CHALMERS
UNIVERSITY OF TECHNOLOGY

Hazards, risks and accidents at sea

A System Safety analysis of the Sea Traffic Management concept

Master's thesis in the International Master´s Programme Maritime Management

MARKUS PAMP

Department of Shipping and Marine Technology
CHALMERS UNIVERSITY OF TECHNOLOGY
Gothenburg, Sweden 2016

MASTER'S THESIS IN THE INTERNATIONAL MASTER'S PROGRAMME IN MARITIME MANAGEMENT

Hazards, risks and accidents at sea

A System Safety analysis of the Sea Traffic Management concept

MARKUS PAMP

Department of Shipping and Marine Technology

CHALMERS UNIVERSITY OF TECHNOLOGY

Göteborg, Sweden 2016

Hazards, risks and accidents at sea, a system safety analysis of the Sea traffic management concept.
MARKUS PAMP

Master's Thesis 2016:16/359
Department of Shipping and Marine Technology

Chalmers University of Technology
SE-412 96 Göteborg
Sweden
Telephone: + 46 (0)31-772 1000

Department of Shipping and Marine Technology
Göteborg, Sweden 2016

Hazards, risks and accidents at sea, a system safety analysis of the Sea traffic management concept.
Master's Thesis in the International Master's Programme in Maritime Management
MARKUS PAMP
Department of Shipping and Marine Technology
Chalmers University of Technology

ABSTRACT

Sea Traffic Management, STM, is a newly developed concept that will be validated and implemented in the near future. The concept aims to enhance safety at sea, improve the efficiency and reduce the environmental impact of the transportation of goods in the maritime industry. This is to be accomplished by an increase of the information exchange between all the actors involved in the concept. In order to investigate how the implementation of the concept will affect the safety at sea for marine traffic a System safety analysis is conducted. The analysis has identified hazards, risks and measures to mitigate accidents that might occur in the concept. System safety is a process commonly used to enhance safety in hazardous operations such as nuclear, chemistry process industry and in developing equipment used in a military context. The system safety process used in this thesis is mainly derived from the processes to enhance safety in the development of military systems and equipment. The results indicate that a number of areas in STM are subject to improvement regarding safety issues, such as ensuring robust routines to avoid over reliance in the system, dealing with actors not compliant to the system and ensuring that the use of the system does not lead to close quarter situations or exchange of incorrect data. The system safety process is regarded suitable in analysing complex systems like STM and a more thorough analysis using more resources may be beneficial in finding further areas to improve regarding safety in the concept

Key words: Accidents, Hazard, Risk, Safety, Sea Traffic Management, System safety

Contents

Preface

This thesis is a part of the requirements for the master's degree in Maritime management at Chalmers University of Technology, Göteborg, and has been carried out at the Department of Shipping and Marine Technology during the spring of 2016.

I would like to thank my family for a great deal of patience and the personnel at ÅF Technology AB, Systems Management in Göteborg,

Höviksnäs, May 2016

Markus Pamp

List of tables

List of figures

List of abbreviations

AIS	Automatic Identification System
ARPA	Automatic Radar Plotting Aid
COLREG	International Regulations for Preventing Collisions at Sea
DVM	Dynamic Voyage Management
ETA	Estimated Time of Arrival
FM	Flow Management
FTA	Fault Tree Analysis
GPS	Global Positioning System
HRO	High reliability Organizations
NAT	Normal accident theory
OOW	Officer of the watch
PHA	Preliminary Hazard Analysis
PHL	Preliminary Hazard List
Port CDM	Port Collaborative Decision Making
SCF	Safety Critical Function
SeaSWIM	Sea System Wide Information Management
SMA	Swedish Maritime Administration
SSP	System safety program
SSPP	System Safety Program Plan
STCC	Sea Traffic Control Centre
STM	Sea Traffic Management
SVM	Strategic Voyage Management
TLA	Top level accident
WP	Way point

1 Introduction

The maritime industry strives, like all other industries; to increase the efficiency, make it safer and more sustainable to the environment (STM Masterplan 2015). In order to fulfil this vision in the maritime sector the concept of Sea Traffic Management, STM, has been introduced. The foundation of the STM concept is sharing of information between all the actors in the maritime transport chain (Siwe et al. 2015). This will hopefully enable services and functions with the potential of making the berth-to berth ship voyage efficient, safe and environmentally sustainable (Hägg & Lind 2015). A number of challenges certainly lie ahead of fulfilling the objective of Sea Traffic management. This thesis will attend to the implementation of the STM concept and focus on issues of safety at sea applying the process of System safety.

The introduction chapter contains a brief background, with a description of the subject, and relation to earlier research in the field. Further the chapter contains the objectives, research questions, scope and delimitations of the thesis and also a guide to how the thesis is structured.

1.1 Background

The STM concept started as the *Mona Lisa project* initiated among others by the *Swedish Maritime Administration, SMA* in 2010 and then developed into the Mona Lisa 2.0 project. The project is driven as a cooperation between the industry, authorities and the academia (Mona Lisa 2.0 2015). Based on enhanced and transparent information sharing a number of functions and services will be available for the actors in the maritime sectors. STM is based on a number of sub-concepts that will provide the actors in the system with services to fulfil the purpose of the system. The sub-concepts are supported and made available through a fifth concept Sea System Wide Information Management, SeaSWIM, that enables sharing of data in a common information framework (Lind et al. 2014).

Enhanced safety is one of the top objectives of the STM concept and will be implemented by services like route exchange between ships, enhanced monitoring of routes and traffic management. Development of enhanced safety in the concept has been made e.g. with a Formal Safety Assessment, FSA, based on input from the *European Maritime Simulation Network*, *EMSN*, simulations made in the *Mona Lisa 2* project. The safety work is still under development and it is assumed that further safety work will be beneficial for the STM concept. This thesis will use methodology based on the System Safety process in order to identify measures that might contribute to enhance safety in the STM concept. System Safety work is a field that has undergone extensive research and been applied in many fields ranging from nuclear to medical safety. It is also the method used by the Swedish Armed forces and many other military services and actors working with defence material to ensure that systems and equipment are designed, developed, used and disposed of with the highest available level of safety (Swedish Armed Forces 2011a). The system safety concept analyses a systems whole life cycle and all parts of it. The thesis uses as System safety approach to try to identify issues and measures to enhance safety as well as determine if System safety is proper analyse method for a concept like STM.

1.2 Objective and purpose

The objective is to identify safety issues that have not been addressed or needs a more thoroughly investigation in the concept of Sea Traffic management. The purpose is then an attempt to enhance the safety in forthcoming concepts and systems like STM.
In order to reach the objective the thesis will strive to answer predefined research questions and identifying the safety issues using a Systems safety methodology.
The purpose for the writer is also to improve the ability of how to use system safety methodology and increase the knowledge of the Sea Traffic Management concept.

1.3 Research questions

- What are the major safety issues in the STM concept and what are suitable measures to mitigate risks and thereby enhance safety?
- Is system safety a suitable methodology to identify safety issues in STM or similar concepts?

1.4 Scope and delimitations

The focus of the report and the system safety work conducted is the STM aim of enhanced safety at sea. All functions available in the STM concept will be presented, but the system safety analysis only process those aspects considered to be of concern for the safety at sea. Not all parts of the system safety process are used in the analysis; only parts relevant to fulfil the objectives of the thesis and keeping it at reasonable level.

1.5 Thesis structure

The thesis is essentially divided into three main parts excluded the introduction.
In the first part the theoretical background is presented with the description of STM and System safety as well as the underlying theories of safety, systems theory and the definition of the STM concept as a system.
The empirical work conducted in the thesis is described in the second part. It contains the presentation of how the system safety process is conducted and what is included.
Results, discussion of both results and methods and conclusion will be found in the last and third part of the thesis.

2 Background and theory

This chapter contains a more extensive background of the subject than in the introduction. The purpose of the chapter is to provide the reader with enough knowledge of the subject in order to interpret, understand and reflect over the results presented in this thesis.

2.1 Sea Traffic Management

This section aims to provide the reader with sufficient knowledge about the Sea Traffic Management concept, STM. In order to follow, understand and put the System Safety analysis into context.

2.1.1 Background

The Sea Traffic Management concept was initially launched in year 2010 as the *MONA LISA* project as an initiative of the Swedish Maritime Administration, SMA.
The concept has then developed into the *MONA LISA 2.0* project presented in 2013 where the experience from the first project where proceeded (Velásquez Correa et al., 2015). *MONA LISA 2.0* is an European project with more than 50 partners from 13 different countries partly financed by the European union (STM Validation Project, 2016). The project will further develop into the *STM validation* project that started 2015 and will be conducted during 2017 and 2018 involving over 300 vessels, ten ports and three shore based centres in order to evaluate the STM concept (STM Validation Project 2015). The STM concepts involve all actors in the maritime transport chain and the concept takes a holistic approach to integrate all the maritime actors by an increased and transparent flow of information. This is a development from point to point information exchange to cloud based services (Siwe et al., 2015).

