6.13, CM6.15
LS.F.13-UCA.9: The FPSO receives command from IM team to disconnect and evade because a threatening iceberg is approaching, but the iceberg were not threatening approaching from that angle. As a result, [...] [H2]	CM6.13, CM6.15
LS.G.14-UCA.9: The IM team's local system (to locate/evaluate icebergs) does not take into account that the weather conditions are very good, and that both navigating IMVs and managing icebergs are easier. The icebergs are managed more efficiently than normal. The command to disconnect and evade are sent too soon. As a result, [...] [H2]	CM6.6, CM6.13
LS.H.15-UCA.9: The IM team's local system (to locate/evaluate icebergs) detects changes in how threatening icebergs are, but the IM team human operator disagrees, and ignores the information. The command to disconnect and evade are not withdrawn. As a result, [...] [H2]	CM6.18
LS.H.16-UCA.9: The FPSO does not receive command from IM team to disconnect and evade, and has no method to detect threatening icebergs itself. Eventually a threatening iceberg is seen with binoculars, but the FPSO does not have enough time to double check with IM team and disconnects and evades to be on the safe side. As a result, [...] [H2]	CM6.13, CM6.18

Table D.9 shows 16 loss scenarios and 29 suggested countermeasures identified for UCA.9.

Table D.10: Loss scenarios UCA.10 and countermeasures

UCA.10: Disconnection and evacuation is provided too early, when it is needed [H.2]	
Loss scenarios	**Suggested countermeasures**
LS.A.1-UCA.10: The IM team's communication system is flawed and command to disconnect and evade is sent automatically too early when it is needed. As a result, the FPSO disconnect and evade when there is no threatening iceberg that exceeds certain kinetic energy and we have loss of production [H2]	CM1.1 CM6.13
LS.A.2-UCA.10: The FPSO disconnection mechanism automatically disconnects itself when it is needed. As a result, [...] [H2]	CM2.4
LS.B.3-UCA.10: The FPSO have received command to prepare to disconnect and evade in a few hours, and when the FPSO suffers from power loss the disconnection mechanism commences because it is a fail-safe system. As a result, [...] [H2]	CM8.1
LS.C.4-UCA.10: The FPSO human operator decides to disconnect without being specifically told by IM team. As a result, [...] [H2]	CM6.13
LS.D.5-UCA.10: The IM team detects a threatening iceberg, but commands FPSO to disconnect and evade too early. As a result, [...] [H2]	CM6.15
LS.D.6-UCA.10: The FPSO receives command from IM team prepare to disconnect and evade in some hours, but the FPSO disconnects and evades immediately. As a result, [...] [H2]	CM6.13
LS.E.7-UCA.10: The IM team's local system (to locate/evaluate icebergs) becomes more precise over time due to replacement and/or upgrade of sensor platforms. Eventually it underestimates how good the information sent is, and icebergs are managed more efficiently than before. Command to disconnect and evade are sent too soon (could wait to disconnect). As a result, [...] [H2]	CM4.4 CM6.13

LS.E.8-UCA.10: The IM team's local system (to locate/evaluate icebergs) does not take into account that the IMVs have been upgraded and have increased speed. The icebergs are managed more efficiently than before. Command to disconnect and evade are sent too soon (could wait to disconnect). As a result, [...] [H2]	CM4.4 CM6.13
LS.E.9-UCA.10: The IM team's local system (to locate/evaluate icebergs) does not take into account that the water cannons have been upgraded. The icebergs are managed more efficiently than before. Command to disconnect and evade are sent too soon (could wait to disconnect). As a result, [...] [H2]	CM4.4 CM6.13
LS.E.10-UCA.10: The IM team's experience over time is that the procedure of when to request disconnection is not conservative enough, and does not listen to the system at all times and commands FPSO to disconnect and evade too early. As result, [...] [H2]	CM6.13
LS.E.11-UCA.10: The FPSO human operators are changed out over time, leaving a less experienced team. Over time, the team is less qualified and commences disconnection too early. Therefore, the FPSO disconnects and evades too early. As a result, [...] [H2]	CM5.4
LS.F.12-UCA.10: The FPSO receives command from IM team to disconnect and evade, but the iceberg is much further away than they are told, so the FPSO human operator plans to disconnect too early. As a result, [...] [H2]	CM6.13

LS.G.13-UCA.10: The IM team's local system (to locate/evaluate icebergs) does not take into account that the weather conditions are very good, and that both navigating IMVs and managing icebergs are easier. The icebergs are managed more efficiently than normal (could wait to disconnect). The command to disconnect and evade are sent too soon. As a result, [...] [H2]	CM6.13
LS.G.14-UCA.10: The FPSO receives command to disconnect and evade too early when it is needed, and have no method to control the quality of the command themselves. Have to trust blindly in the command and can not postpone the disconnection themselves. The FPSO disconnects and evades too early. As a result, [...] [H2]	CM6.13
LS.H.15-UCA.10: The IM team's local system (to locate/evaluate icebergs) detects changes in when a threatening iceberg will arrive, but the IM team human operator disagrees, and ignores the information. The command to disconnect and evade are not postponed. As a result, [...] [H2]	CM6.13, CM6.15
LS.J.16-UCA.10: The FPSO have received command to prepare to disconnect and evade in a few hours, and when the FPSO disconnection has a alarm signal the disconnection mechanism commences because it is a fail-safe system. As a result, [...] [H2]	CM8.1

Table D.10 shows 16 loss scenarios and 21 suggested countermeasures identified for UCA.10.

Table D.11: Loss scenarios UCA.11 and countermeasures

UCA.11: Disconnection and evacuation is provided too late [H.1]	
Loss scenarios	**Suggested countermeasures**
LS.A.1-UCA.11: The IM team's communication system has failed, and request to disconnect and evade is not sent to FPSO immediately. As result, a threatening iceberg that exceeds certain kinetic energy drifts towards the FPSO, and may collide if FPSO does not disconnect [H1]	CM1.1
LS.B.2-UCA.11: The IM team's communication system does not function because of power failure. IM team sends request in an alternative way, but it is not sent correctly, and FPSO takes longer time to disconnect and evade. As a result, [...] [H1]	CM1.1
LS.B.3-UCA.11: The FPSO's communication system suffers from power failure during command from IM team to disconnect and evade, and FPSO attempts to reestablish contact with IM team to verity the command before disconnecting. FPSO disconnect and evade too late. As a result, [...] [H1]	CM1.1
LS.C.4-UCA.11: The IM team detects a threatening iceberg, and overestimates the IMVs capability to manage icebergs. As a result, [...] [H1]	CM4.3 CM6.15
LS.C.5-UCA.11: The IM team detects a threatening iceberg, and underestimates the time needed to safely disconnect and evade. As a result, [...] [H1]	CM4.3 CM6.15
LS.C.6-UCA.11: The IM team's communication system is flawed, and wrong time of latest safe disconnection and evacuation is sent. The FPSO starts disconnecting and evacuation too late. As a result, [...] [H1]	CM1.1 CM6.1, CM6.13
LS.C.7-UCA.11: The FPSO receives command from IM team to disconnect and evade, but does not follow procedure and does not disconnect immediately. As a result, [...] [H1]	CM6.1, CM6.17

LS.C.8-UCA.11: The FPSO receives command from IM team to disconnect and evade, but struggles to disconnect immediately due to inadequate procedures. As result, [...] [H1]	CM5.4 CM6.15
LS.C.9-UCA.11: The FPSO receives command from IM team to disconnect and evade, but struggles to disconnect immediately due to inadequate training/experience of human operators. As result, [...] [H1]	CM5.4 CM6.15
LS.D.10-UCA11: The IM team detects a threatening iceberg, but the set parameters for when to request disconnection and evacuation are not conservative enough. The FPSO receives command too late. As result, [...] [H1]	CM4.1 CM6.15
LS.D.11-UCA.11: The IM team gives command to disconnect and evade, but it is not enough time to disconnect and evade safely. As a result, [...] [H1]	CM4.2, CM4.3 CM6.15
LS.D.12-UCA.11: The FPSO receives command to disconnect and evade, but a critical operation at the FPSO leads to that one can not evacuate as fast as one can in an optimal scenario. The FPSO disconnects too late. As a result, [...] [H1]	CM4.1 CM6.1, CM6.15
LS.D.13-UCA.11: The FPSO receives command from IM team to disconnect and evade, but it is not specified where the iceberg is located or how urgent it is, so the FPSO does not disconnect and evade in in time. As a result, [...] [H1]	CM6.1
LS.E.14-UCA.11: The IM team's experience over time is that the procedure of when to request disconnection is too conservative, and does not listen to the system at all times and waits to long before commanding FPSO to disconnect and evade. As result, [...] [H1]	CM6.18