2.1.2 Purpose, objective and benefits

The main objectives of the Sea Traffic Management concept are improved safety at sea, a more efficient maritime logistical chain and a decrease of the environmental foot print made by the maritime sector (Siwe et al. 2015). Enhanced safety is to be reached by increased exchange of information at sea: ship-to-ship, shore-to-ship and ship-to- shore. The desired effect is an improved situational awareness for all actors that will e.g. decrease the risk of collision and grounding or sailing into navigational hazards (Hägg & Lind 2015). The increased information exchange will allow all actors in the system to take part of intentions, plans and statuses of each other with the intention of improved efficiency. The sea traffic will also have the ability to flow more effectively when ships at sea can use all the resources of actors a shore (Sjöfartsverket, 2016). Further will the increased exchange of information enable effective traffic management and flow of the sea traffic, ships will use less energy for the sea voyage, port calls will be synchronized with minimal waiting time and effective use of resources and estimated time of arrivals will be adjusted to optimise green steaming (Hägg & Lind 2015).
The desired benefits and improvements in the shipping industry of implementing the system are summarized as followed:

- **Situational awareness** is enhanced by better awareness of others intentions and routes.
- **Predictability** enable**s** more accurate arrival and departure times.

- **Just-in time operations** all involved actors have access to relevant information and can optimize their resources.
- **The innovation capability** might rise and create now unforeseen services and functions.

The concept includes as all actors both at sea and ashore, involved in the maritime chain of transporting goods from one port to another. And the key concept might be expressed with "… *all parties know exactly when they are expected to take action, and what they are expected to achieve* "(Heurlin 2015 p .1).

2.1.3 Structure and characteristics

The logical construction of the STM concept is based on a number of principles as described by Siwe et al, 2015 and Hägg & Lind 2015. Every voyage with its characteristic is given a unique identification, the operative intentions of the actors involved in a specific voyage are presented and available for all providing actors. The situational awareness is gained with data from a vast amount of sources, optimising of routes is available by service providers and finally services and information is exchanged in a secure and federation governed infrastructure. One single point of reporting is used instead of reporting to a variety of actors. To realize these core principles the concept is dived into five sub- concepts. Four concepts that enable distribution of required services and one sub-concept that ensure that necessary information can be distributed to all requiring actors. Every sub-concept contains a number of enablers that support the sub-concept of reaching the main objective of a safer, effective and sustainable maritime sector. That is every sub-concept supports different parts of the voyage by providing services involved in the different parts (Siwe et al. 2015).

2.1.4 Sub-concepts

Here follows a brief description of each the sub-concepts in STM. The system safety analysis of STM that is presented later in the thesis does not involve all of the sub-concepts. The analysis focus on the sub-concepts that are directly affecting the ships performance at sea i.e. Flow Management, Dynamic Voyage Management and to some extent SeaSWIM.

Strategic Voyage Management, SVM*(Falnes 2015), (STM Validation Project 2015)*
The intention of Strategic Voyage Management is to optimize the planning of sea voyages before the voyage starts. Optimized planning will increase the operationally efficiency of voyages and making it safer, environmentally sound and cost effective.
SVM enables all actors to conduct planning and coordination in an early phase of the voyage. All actors exchange the required information to optimize the voyage and create a common situational picture. Delays, change of berths and other matters will be dealt with in an effective manner since all actors are linked and share up to date information i.e. improved co-ordination between all actors. The strategic planning involves long term planning involving actors such as traders, ship owners, charterers with a time span of years, weeks or days. Then follows the dynamic operation that is the making of the nautical plan i.e. how the actual navigation of the ship will be conducted. The concept is realized through a number of services exchanged among the involved actors. The services are e.g. nominating which actors that provide which services and functions, voyage analysis to improve coming voyages and updated information about legal and environmental restrictions.

Dynamic Voyage Management, DVM *(Svedberg & Andreasson 2015), (Hägg 2015)*
DVM will continuously adjust the voyage plan in order to sail in the most safe and efficient way. This by modernizing and improving route planning and voyage execution by providing services with new technology and real time access to relevant information during the sea voyage. During the sea voyage conditions are ever changing and all factors cannot be foreseen. With the ability to continuously receive information about other ships intentions and as well integrated in navigational systems the voyage plan can in an effective manner be adjusted during the voyage. Implementation will lead to improved situational awareness, safer and more efficient routes, smoother and easier reporting and access to updates.
The concept is realized through following provided services.

- **Route Exchange:** Enables ships within AIS range to send and receive each other's route directly on ECDIS display.
- **Route Crosscheck:** A shore to ship service that cheeks that the planned and on going route is accurate and safe for the prevailing conditions.
- **Route Optimization:** Optimizing the route berth to berth e.g. to enable synchronized ETAs and fuel-efficient steaming.
- **Shore based Navigational Assistance Services:** Shore to ship service sending e.g. information about confined areas and dense traffic.
- **Single Reporting**: The need to send several different reports to different stakeholder will with this service vanish. In long term all reporting will be automated.

Flow Management, FM *(Hägg & Ferrús Clari 2015) (Hägg 2015)*
The Flow management sub- concept will enhance the coordination of ship routes by sharing the routes ship-to-ship and ship-to-shore creating a possibility to synchronize and monitoring the traffic. By monitoring and creating a clear situational awareness of the traffic and also knowing the ships intentions concerning ETAs at specific harbours the traffic can be directed to flow better. This will enhance safety by raising the awareness of the actor's intentions as well environment e.g. by increasing the possibility to adept routes for slow steaming.
The concept is realized by the following services:

- **Enhanced Shore-based Monitoring:** Ships routes are monitored from shore based centres. This enhances the control of the ships and will enhance safety when all ships routes are presented in a common display.
- **Flow Optimization:** When ships route presented on ships and at shore centres, the possibility to enhance the navigational efficacy rises by the ability to synchronize routes. Shore centres e.g. can advice and direct traffic based on traffic situation and ships planned ETA to certain waypoints.
- **Area Management**: Updated information in specific area transmitted to ships e.g. to avoid certain areas due to accident, environmental concerns etc.
- **Maritime Traffic Pattern Analysis**: Service and availability to analyse sea traffic by collecting all available data such as routes and safety warnings.

Port Collaboration Decision Making, Port CDM *(Lind & Haraldsson 2015)*
The intention of Port CDM is to facilitate and improve the processes made in the part of the sea voyage that is taken place in and at the vicinity of the port. The objective is reached by extensive information sharing and common situational awareness of all involved actors. Major outcomes of this are increased interaction and predictability that enables just-in-time operations, minimal waiting time and effective use of resources. Port CDM clearly supports the main objective of higher efficiency and sustainability in STM. The services provided in this sub-concept optimize the port calls making them highly synchronized with fast turn a rounds and all actors performing their services in a just-in-time manner.

Sea System Wide Information Management, Sea SWIM *(Lind et al. 2015) (Heurlin 2015)*
SeaSWIM is the function that all information flows through or the service that enables that all the actors in the system can exchange required information both by sending and receiving. All actors in the system collect and request required information such as route segments, loading conditions or intentions. The concept is based on a number of assumptions that must be realised to make it work. A common standard is essential both regarding hardware and procedures. The information is governed by the owner i.e. the information owner decide upon who has access to the information. Meaning that data must be able to be protected and not shared between all for competitive reasons. Relevant information for a certain actor must be discoverable and not suppressed by other irrelevant information.

2.2 System and safety theory

This section describes definitions and terms used in system safety and to provide the reader with a theoretical background of systems and safety theory.

2.2.1 Terms and definitions

The terms and definition of *safety, hazard, risk* and *accident* are presented and explained due they are key definitions in the System safety process. Also the definitions of *Top-level-accident, TLA* and *Safety Critical Function, SCF* are explained.

Safety has many definitions, they may vary a bit but the meaning is basically the same, that safety is the situation when risks of accidents are at tolerable level, as quoted *"A situation without intolerable risks"* (Shahriari 2013). The definition used in military publications such *MIL-STD 882* and *Armed Forces' Handbook on System Safety 2011 Part 1 – Common* defines safety likewise, as the situation where there are no conditions that can cause unacceptable damages, injures or other risks and absences of accidents. This definition is also used by Leveson (Leveson 2011).
Hazard according to (Shahriari 2013) is a condition with the potential of resulting in an event resulting in death, injury or other damages. Hazard is also defined as a condition that can cause an accident (Ericson 2011) or a prerequisite to an accident (DoD 1993). The expression **Hazardous event** is used in some occasions and has a similar meaning as hazard *"An event that occurred by misadventure, that is, without intention, unplanned, and which may result in an accident or incident if someone or something is exposed."* (Swedish Armed Forces 2011a).