LS.E.15-UCA.11: The FPSO disconnection system becomes more stuck over time (rust and friction), and the process of disconnecting does not go as fast as it is supposed to. Therefore, the FPSO disconnects and evades too late. As a result, [...] [H1]	CM1.5 CM2.4
LS.E.16-UCA.11: The FPSO human operators are changed out over time, leaving a less experienced team. Over time, the team is less qualified and spends more time to disconnect and evade than planned for. Therefore, the FPSO disconnects and evades too late. As a result, [...] [H1]	CM5.4
LS.F.17-UCA.11: The FPSO receives command from IM team to disconnect and evade, but the iceberg is much closer than they are told, so the FPSO human operator plans to disconnect too late. As a result, [...] [H1]	CM4.1, CM4.2, CM4.3
LS.G.18-UCA.11: The IM team concludes that the IMVs have enough time to manage all icebergs when in fact it was not so. The IM team requests disconnection and evacuation too late. As a result, [...] [H1]	CM4.2, CM4.3
LS.G.19-UCA.11: The IM team does not read the sensor information correctly, and realises too late that disconnection and evacuation is necessary. The FPSO disconnects and evades too late. As result, [...] [H1]	CM4.2, CM4.3
LS.G.20-UCA.11: The IM team's local system (to locate/evaluate icebergs) detects changes in how threatening icebergs are, but the IM team human operator disagrees that disconnection is necessary and ignores the information. The human operator changes his mind after a while, but it is too late to safely disconnect and evade. As a result, [...] [H1]	CM6.18

LS.G.21-UCA.11: The IM team's local system (to locate/evaluate icebergs) does not take into account that the weather conditions are very bad, and that both navigating IMVs and managing icebergs are harder. The icebergs are managed less efficiently than normal. The command to disconnect and evade are sent too late. As a result, [...] [H1]	CM6.7, CM6.10
LS.G.22-UCA.11: The IM team's local system (to locate/evaluate icebergs) detects a threatening iceberg, but IM team human operator wrongly assumes that the FPSO have begun to disconnect. When the IM team human operator realises this and sens command it is too late to safely disconnect and evade. As a result, [...] [H1]	CM6.17 CM7.8
LS.G.23-UCA.11: The FPSO receives command from IM team to disconnect and evade, but does not act immediately because the FPSO human operator are occupied with other tasks. As result, [...] [H1]	CM6.17 CM7.8
LS.G.24-UCA.11: The FPSO receives command from IM team to disconnect and evade, but the FPSO human operators wrongly assumes that they can proceed with ongoing tasks before commencing disconnection and evacuation. As result, [...] [H1]	CM6.17
LS.H.25-UCA.11: The IM team's local system (to locate/evaluate icebergs) detects that a previous non-threatening iceberg now are threatening, but the IM team human operator are occupied with other tasks and fails to command FPSO to disconnect and evade immediately. The command to disconnect and evade is sent too late. As a result, [...] [H1]	CM6.1 CM7.1

LS.H.26-UCA.11: The IM team's local system (to locate/evaluate icebergs) wrongly detects an iceberg and identifies it as non-threatening, because one of the sensors in the sensor platform have failed. Correct information that the iceberg is threatening arrives too late, and the command to disconnect and evade is sent too late. As a result, [...] [H1]	CM2.2 CM3.4
LS.H.27-UCA.11: The IM team's local system (to locate/evaluate icebergs) wrongly detects an iceberg and identifies it as non-threatening, because one of the sensors in the sensor platform does not manage to attain data due to weather conditions. Correct information that the iceberg is threatening arrives too late. The command to disconnect and evade is sent too late. As a result, [...] [H1]	CM3.4
LS.H.28-UCA.11: The FPSO does not receive command from IM team to disconnect and evade, and has no method to detect threatening icebergs itself. As a result, [...] [H1]	CM6.8
LS.H.29-UCA.11: The FPSO does not receive command from IM team the first time it is sent because FPSO human operator are not with the communication system when the message is sent. As a result, [...] [H1]	CM6.1
LS.J.30-UCA.11: The FPSO receives command from IM team to disconnect and evade, but it does not happen immediately because of problems with actuators. As a result, [...] [H1]	CM1.5 CM2.4

Table D.11 shows 30 loss scenarios and 53 suggested countermeasures identified for UCA.11.

Bibliography

Abdulkhaleq, A. and Wagner, S. (2015). A Controlled Experiment for the Empirical Evaluation of Safety Analysis Techniques for Safety-Critical Software. In *International Conference on Evaluation and Assessment in Software Engineering*.