Accidents are considered to be unplanned event/s with a result that not is accepted, e.g. injury to personnel, damages to materiel equipment and property or causing harm to the environment (Ericson 2011), (Swedish Armed Forces 2011a) and (Leveson et al. 2009).
The definition of **Risk** varies but the basic meaning of the definition, as to be understood in this thesis, states that risk is the combination of probability of an event to occur and the consequences of that event (Leveson et al. 2009) and (Swedish Armed Forces 2011a).
The term mishap is mainly used in US and is here replaced by the term accident which has the same meaning (Swedish Armed Forces 2011a). Therefor Top-level-mishap is replaced with Top-level-accident in order of minimising the number of terms and definitions. The process can end up in a vast number of hazards identified and in order to handle the hazards effectively in the system safety process, therefore hazards with the same potential accident are grouped together in Top-level-accidents, TLAs (Ericson 2011).
Safety critical function, SCF, is connected to TLA in the way that failure of a Safety Critical function will lead to severe impact such as loss of the system, death or heavily affecting the environment (Ericson 2011). The meaning of designating functions, as SCF in the process is to clarify that the failure is severe to the system. SCFs have been derived from the top-level-accidents to indicate the most severe accidents.

2.2.2 What is a system?

Vital to the understanding system safety is an apprehension of what a system is. The term **System** may have many various definitions, also depending of what kind of system that is intended. Everybody basically know what a system is and that there are several kinds of systems e.g. the financial system, eco – system, solar system etc. Some systems are natural like the eco-system and others are manmade like technical systems "*Man made systems are made for purposes that are achieved with the output from the system"* (Ericson 2011). The socio-technical system discussed by Rasmussen (Rasmussen 1997) and Leveson in (Leveson et al. 2009) are systems that involves several levels from legislators, managers to system operators (Rasmussen 1997). The discussion includes how to increase safety in systems and that that should be done with cross-disciplinary studies with a system oriented approach. The system model cannot be built from a bottom down view; a system-oriented approach requires a top down perspective. A collection of parts and components is not a system if not he parts and components are interrelated and interdependent of each other. It can be composed of various kinds of components like operators, equipment and procedures (Ericson 2011). The key understanding is also that the performance of the system is greater than if the components operate independently, like stated by Rasmussen *"A system is more than the sum of its elements"* (Rasmussen 1997). The definition of system found in MIL-882C supports this view of what a system is and explains that a system can have many levels of complexity, consist of different kinds of parts and is used to accomplish a specific task or objective (DoD 1993).

2.2.3 Safety in systems

A general explanation of why safety work is needed is found in *Armed Forces´Handbook on System Safety 2011 Part 1 – Common.* It states that many systems today are very complex and it is difficult to foresee all accidents that might happen. And that the development of new systems and technology might lead to new hazards and risks not foreseen before. There are many different approaches and

theories on how to deal with safety. All of them cannot be presented in the thesis but some approaches closely linked on how to regard safety in systems are presented.
Interesting theories identified in the literature review that discusses how to approach safety in systems are Normal accident theory, NAT, presented by Charles Perrow after the nuclear power plant accident at Three Mile Island and High Reliability Organizations theory, HRO. The Normal accident theory suggests that accidents are such events that normally happen and are inevitable (Leveson et al. 2009). Some systems are so complex and the systems components interact and are so tightly connected in such a way that is impossible to foresee and prevent accidents. Unforeseen actions or small incidents spread in the system in such a fast pace that cannot be stopped or understood. Leading to that the whole system is affected and/or damaged. The thought of that accidents can be prevented by effective management and design is not reliable, accidents will happen anyway (Sagan 1993). The NAT theory also emphasis that efforts to enhance the safety makes the system more complex and even more difficult to survey and control. Adding safety measures will make mistakes harder to detect and personnel operating the system tends to take more risks (Sagan 1993).

High Reliability Organizations are systems with operations that are considered to be hazardous with extensive consequences if something goes wrong e.g. nuclear power plants or air traffic control systems. The organizations obtains a high level of safety with few or none accidents for long time periods (LaPorte & Consolini 1991). They manage complicated tasks during high time pressure often under a concentrated period of time (Reason 2000). The organisations constantly strive to improve safety, the organisation excepts accidents and train to avoid and handle accidents if they occur (Reason 2000). The operating objectives are often challenging and requires an effective system to effectively produce the demanded outcomes at the same time handling safety issues with potential of causing severe damages and consequences (LaPorte & Consolini 1991). Either NAT or HRO theory addresses the real issues of safety in systems according to (Leveson et al. 2009), the theories simplify the causes of accidents and do not distinguishing between safety and reliability.
A system can be reliable but unsafe, since accidents are frequently the outcome of components working perfect but the interaction causes the accident. To ensure safety in a system components cannot be assessed one by one, the interaction and the whole system must be analysed. As also emphasized by (Ericson 2011) that a system should be considered by looking at how the different parts interact with each other. The alternative theory suggested, is a systems approach to technical and organizational safety and is suggested by e.g. (Leveson 2004) and (Rasmussen 1997). The system approach is characterised by a top down system thinking, seeing safety issues as a whole and not a bottom up perspective, not seeing the interaction between all parts. (Leveson et al. 2009).
Other interesting theory of safety in systems is James Reason human error approach (Reason 1990) where the source of error is discussed by comparing a system or person approach to safety. Reason also argue that a system approach is the best way of handling hazards in an organization, even though HRO is categorized as a system approach and Leveson (Leveson et al. 2009) argues that it is not. Reason discusses two different approaches of how errors can be handled. There is always a risk for accidents, but what causes them, human error or systems fault? The person approach focuses on the errors that humans make and the cure is to change the human and prevent them from making mistakes. The errors become isolated events in the system

without a system context. "*The same set of circumstances can provoke similar errors, regardless of the people involved"* (Reason 2000) The system approach states that errors happens in all organizations, humans cannot be changed but the organization/conditions can be changed and by that the errors can decrease. Building systems that can handle errors and contain the damage. That is taking a comprehensive approach at the personnel, workplace, system as whole etc. making the system as robust as possible. Failures in a system should not be isolated, they should be put into a systems context to be best understood and prevented (Reason 2000).

2.3 System safety

The aim and purpose of systems safety is to identify and deal with hazards in systems through different processes and methods (Leveson 2003), to act proactive and build safety in into the system from the start (Ericson 2011).
The concept of system safety was introduced in the 1940s mainly in the airplane manufacturing industry. The need arise to enhance safety and find the errors before trials to minimize the number of accidents. There was a need to find other safety methods than fly-fix –fly aka safety by accident methods (Ericson 2011).
Systems became more and more complex and a systematically approach that eliminated hazards before trials where required. Meaning basically that the design must be safe and all measures taken to enhance safety instead of testing a design and see what goes wrong (Ericson 2011). When industries developed and more and more hazardous operations where conducted such as those in nuclear power plants and chemical industry a fly-fix-fly approach was not accepted since the consequence of an accident were to be too severe. Another method was required to prevent accidents before they happened (Leveson 2003). The US Air force took in many ways the lead in the development of systems safety and it spread into the other branches of the armed forces. Different standards and manuals where established and the MIL-STD 882 is to now prevailing standard. The standard (Swedish Armed Forces 2011a) and (Swedish Armed Forces 2011b) used by the Swedish Armed forces and Swedish Defence Material Administration, FMV is based on the MIL-STD 882C (DoD 1993) standard developed by US department of defence .

2.3.1 Definition of System Safety

The literature provides various definitions of **System safety**. They could be viewed as different interpretations with basically the same meaning.

MIL-STD 883C
"The application of engineering and management principles, criteria, and techniques to optimize all aspects of safety within the constraints of operational effectiveness, time, and cost throughout all phases of the system life cycle" (DoD 1993).

Armed Forces´Handbook on System Safety 2011 Part 1 – Common
"*System safety is defined as the property of a technical system that does not intentionally cause injury/damage to a person, property or the external environment"*(Swedish Armed Forces 2011a).

White paper on approaches to safety engineering
"The primary concern of system safety is the management of hazards: their identification, evaluation, elimination, and control through analysis, design and management procedures" (Leveson 2003)

Concise Encyclopedia of System Safety
"System safety is the process for eliminating or reducing potential mishaps[1] *through a process of hazard identification, risk assessment, and risk control"* (Ericson 2011)

Moving Beyond Normal Accidents and High Reliability Organizations: A Systems Approach to Safety in Complex Systems
"…managing system safety is a continuous process of trying to determine how much risk exists in particular activities and decisions, how much risk is acceptable, and how to achieve multiple system goals and requirements" (Leveson et al. 2009).

A summary of the definition of System safety indicates that Systems safety is a process used to enhance safety in systems using different processes and techniques, identifying hazards and controlling the amount of risks in a structured process.
It also stated in the literature that System safety is applied on the systems whole life cycle, different techniques are used to identify hazards and risk at the various phases. The defined phases of a system are concept, design, production, operations and disposal (Ericson 2011).

[1] *Mishap* is the US term for accident.

2.3.2 The system safety process

The system safety process consist of a number of phases, each phase with is specific objective and purpose. The process used in *Armed Forces´Handbook on System Safety 2011 Part 2 – Methods* and *MIL-888C* are structured according to those phases. The phases are established and commonly accepted to be the System safety process as presented below (Ericson 2011).

1. Planning: Meaning that the system safety work should be planned and how the system safety process will be conducted to suit the specific demands of the system being analysed. The planning of the process is initially applied by establishing a *System Safety Program, SSP* by the orderer of the system/product. The SSPs holds the requirements for the system. The SSP is then revised and a System Safety Program Plan, SSPP is established which is a plan that describes what system safety activities and methods that should be applied on the system (Swedish Armed Forces 2011b). The empirical part of the thesis is based on a SSPP issued by Swedish Defence Material Administration, FMV. "Activities" are the predefined analysis steps following the methods presented by (Swedish Armed Forces 2011b) and (DoD 1993).
2. Identify hazards: Hazards in the system are identified using Hazard Analysis Techniques such as PHL, PHA and FTA.
3. Risk assessment. Assessing the probability and severity if a hazards leads to an accident. This is vital in order to prioritize the order of which hazards to deal with.
4. Mitigation: Find measures that eliminate the hazards or put the risks into an acceptable level.
5. Verification: The mitigation measures must be verified to ensure that they serve their purpose.
6. Risk acceptance: Evaluate and decide what level of risk in the system is acceptable. Decreasing risk is also a matter of resources and some risks are not effective to countermeasure with all means.

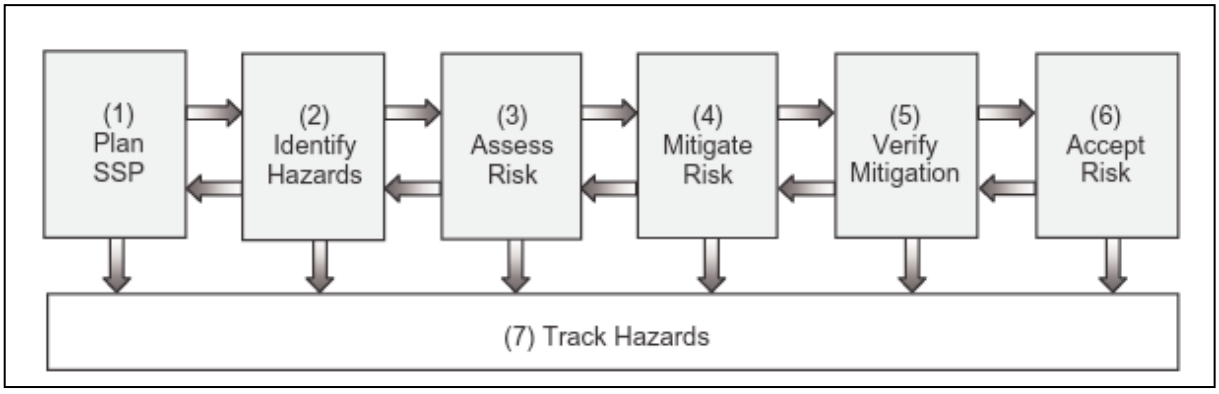


Figure 1, The system safety process (Ericson 2011).

2.4 Sea Traffic Management as a system

To identify, assess and mitigate risks and hazards in the Sea Traffic Management concept with a system safety approach, the concept must be defined and regarded as a system.
In the definition of the system it is clear that a system is a structure of several different kinds of parts and components used to accomplish an intended purpose that will achieve a certain task, objective or mission. (Swedish Armed Forces 2011b), (Ericson 2011), (DoD 1993). A system can be constructed of several sub-systems. A sub-system could include equipment, components, personnel, facilities, processes, documentation, procedures, software etc. connected into the system to accomplish the overall system objective (Ericson 2011). And that the system is a unit consisting of elements that is greater than if the elements would be working one by one (Ericson 2011). STM is based on sub- concepts, which in turn are based on different enablers also mentioned as services that will perform specific functions that contribute to fulfil the purpose and objective of the system. All actions in STM are enabled by the interaction of different components such as navigational equipment, operators and procedures. One by one there is no effect but the interaction enables the functions. The sub-concepts fulfil certain tasks e.g. route exchange and directing sea traffic. The tasks performed by the sub-concepts will then support the overall objectives of improved safety, enhanced operational efficiency and environmental sustainability

2.5 Other safety work concerning STM

Two relevant documents have been studied and used as sources to conduct the empirical part of the thesis i.e. the system safety analysis. It is the *FSA – Formal Safety Assessment of the STM concept* (Andersson & Forsman 2015).
And *Taktiskt ruttutbyte ship-to-ship och dess relation till COLREG* (Gustafsson & Åding 2014) a thesis conducted in 2014 at the master mariner programme at Chalmers university of technology.

Formal Safety Assessment, FSA
The conducted FSA as described in (Andersson & Forsman 2015) is a safety assessment of the STM concept. The input data in the assessment are simulations made in the *European Maritime Simulation Network, EMSN* and from theoretical calculations and accident statistics (Andersson & Forsman 2015). The risk control measures primarily aiming at prevention of human factors related navigational accidents. The FSA conducted in the framework for STM presented a number of hazards that where identified. Some of these hazards were used as input to the system safety analysis of STM. The hazards used are: Information overload, Cultural hierarchic traditions, over – reliance, information overload and preferred ship speed.

Taktiskt ruttutbyte ship-to-ship och dess relation till COLREG
The empirical work in the study was a series of interviews of experts in the field of COLREG, route exchange and seamanship (Gustafsson & Åding 2014). The experts have elaborated their views of certain complicated traffic situations and the positive and negative effects of using route exchange in such situations.
The results presented in the thesis indicate that over reliance in the route exchange function, cultural hierarchy, and workload are factors that must be considered in the development of the STM concept. And that route negotiating ship to ship in close

ranges is a hazardous condition. It also presents that the route exchange function would result in a higher situational awareness concerning sea traffic and simply VHF communication to solve traffic situations.

3 Research methodology

3.1 Research design

The intention has been to develop a research design that will strive to answer the research questions. Various methods have been used to collect the data used in the thesis. A literature review was initially done to gain understanding of the theoretical background and deepen the knowledge of the subject. Interviews were made to complement the literature review. The collected data was then compiled and used as input to accomplish the system safety analysis.

The work conducted may both be categorized as descriptive and explanatory. Descriptive research answer the question of *"What is going on"* and the explanatory research *"Why is it going on"* (Vaus & Vaus 2001). It is descriptive in the manner of explaining the STM concept and System safety process, providing knowledge that will be used for the explanatory part of the study. The explanatory part is the system safety analysis that aims of identifying hazards, risks and measures to reduce these.
The study should in its whole be considered to have a deductive approach to the research questions since the RQs primarily are answered by the results of the system safety analysis. System safety is considered to be a theory of how to enhance safety in systems and STM is then tested in this theory to answer the RQs. Deductive approach is to test a theory with observations (Vaus & Vaus 2001). STM has been observed as a system and tested with the system safety methodology to find answers and assess the suitability of using system safety methodology on a concept like STM. Though considering STM as a system might be classified as an inductive approach, since inductive research is "theory building" (Vaus & Vaus 2001) and there is a reasoning about identifying STM as a system in order to be able to do a system safety analysis of the concept.
In the meaning if the study is done in a qualitative or quantitative manner i.e. how the data collection has been done. As stated in the reference literature typically quantitative data can be counted and classified (Höst et al. 2006) examples to collect data is surveys and experiments (Vaus & Vaus 2001). Qualitative data are typically interviews and observations (Raviola 2014), (Vaus & Vaus 2001). Data is also categorized as primary or secondary data. Secondary data have been collected primarily with the literature review and is considered to be a quantitative method for data collection. The purpose of collection of secondary data is to prepare for primary data collection, achieve a deepen understanding of the subject in order to have a base where the research question can be approached from. Primary data is collected by the researcher to answer/address the specific research objective (Raviola 2014). In this thesis the primary data collection is the system safety analysis and input from interviews.

3.2 Literature review

The purpose of a literature survey is to collect data, in this case secondary data to build a theoretical framework and background of the subject to be study. Most research starts with a literature review and is an important part of the research (Kitchenham 2004). Literature review supports the objective of building the report/thesis on existing knowledge about the subject. It is also important to present the sources of data and how the data was extracted (Höst et al. 2006) The review

usually according to (Kitchenham 2004) consist of three phases: planning, conducting and reporting the review. The literature review in this report followed those phases The phases and the conduct was also done with guidelines from (Kitchenham 2004). Even if the next phase starts when the one before is done the literature review is an iterative process (Höst et al. 2006). Meaning that during the research when the knowledge in the topic deepens the literature review will run along the whole study conducted in the thesis. Concerning also that the primary data collection might give guidance to relevant literature that might require to be studied.