Afenyo, M., Khan, F., Veitch, B., and Yang, M. (2017). Arctic shipping accident scenario analysis using Bayesian Network approach. *Ocean Engineering*, 133:224–230.

AMAP (2011). Map of the NWP and NSR. https://www.amap.no/documents/doc/snow-water-ice-and-permafrost-in-the-arctic-swipa-climate-change-and-the-cryosphere/743.

Atlas (2019). Common terms used in sea ice research. http://seaiceatlas.snap.uaf.edu/glossary.

Balchen, J. G., Andresen, T., and Foss, B. A. (2004). *Reguleringsteknikk*. NTNU-trykk, Trondheim, fifth edition.

Björnsdóttir, S. H. (2017). 5th European STAMP/STPA Workshop and Conference. https://stiki.eu/5th-european-stamp-stpa-workshop-conference/.

Desch, S. J. et al. (2017). Arctic ice management. *Earth's Future*, 5:107–127.

DNVGL (2017). DNV rules for classification of ships. Technical report, DNV GL.

Eicken, H., Jones, J., Meyer, F., Mahoney, A., Druckenmiller, M., Mv, R., and Kambhamettu, C. (2011). Environmental Security in Arctic Ice-Covered Seas: From Strategy to Tactics of Hazard Identification and Emergency Response. *Marine Technology Society Journal*, 45(3):37–48.

Eik, K. and Løset, S. (2009). Specifications for a Subsurface Ice Intelligence System. In *the 28th International Conference on Ocean, Offshore and Arctic Engineering*, volume 5, pages 103–109.

Eik, K. J. (2008). Review of Experiences within Ice and Iceberg Management. *The Journal of Navigation*, 61(4):557–572.

Eik, K. J. (2010). *Ice Management in Arctic Offshore Operations and Field Developments*. PhD thesis, Norwegian University of Science and Technology.

Farid, F., Lubbad, R., and Eik, K. (2014). A Hybrid Bayesian Belief Network Model for Risk Modeling of Arctic Marine Operations. In *International Conference on Ocean, Offshore and Arctic Engineering*, volume 10.

Fu, S., Zhang, D., Montewka, J., Yan, X., and Zio, E. (2016). Towards a probabilistic model for predicting ship besetting in ice in Arctic waters. *Reliability Engineering and System Safety*, 155:124–136.

Gautier, D. L. et al. (2009). Assessment of Undiscovered Oil and Gas in the Arctic. *Science*, 324:1175 – 1179.

Goerlandt, F., Montewka, J., Zhang, W., and Kujala, P. (2017). An analysis of ship escort and convoy operations in ice conditions. *Safety Science*, 95:198–209.

Gordon-Foundation (2015). RETHINKING THE TOP OF THE WORLD: ARCTIC PUBLIC OPINION SURVEY, VOL.2. http://gordonfoundation.ca/.

Gürtner, A., Baardson, B., Kaasa, G., and Lundin, E. (2012). Aspects of Importance Related to Arctic DP Operations. In *ASME. International Conference on Offshore Mechanics and Arctic Engineering*, volume 6: Materials Technology; Polar and Arctic Sciences and Technology; Petroleum Technology Symposium, pages 617–623.

Hamilton, J., Holub, C., Blunt, J., Mitchell, D., and Kokkinis, T. (2011). Ice Management for Support of Arctic Floating Operations. In *Offshore Technology Conference*.

Hamilton, J. M. (2011). The Challenges of Deep Water Arctic Development. In *Proceedings of the Twenty-first International Offshore and Polar Engineering Conference*.

Haugen, J., Imsland, L., Løset, S., and Skjetne, R. (2011). Ice Observer System for Ice Management Operations. In *Proceedings of the International Offshore and Polar Engineering Conference*.

Ishimatsu, T., Leveson, N. G., Thomas, J., Katahira, M., Miyamoto, Y., and Nakao, H. (2010). Modeling and Hazard Analysis Using Stpa. In *the 4th IAASS Conference, Making Safety Matter*.

Khan, B., Khan, F., Veitch, B., and Yang, M. (2018). An operational risk analysis tool to analyze marine transportation in Arctic waters. *Reliability Engineering and System Safety*, 169:485–502.

Kjerstad, Ø., Lu, W., Skjetne, R., and Løset, S. (2018). A method for real-time estimation of full-scale global ice loads on floating structures. *Cold Regions Science and Technology*, 156:44–60.

Kum, S. and Sahin, B. (2015). A root cause analysis for Arctic Marine accidents from 1993 to 2011. *Safety Science*, 74:206–220.