During the **planning** phase some of the concerns regarded were if there are any existing literature reviews in the field already and were there any suitable primary sources to extract data from? To ensure that the review would be done with a clear strategy and in a structured manner a search protocol was established. The **conduct** of the literature review followed a predetermined plan in order to fill in the search protocol and secure a documentation of how the search proceeded.
As earlier mentioned a literature review is an iterative process where the researcher often repeats and goes back and forth of the different phases. The literature review was conducted in the following manner which is a typically approach according to (Höst et al. 2006). Even if all subjects not where reviewed in exactly the same way the overall approach was like the following description.
First a **broad literature** survey was done which included

- Searching for literature reviews in same or similar subject
- Searching with key words in databases. Mainly using summon by Chalmers library services and Google scholar.
- Advising reference list of literature in the field of the topic
- Studying reference list of other master thesis with similar scopes to get guidance of recognized authorities in the specific topic.
- A structured search of company, institutes and authorities documents and webpages acting in the specific field.
- Asking interviewees of advice for relevant literature.

The results from the broad search was scrutinized and based on the result of the initial broad search a selection of articles, books and other suitable sources were determined to be subject for deeper studies. The selected sources where studied to deepen the understanding of the subject and finding new suitable key words and phrases based on the terminology used in the specific topic/area to a more focused search of literature than the initial broad search/survey.
During a literature review it is important to objectively evaluate the extracted data i.e. the credibility of the surveyed literature must be questioned to ensure that trustworthy data is used in the report (Höst et al. 2006,). The researcher should consider about the sources if they are reviewed and by whom. Is the result and subject relevant to answer the research questions of the thesis? Are the results confirmed and recognized in a trustworthy context (Höst et al. 2006). These issues will also be discussed more thoroughly in the section “Discussion of method” at the final part of the report.
The **reporting** of the literature review is naturally to be represented by the reference list. All the sources where continuously added to the reference list, only sources used as references are listed in the reference list.

3.3 Interviews

Three interviews have been conducted in order to collect primary data to the thesis. First a shorter interview was conducted with a person employed at the consultant firm *ÅF*. Then an interview with a person involved in the MONA LISA 2 project, STM concept, was conducted. Finally the interviewee at ÅF was once again engaged in a longer interview.

The purpose of the interviews was to collect additional primary data to the thesis and gaining expert knowledge in the thesis subjects. From the STM expert confirming facts about the system and identifying hazards was the primary objective of the interview. The employee at ÅF, previous involved in System safety analysis, were asked questions about the system safety process with the objective of identifying how the process could be conducted and how to avoid common pit falls.

The preparation before the interviews included the preparation of a list of questions and topics to be discussed to fulfil the desired objectives. A semi-structured approach was chosen. A semi – structured interview is conducted with a list of prepared questions but the questions may not be asked in a certain order (Höst et al. 2006). The questions are prepared and formulated with the intention of getting the interviewees opinion and knowledge of a certain area (Lantz 2007). Depending on how the interview developed and how the questions were answered the order of the question varied as well as new not prepared questions were asked. The interviews were documented by taking notes; the interviewees preferred that the interviews not were recorded. The results from the interview were used in the thesis in the following manner. From the interview concerning STM it was confirmed that the required knowledge from the literature review was mostly correct and hazards to be used in the system safety process were collected. The interview regarding the system safety process delivered some useful directions of how to the conduct the process and of what parts to be included to fulfil the objectives of the thesis.

3.4 Methods in the system safety process

Here follows description of the Hazard analysis techniques used in the process. The system safety process is presented in chapter 2, section 2.3.2.

3.4.1.1 Preliminary Hazard List

The purpose of conducting the activity Preliminary Hazard List, PHL is to at an early phase of a systems design and concept development identify and list potential hazards and accidents in the system. The general result from the activity is basically a list with all the identified hazards presented.

The methodology is to produce a list of relevant components and functions in the system and comparing these to lists of potential hazards and/or accidents. Components and functions are denominated as *Items* in the analysis. List of hazards where extracted from the *Hazards and hazardous conditions PHL- template* (FMV 2015a). Further hazards where identified from contemplation of the literature used and interviews. From the literature especially the report *FSA – Formal Safety Assessment of the STM concept* (Andersson & Forsman 2015) and the Bachelor thesis *Taktiskt ruttutbyte ship-to-ship och dess relation till COLREG* (Gustafsson & Åding 2014) where valuable sources of finding hazards applicable in the analysis. Hazards where also identified by brainstorming sessions using knowledge of the system and hazards that might occur. The brainstorming method for this activity is generally accepted and used according to (Ericson 2011) and interviewee at ÅF.

Then the effects of each hazard were considered and what accident the release of the hazard could cause. If the hazard condition is released an unplanned event with a negative effect will occur i.e. an accident. The accidents where then compiled into top-level- accidents, TLAs and Safety Critical Functions, SCFs which were to be used in the other activities PHA and FTA. Output data from the activity is list of identified hazards, effect of hazards, accidents, TLAs and SCFs.

3.4.1.2 Preliminary Hazard Analysis

The system safety activity Preliminary Hazard Analysis, PHA, further analyses and compiles the hazards identified in the PHL. The activity aims to identify causes, effects of the hazard as well as suggest actions to mitigate the risks (Ericson 2011). Instead of using all the identified hazards from the PHL the extracted TLAs and SCFs were subject to the analysis. The same *Items* used in the PHL were listed and analysed to the TLAs. This will extract causes, effects and mitigation measures to hamper or eliminate the hazards that might lead to accidents.
Risk assessment of each hazard might be conducted in the PHA, though the risk assessment was given an own section focusing of the consequences of the TLAs. A risk assessment in this activity of all hazards was considered to be too comprehensive and risk evaluation of the TLAs is sufficient of achieving the thesis objectives.
Output from the activity are recommendation of how to mitigate hazards and risks as well as which hazards that should be subject to further analysis.

3.4.1.3 Fault Tree Analysis

FTA is a deductive method used to backtrack accidents to identify the causes of the accident. It can be used both in a quantitative manner of calculating probability of an event to occur or qualitative manner to find causes or combination of causes of the accident (Shahriari 2013) The method in the system safety process is useful by finding root causes of accidents and how to mitigate the potential accidents.
The events are combined using Boolean gates stating OR/AND i.e. an event causes an event on a higher level either with combination with another event – AND. Or if a single event fails it causes the event on the higher level – OR.
The method was applied according to (Shahriari 2013). The top events/accidents were derived from the PHL and PHA. In this case the accidents *Grounding* and *Collision*. Then the Fault tree was developed until the basic causes of the top events were identified. The basic causes were then listed and compiled to find countermeasures to mitigate the hazards and risks of accidents in the system.

3.4.1.4 Risk assessment

Risk evaluation in this analysis is an estimate of what consequence and probability the identified TLAs and SCFs have if they occur. The risk assessment is conducted using the Risk assessment matrix from MIL-882C (DoD 1993).
The classifications of severity of the accidents are obtained from the references (FMV 2015c) and developed to describe the risks in the STM concept.

Personnel
Personnel might get injured if accidents occur. Severity classified I to IV.
I - Death
II – Serious injury requiring hospital care, and full recovery might not be able
III – Less serious injury that requires medical attention and the person will be fully recovered.
IV – The injury is negligible and the person can return to duty after minor medical care.

Ship/system damage
The accidents might cause damages on property such as structural damages
Severity classified I to IV
I – Systems cannot be repaired. Ship sinks or is damaged beyond chance of repair.
II – Ship is affected in such a way that in cannot conduct its tasks in the system.
III – Ship or system is affected but still conducts it tasks in the system.
IV – No restrictions.

Environment
Accidents in the system might have effect on the surrounding environment. Severity classified I to IV
I – Serious effect on the environment that requires considerable efforts to restore. The natural effect to restore is heavily affected.
II – Serious effect. The environment will recover, considerable efforts required to assist the naturel recovery.
III – Less serious effect that requires small efforts to restore, the natural recover will be effective
IV – Small or less serious effect that do not require any recovery measures. The natural recovery is sufficient.

The probability A-E and the severity are the subjective estimate of the writer based on experience and information gained during the work with the thesis.
The risk assessment provides a qualitative measurement of the risk if the accident caused by the hazard would occur. The assessment has been done regarding risk of injury of personnel, damage of system/ship and negative effect on the environment.

Table 1: Risk assessment matrix (Ericson 2005)

Severity	Probability
I. Catastrophic	A. Frequent
II. Critical	B. Probable
III. Marginal	C. Occasional
IV. Negligible	D. Remote
	E. Improbable

The probability of occurrence, based on quantitative statistics, has not been dealt with since the analysis focus on the design and concept phase of the system. Statistics are in some extent available in *FSA – Formal Safety Assessment of the STM concept* report (Andersson & Forsman 2015).

4 System safety analysis

4.1 Introduction

The analysis is based on the instructions provided in *Armed Forces´Handbook on System Safety 2011 Part 2 – Methods* (Swedish Armed Forces 2011b) and documents provided by Swedish Defence Material Administration, FMV. The structure of how the activities are presented is following the guidelines provided in the document *Systemsäkerhetsplan (SSPP) för leveratör* (FMV 2015b).

Different approaches and definitions of system safety are discussed in previous chapters of the report. Even if the academic theory can be said to be a bite fragmented the analysis is assessed to stand firm on the above-mentioned documents as well as support from (Ericson 2011), (Ericson 2005) and (Vincoli 2014). The system safety process is structured according to a System Safety Program Plan, SSPP. The SSPP structures what measures and activities that will be conducted when doing a system safety analysis of a certain system. Here the SSPP is adjusted to conduct relevant activities to fulfil the objectives of the thesis. In order to fulfil the objectives of the thesis the phases of identifying hazards, assessing risk and mitigation of risk are conducted. Verification of mitigations measures and risk acceptance are not processed since not required to fulfil thesis objective and keeping the contents of the analysis at a reasonable level.

4.1.1 Included parts

The thesis focus primarily on safety issues and strives to identify hazards in the STM concept. Sub-concepts of STM that are included in the analysis are Flow management, FM, Dynamic voyage management, DVM and SeaSWIM. FM and DVM are categorized as operational services (Hägg 2015). The definition of sub-concepts and the included services should not be regarded as limitations or restrains in the analysis. The actual functions derived from the sub-concepts that are handled in the analyse techniques are defined and presented.

4.1.2 Excluded parts

The sub-concepts Strategic Voyage Management, SVM and Port Collaboration Decision Making, Port CDM are not considered, even though services and functions of these concepts might be incorporated since some services are similar to the services in the sub-concepts subject to the analysis.

4.2 Objective and Scope

The objective of the system safety work, presented in this analysis, is to identify, analyse and evaluate hazards that might lead to accidents in the Sea Traffic Management concept, STM. The scope of the system safety work conducted is limited to the elements of the system that are determined to cause the most relevant and severe hazards and risks at sea.

4.3 Definition of the system

In order to carry out the system safety work an understanding of the system, the operational environment and the mission of the system are essential.
A definition of the system is made that sets the frames of the system that will be subject to the System safety process. Such a definition should be made before the system safety process starts. The definition used in the following analysis is based on and contents the requirements according to the document *Systemsäkerhetsplan (SSPP) för leveratör* (FMV 2015b). The definition of the system and what parts of it that will be analysed is based on the description of the STM concept retrieved in the literature review. Interviews, (Andersson & Forsman 2015) and (Gustafsson & Åding 2014) have also contributed of what parts to be analysed to strive of fulfilling the thesis objectives and answer the research questions.

4.3.1 Function of the system

The overall function of the system is to contribute to improved safety, environmental sustainability and operational efficiency in shipping. This will be achieved through an increased exchange of information between the actors and standardization of the digitizing of the shipping industry. The system coordinates the efforts of industry, academia and authorities.

4.3.2 System function operational services

The analysis focus on functions identified in the operational services FM and DVM and too extent SeaSWIM. The core function is the flow of information, especially for the analysis the route exchange function ship-to-ship, ship-to-shore and shore-to-ship.

4.3.3 Part of other systems

The system is part of the whole logistical chain ranging from sea, land and air.
It is part of and interacts with all marine activities not included in the system. E.g. other sea traffic including fishing vessels, merchant vessels and pleasure crafts.
All vessels at are subject to COLREG, which also can be considered to be a system that affects STM.

4.3.4 Components and parts

Following components and parts have been identified as relevant components to be analysed.
GPS, AIS, Interconnection i.e. the hard- and software that enables the communication, Navigational equipment, Officer of the Watch, OOW, Route receiving and sending, Ship, STCC and system. These components are categorized as “Items” in the analysis.

4.3.5 Basic Design /System structure

The system is based on four sub-concepts and *SeaSWIM.* The sub-concepts contain a number of enablers mentioned as services. The enablers within the system supports the function and the objective of the system by interaction made possible by data streams that connects all components and parts of the system by transmitting and receiving information.

4.3.6 Operational environment

The system will be operational in all sea areas and in all weather conditions. The functions and services included in the analysis are mainly used in coastal regions, as described in (Hägg & Ferrús Clari 2015) with the characteristic of:

- High traffic density fairways, port entrances and other waterways.
- Environmentally sensitive areas
- Marine infrastructure such as oil, gas, and wind energy installations

Factors such as wind, wave height, current, and conditions due to tide and their effect on the operational conditions are considered in the analysis.

4.3.7 Resistance to external influences

The system is assumed/estimated to be operational under normal conditions. Events with severe disturbance such as natural disasters, terrorist attacks and armed conflicts are not considered in the analysis.

4.3.8 Actors

Actors are functions, items or sub-systems that are operated by an operator that makes decisions that affect what action is executed. Actors to be considered in the analysis are STM compliant ships, None STM compliant ship, shore based operators/STCC.
Training level of operators and ability to perform desired tasks are included in the analysis.

4.3.9 References

General documents
Laws, regulations, standards and applicable instructions. The use of COLREG is accounted for in the analysis.

Methodology
Documents that support the analysis with methodology i.e. how the methods in the analysis are performed. Following documents have been used in the analysis process.

- Armed Forces´Handbook on System Safety 2011 Part 2 - Methods (Swedish Armed Forces 2011b)
- Basic guide to System Safety (Vincoli 2014)
- Checklist of Hazards and hazardous conditions (FMV 2015a)
- Concise Encyclopedia of System Safety (Ericson 2011)
- Hazard analysis techniques for system safety (Ericson 2005)
- Main concepts of risk in engineering (Shahriari 2013)
- MIL-STD-882C (DoD 1993)
- Systemsäkerhetsplan (SSPP) för leverantör (FMV 2015b)

Governing documents
Documents that sets the framework and guidelines of the analysis are:

- Armed Forces´Handbook on System Safety 2011 Part 1 – Common (Swedish Armed Forces 2011a)
- Armed Forces´Handbook on System Safety 2011 Part 2 - Methods (Swedish Armed Forces 2011b)
- MIL-STD-882C (DoD 1993)

System specific documents
Documents that provide the person(s) conducting the analysis with facts about the system. The sources consist of articles, documents downloaded from http://stmvalidation.eu/documents/ and interviews. All documents are included in the reference list chapter 8.

4.4 System safety activities

The actual hazard analysis techniques used in the process are
Preliminary Hazard List, Preliminary Hazard Analysis and Fault Tree analysis and Risk Matrix.

4.5 Reporting and documentation

The reporting and documentation of the result of the system safety process are integrated in the thesis and presented mainly in the result and discussion chapter.

5 Results

This chapter present the results from the System safety analysis. Results considered to be significant are emphasized; details of the analysis are available in chapter 9 as Appendixes 9.1-9.3.

5.1 Results from the system safety analysis

The setup of the analysis was determined in the initially process of identifying the system and its parts, actors etc. and is presented in chapter 4, *System safety analysis*.
The results are presented in the same order as conducted in the analysis i.e. PHL, PHA, FTA, risk assessment and mitigation measures.
In the analysis Preliminary Hazard List, PHL, was used to identify and structure hazards in the system and also to identify accidents that might occur. Preliminary Hazard Analysis, PHA, primary identifies effects and causes of the hazards.
The PHA and PHL resulted in two major accidents, *Collision and Grounding*, that were used as top events in the Fault tree analysis to identify root causes of the accidents. The risks of the accident were assessed and evaluated and finally mitigation measures were identified.

5.1.1 Preliminary Hazard List

A brief explanation of the *Item* is presented above an extract from Appendix 9.1.
The first column indicates the hazard followed by the effect of the hazard and then the potential accident.

AIS
The function of AIS is vital for the system, both by receiving and transmitting ships position, data and relevant segments of the route.
If not functional i.e. not sending correct information or not sending any information at all, affects the function and safety of the system.

Table 2 System Item AIS, PHL

Hazard	Hazard effects	Accident
Inaccurate voyage data - UKC	Navigational danger	Grounding
Inaccurate dynamic data - Rate of turn	Deviation from route	Close - quarters
Inaccurate dynamic data - position	Inaccurate position displayed	Deviation from route
Inaccurate dynamic data - Navigational status	COLREG deviation	Close - quarters
Inaccurate dynamic data - COG, SOG	Traffic perplexity	Close - quarters
Ghost vessels	Traffic perplexity	Navigational danger

GPS

GPS provides AIS and the navigational system with positional data. E.g. the ships speed over ground and course over ground are extracted from that data.
If the ability to provide the system with accurate positional data the route exchange function will be hampered and the ability to use GPS as a mean for navigation will not be possible.

Table 3 System Item GPS, PHL

Hazard	Hazard effects	Accident
Position error GPS	Inaccurate position displayed	Deviation from route
Deviant geodetic datum	Inaccurate position displayed	Deviation from route

Interconnection

The Interconnection is the gateway, cloud service and other equipment and means that links the information necessary to provide the different services in the STM concept. Error in the interconnection will have extensive effect on the systems performance.