Leveson, N. G. (2004). A new accident model for engineering safer systems. *Safety Science*, 42(4):237–270.

Leveson, N. G. (2012). *Engineering a Safer World: Systems Thinking Applied to Safety*. The MIT Press, Cambridge, MA.

Leveson, N. G. and Thomas, J. P. (2018). *STPA Handbook*.

Lindsay, R. and Schweiger, A. (2015). Arctic sea ice thickness loss determined using subsurface, aircraft, and satellite observations. *The Cryosphere*, 9:269–283.

Lindstad, H., Bright, R. M., and Strømman, A. H. (2016). Economic savings linked to future Arctic shipping trade are at odds with climate change mitigation. *Transport Policy*, 45:24–30.

Metrikin, I. (2014). A Software Framework for Simulating Stationkeeping of a Vessel in Discontinuous Ice. *MIC*, 35(4):211–248.

Metrikin, I., Gürtner, A., Bonnemaire, B., Tan, X., Fredriksen, A., and Sapelnikov, D. (2015). SIBIS: A Numerical Environment for Simulating Offshore Operations in Discontinuous Ice. In *Proceedings of the International Conference on Port and Ocean Engineering Under Arctic Conditions*.

Milakovića, A.-S., Gunnarsson, B., Balmasov, S., Hong, S., Kitae, K., Schütz, P., and Ehlers, S. (2018a). Current status and future operational models for transit shipping along the Northern Sea Route. *Marine Policy*, 94:53–60.

Milakovića, A.-S., Schütz, P., Piehl, H., and Ehlers, S. (2018b). A method for estimation of equivalent-volume ice thickness based on WMO egg code in absence of ridging parameters. *Cold Regions Science and Technology*, 155:381–395.

Moran, K., Backman, J., and Farrel, J. W. (2006). Deepwater drilling in the Arctic Ocean's permanent sea ice. In *Integrated Ocean Drilling Program*, volume 302.

Nesse, C. V. (2019). Systems Theoretic Process Analysis (STPA) and Ice Management of Marine Operations in Harsh Arctic Environments. Project Thesis NTNU.

Neville, M. A., Scibilia, F., and Martin, E. H. (2016). Physical Ice Management Operations - Field Trials and Numerical Modeling. In *Offshore Technology Conference*.

NSIDC (2018). Map of the Arctic Ocean. http://nsidc.org/arcticseaicenews/map-of-the-arctic-ocean/.

Qureshi, Z. (2007). A review of accident modelling approaches for complex socio-technical systems. *DSTO*, 86.

Rasmussen, J. (1997). Risk Management in a Dynamic Society: a Modelling Problem. *Safety Science*, 27(2/3):183–213.

Rausand, M. (2011). *Risk Assessment.* Wiley, Hoboken, NJ.

Rausand, M. (2014). *Reliability of Safety-Critical Systems: Theory and Applications.* Wiley, Hoboken, NJ.

Rausand, M. and Høyland, A. (2004). *System Reliability Theory: Models, Statistical Methods, and Applications.* Wiley, Hoboken, NJ, 2nd edition.

Seligmann, B. J., Németh, E., Hangos, K. M., and Cameron, I. T. (2012). A blended hazard identification methodology to support process diagnosis. *Loss Prevention in the Process Industries*, 25(4):746–759.

Sigurdsson, J. H., Walls, L. A., and Quigley, J. L. (2001). Bayesian belief nets for managing expert judgement and modelling reliability. *Quality and Reliability Enginerring Journal*, 17:1.

SIMA (2017). Snow & Ice Management Standard Glossary of Terms.

Skjetne, R., Imsland, L., and Løset, S. (2014). The Arctic DP Research Project: Effective Stationkeeping in Ice. *MIC*, 35(4):191–210.

Sulaman, S. M., Beer, A., Felderer, M., and Höst, M. (2017). Comparison of the FMEA and STPA safety analysis methods-a case study. *Software Quality Journal*, pages 1–39.

Teikari, O. (2014). Hazard analysis methods of digital I&C systems. *Research Report by VTT Technical Research Centre of Finland (VTT).*

Zhang, M., Zhang, D., Fu, S., Yan, X., and Goncharov, V. (2017). Safety distance modeling for ship escort operations in Arctic ice-covered waters. *Ocean Engineering*, 146:202–216.

Zhang, Q. and Skjetne, R. (2014). Image Techniques for Identifying Sea-Ice Parameters. *MIC*, 35(4):293–301.