Table 4 System Item Interconnection, PHL

Hazard	Hazard effects	Accident
Power failure	No route exchanged	Deviation from route
Power failure	No route received	Deviation from route
Power failure	No route sent	No route displayed
Information overload - in communication equipment	No route displayed	Traffic perplexity
Communication interruption	No route displayed	ETA deviation

Navigational equipment

The navigation of the ship is conducted by all available means. The use of other navigational equipment beside the route information provided is mandatory. Both to ensure the safe navigational of the vessel as controlling the reliability of the information provided via the services in the STM concept. Deviation between the information provide from different equipment must be controlled.

Table 5 System Item Navigational equipment, PHL

Hazard	Hazard effects	Accident
Radar and ECDIS position deviates	Uncertain route	Deviation from route
Compass displays incorrect course	Deviation from route	Deviation from route
Arpa and Route calculations deviates	Uncertain route	Navigational danger

Officer of the Watch, OOW

The performance of the OOW is critical for the safe navigation of the vessel and faults, misjudgements and poor decision-making are the source of numerous hazards. The OOW operates the system and makes calls based on how the system information is apprehended.

Table 6 System Item Officer of the watch, PHL

Hazard	Hazard effects	Accident
WP/Route negotiation	Close - quarters	Close - quarters
Workload -decision making	Stress	Poor decision making
Simultaneous change of route by ships/shore centre	Close - quarters	Congestion
Simultaneous change of route by ship to ship	Close - quarters	Close - quarters
Route not adapted to ship parameters	Navigational danger	Grounding
Reduced visibility	No visual confirmation available	Deviation from route
Over reliance of other ships route following	Ship do not follow route	Close - quarters
Over reliance	Inattentive	Close - quarters
Over reliance	Navigational danger	Grounding
Over reliance	No readiness of unexpected manoeuvres	Close - quarters
Over reliance	Reduces safety margins	Close - quarters
Not updating route after evasive manoeuvre	Deviation from route	Navigational danger
Not considering non STM compliant ship while altering route	Ship do not follow route	Close - quarters
Not consider drifting due to wind and current.	Deviation from route	Deviation from route
Not consider drifting due to wind and current.	Ship do not follow route	Close - quarters
None STM compliant ship	Congestion	Close - quarters
None STM compliant ship	Traffic perplexity	Close - quarters
No visual or radar confirmation of changed route	Traffic perplexity	Navigational danger
Misconception of distances ship to ship	Close - quarters	Close - quarters
Insufficient training in system	Uncertain route	Navigational danger
Insufficient training in system	Uncertain route	Navigational danger
Information overload - Override and block warnings	Poor decision making	Navigational danger
Information overload - Not observing all relevant ship routes	Close - quarters	Close - quarters
Information overload - blocks information	Poor decision making	Navigational danger
Information overload - Acoustic and visual pollution	Poor decision making	Navigational danger
Information overload	Poor decision making	Navigational danger
Incorrect WP data in route	Deviation from route	Close - quarters
Disagreement on route negotiation	Ship do not change route	ETA deviation

Disagreement on route negotiation	Ship do not follow route	ETA deviation
Disagreement on route negotiation	Ship do not follow route	Close - quarters
Deviation from route not observed	Close - quarters	Close - quarters
Deviation from route not observed	ETA deviation	ETA deviation
Deviation from route not observed	Traffic perplexity	Traffic perplexity
Cultural-hierarchic traditions	Ship do not change route	ETA deviation
Cultural-hierarchic traditions	Ship do not change route	Close - quarters
Cultural-hierarchic traditions	Ship do not follow route	ETA deviation
Cultural-hierarchic traditions	Ship do not follow route	Close - quarters
COLREG deviation agreed upon between ships	COLREG deviation	Close - quarters
COLREG deviation agreed upon between ships	Traffic perplexity	Close - quarters
Changing WP/route on short distances	Close - quarters	Close - quarters
Changing WP/route on short distances	Traffic perplexity	Close - quarters

Route receiving and Route sending

The system function of receiving and sending routes is the core function of the system. It is essential for the function of the system that the routes are displayed on the screens of the actors in the system

Table 7 System Item Route receiving as route sending, PHL

Hazard	Hazard effects	Accident
No ship to ship exchange	No route displayed	Deviation from route
No ship to shore exchange	No route displayed	Deviation from route
No transmission of route	No route displayed	ETA deviation
No transmission of route	No route displayed	Deviation from route
No transmission of route	No route displayed	Traffic perplexity
No ship to ship exchange	No route displayed	Deviation from route
No ship to shore exchange	No route displayed	Deviation from route
No transmission of route	No route displayed	ETA deviation
No transmission of route	No route displayed	Deviation from route
No transmission of route	No route displayed	Traffic perplexity

Ship

The ship is the overall hardware affected by external conditions such as wind, waves and current. Routes must in order not to cause hazards be adapted to the ships characteristics; there are a numerous ways of misinterpreting the information and feeding the system with fault data.

Table 8 System Item Ship, PHL

Hazard	Hazard effects	Accident
Wind	Deviation from route	Deviation from route
Rate of turn not in accordance to route/WPs	Deviation from route	Deviation from route
Preferred ship speed	Deviation from route	ETA deviation
Preferred ship speed	Deviation from route	Time separation error

Loss of propulsion	Deviation from route	Close - quarters
Loss of propulsion	Navigational danger	Close - quarters
Loss of propulsion	Speed decline	ETA deviation
Icing	Change of Rate of turn	Deviation from route
Icing	Change of Rate of turn	Close - quarters

Sea Traffic Control Centre, STCC

As STCC is a collection name of all the actors a shore that provide the ships with services included in the sub-concepts. As well as the OOW the operator a shore must interpret information and make decision to act upon. Misconceptions of the information about the traffic situation and ship parameters are certain sources of hazards. As well as sending route to direct traffic based on incorrect information.

Table 9 System Item Sea Traffic Control Centre, PHL

Hazard	Hazard effects	Accident
Workload -decision making	Stress	Poor decision making
Route not adapted to ship parameters	Navigational danger	Collision
None STM compliant ship	Congestion	Close - quarters
None STM compliant ship	Traffic perplexity	Close - quarters
No visual or radar confirmation of changed route	No confirmation of changed route	Deviation from route
No route updating between different Shore centres	Decline in flow optimisation	Inefficiency
No route updating between different Shore centres	Decline in flow optimisation	ETA deviation
Misconception of distances ship to ship	Close - quarters	Close - quarters
Incorrect WP data in route	Deviation from route	Close - quarters
Incorrect WP data in route	Incorrect route	ETA deviation
Disagreement on route negotiation	Ship do not change route	ETA deviation
Disagreement on route negotiation	Ship do not follow route	ETA deviation
Deviation from route not observed	Close - quarters	Close - quarters
Deviation from route not observed	ETA deviation	ETA deviation

System

Some hazards are more generic and connected to the overall performance of the system then to one of the defined system items.
Such as if system intentionally is disrupted or the hazard of a bad ergonomic working setup.

Table 10 System Item System, PHL

Hazard	Hazard effects	Accident
Route information disrupted intentionally	No route displayed	Navigational danger
Route information disrupted intentionally	Congestion	Close - quarters
Route information disrupted intentionally	Ship do not follow route	Close - quarters
Information overload	No route displayed	Traffic perplexity

Information expressed in foreign language or in unfamiliar terms	Poor decision making	Navigational danger
Important information hidden/ placed under sub functions	Poor decision making	Navigational danger
Ergonomic strain	Poor decision making	Navigational danger
Constrained work area	Poor decision making	Navigational danger

Top-Level-Accidents, TLA, and Safety Critical Functions, SCF.
Deviation from route and ETA deviation are not accidents with the directly effect of injuring personnel, ship or the environment. But the effects of those events have impact on the system and have been considered then in the analysis as accidents.

- Close – quarter, a number of hazards has the potential of putting the ship into close – quarter. A situation with a high risk of causing a collision. Collision is therefor considered to fulfil the requirements of a SCF. If system functions fail to prevent a collision, it is in this analysis considered to fulfil the requirements of a SCF.
- Collision is also identified as a TLA. A number of various hazards have the potential of causing a collision.
- Deviation from route: Ships that deviates from STCC suggested route, may risk of delaying planned ETA to other WPs or port call. As well as the deviation might cause grounding.
- ETA deviation: A number of hazards have the potential of deviating the route both in distance and speed. The outcome of the realisation of such hazards will cause delays in ETA.
- Grounding: Might be caused directly, as the effects of some hazards such as route not adjusted to ship parameters or over reliance in the system. Grounding is both a TLA and a SCF.
- Navigational Danger: A number of hazards have the potential of causing navigational danger both regarding own ship as for other traffic. E.g. workload of the OOW might cause poor decision making causing unnecessary complex traffic situations. The TLA is considered to cause both the SCFs Grounding and Collision.

5.1.2 Preliminary Hazard Analysis

The method of the Preliminary Hazard Analysis, PHA, uses the results from the Preliminary Hazard List, PHL, where hazards have been identified and TLAs and SCF have been defined.
The results from PHA are presented with tables extracted from Appendix 9.2.
Top – level – accident: One of the TLAs identified in the PHL method.
Hazard: The hazard being evaluated/tested.
Cause: Conditions, actions and events with the potential that can make the hazard develop into an accident.
Effect: The potential effect that the hazard and accident might develop into.
Mitigation/recommendation: Measures to mitigate or eliminate the hazard.

AIS
Table 11 System Item AIS, PHA

Top level accident	Hazards with potential to cause TLA	Cause	Effect	Mitigation/ recommendation
Close - quarter	AIS sends incorrect position	GPS error, Error in input settings e.g. geodetic datum	Collision	Back up and warning systems. Confirm position with all means
Collision	AIS sends incorrect position	GPS error, Error in input settings e.g. geodetic datum	Collision	Back up and warning systems. Confirm position with all means
Deviation from route	Wrong AIS information from other ship/STCC	Error in route transmission	Route negotiate error	Back up and warning systems. Confirm position with all means
Grounding	Wrong draught in Voyage specific data	Error in draught calculations or input	Ship may sail on route without acquired depth	Routines to confirm calculations and correct input to AIS
ETA deviation	AIS sends incorrect position to route	GPS error, Error in input settings e.g. geodetic datum	Ships position is wrong presented	Back up and warning systems. Confirm position with all means
Navigational danger	AIS sends incorrect position to route	GPS error, Error in input settings e.g. geodetic datum	Traffic perplexity	Back up and warning systems. Confirm position with all means

GPS

Table 12 System Item GPS, PHA

Top level accident	Hazards with potential to cause TLA	Cause	Effect	Mitigation/ recommendation
Close - quarter	Inaccurate position	Fault position sent to Navigational equipment and Route display	Safety distances not kept	Back up system, Confirm accurate position by all means
Deviation from route	Inaccurate position	Fault position sent to Navigational equipment and Route display	Wrong position displayed on route	Back up system, Confirm accurate position by all means
ETA deviation	Inaccurate position	Fault position sent to Navigational equipment and Route display	ETA delayed or miscalculated	Back up system, Confirm accurate position by all means
Grounding	Inaccurate position	Fault position sent to Navigational equipment and Route display	Grounding	Back up system, Confirm accurate position by all means
Navigational danger	Inaccurate position	Fault position sent to Navigational equipment and Route display	Fault navigation	Back up system, Confirm accurate position by all means

Interconnection

Table 13 System Item Interconnection, PHA

Top level accident	Hazards with potential to cause TLA	Cause	Effect	Mitigation/ recommendation
Close - quarters	No route exchange	Error in transfer of route data	Ship routes not presented on own display	Back up system. Use all means to position surrounding traffic
Collision	No route exchange	Error in transfer of route data	Ship routes not presented on own display	Back up system. Use all means to position surrounding traffic
Deviation from route	No route exchange	Error in transfer of route data	Traffic perplexity	Navigate on route with all navigational means
ETA deviation	No route exchange	Error in transfer of route data	Delayed or disrupted ETA	Back up system. Readiness to calculate ETA with other means

Navigational equipment

Table 14 System Item Navigational equipment, PHA

Top level accident	Hazards with potential to cause TLA	Cause	Effect	Mitigation/ recommendation
Close - quarter	ARPA and route prediction deviates	Error in route display or radar	Uncertainty of forthcoming traffic situation	Routine to ensure reliable ARPA function
Collision	Radar and ECDIS position deviates	Uncertainty of position on route	Uncertainty of correct position	Routine to ensure reliable ECDIS function
Deviation from route	Radar and route position deviates	Fault radar settings	Uncertainty of correct position	Routine to ensure reliable Radar function

Officer of the watch, OOW

Table 15 System Item Officer of the watch, PHA

Top level accident	Hazards with potential to cause TLA	Cause	Effect	Mitigation/ recommendation
Close - quarter	OOW do not keep distance to ensure freedom of manoeuvrability	Routes look safe on display, not using all navigational means or regarding external factors like and current	Ship might come into dangerous distance to other ship or obstacle	Control that safety distances are kept with all navigational means
Deviation from route	Not joining route after evasive manoeuver	Manoeuvring for other ship or obstacle	Ship not following route	Route deviation must be displayed on all ships/shore centres
ETA deviation	Not sailing at recommended speed to keep ETA	OOW uses ship preferred speed	ETA will not be accomplished	Ships preferred ship must be calculated with in Flow optimisation
Grounding	Do not control depth for suggested route	Draught exceeds depth in route	Grounding	Establish routines to check suggested routes before acceptance
Navigational danger	System functions leads to extensive workload	To much information presented to OOW	Increased risk of faulty navigation	Highlight relevant information and hide irrelevant information

Route receiving and Route sending

Table 16 System Item Route receiving and Route sending, PHA

Top level accident	Hazards with potential to cause TLA	Cause	Effect	Mitigation/ recommendation
Close - quarter	Route exchange not conducted	Equipment malfunction, Operational incapability	Route not displayed	Back up system, Sufficient training of operators
Collision	Route exchange not conducted	Equipment malfunction, Operational incapability	Route not displayed	Back up system, Sufficient training of operators
Deviation from route	Route exchange not conducted	Equipment malfunction, Operational incapability	Route not displayed	Back up system, Sufficient training of operators
ETA deviation	Route exchange not conducted	Equipment malfunction, Operational incapability	Route not displayed	Back up system, Sufficient training of operators
Grounding	Route exchange not conducted	Equipment malfunction, Operational incapability	Route not displayed	Back up system, Sufficient training of operators
Navigational danger	Route exchange not conducted	Equipment malfunction, Operational incapability	Route not displayed	Back up system, Sufficient training of operators

Ship

Table 17 System Item Ship, PHA

Top level accident	Hazards with potential to cause TLA	Cause	Effect	Mitigation/ recommendation
Close - quarter	Ship losses propulsion	Mechanical error.	Collision, grounding	Readiness to drop anchor in congested areas
Deviation from route	Rate of turn exceeds turns in route	Ships deviate rom route when altering course at WPs	Collision, grounding	Ship characteristics must be checked for all conditions
ETA deviation	External conditions hampers suggested speed	Wind, icing, current	Speed is reduced	Weather and other conditions must be calculated with when determining ETA
Grounding	Draught exceeds depth	Miscalculation of loading conditions	Route is to shallow for ship	Draught calculations must be coordinated with depth of route.

Sea Traffic Control Centre, STCC

Table 18 System Item Sea Traffic Control Centre, PHA

Top level accident	Hazards with potential to cause TLA	Cause	Effect	Mitigation/ recommendation
Close - quarter	STCC suggests route with to small margins of navigational safety	In order of optimising traffic flow	Ships will come into unsafe distance	Routes must be separated according to relevant safety distances
Congestion	Flow optimisation algorithm error	Algorithm does not calculate with none STM compliant ships	Ship traffic will not flow	All ships STM compliant
Deviation from route	STCC does not observe ships deviating from routes	No alarm system, Error in flow algorithm	Traffic will not flow according to plan	Warning system and routine of checking route following
ETA deviation	Flow optimisation algorithm error	Fault in algorithm	Port calls delayed	Algorithm must be adjusted and performance monitored
Grounding	Suggesting routes with not enough depth	Not regarding ship draught when distributing routes	Grounding	Routes must be cross checked

System

Table 19 System Item System, PHA

Top level accident	Hazards with potential to cause TLA	Cause	Effect	Mitigation/ recommendation
Close - quarter	Information overload	Operator/OOW can not make proper decision based on the amount of information presented	Navigational danger	Suppress irrelevant information
Collision	Workload	System is to complex to operate	Proper decision making is hampered	System design must enable efficient operating
Deviation from route	System not configured to present ETA calculations	System does not present relevant information	Correct ETA not presented	System configured to requested task
Grounding	System parameters are incorrect	Incorrect ship parameters enter into system	Risk of grounding	Routine to control parameters and data entered into the system

5.1.3 Fault Tree Analysis, FTA

Top events used in FTA are the results of the hazard identification methods represented by the PHL and PHA. The top events used in the FTAs were the two identified accidents *Collision* and *Grounding*. The "Tree structure" of the FTAs is attached to thesis as Appendix 9.3.

5.1.3.1 Collision

Top event: Collision, the event of that two or more ships run into each other.

Intermediate event: **Interaction**
Meaning that the distance between two or more ships will initiate interaction and collision will be inevitable. The intermediate event of **Interaction** is followed by the events of **Routes intersect** and **Routes to close.**

*Table 20: List of events, Top event **Collision**, Intermediate event **Interaction**, Primary events **Route interest** and **Routes to close.***

Primary event	Secondary event(s)	Basic event
Routes intersect	Routes not separated in time	Ship uses preferred ship instead of suggested speed by STCC
Routes intersect	Ship stays on route	Cultural hierarchy
Routes intersect	Ship stays on route	Error in receiving new route
Routes intersect	Ship stays on route	Workload
Routes intersect	No perception of none STM compliant ship	Over reliance in system
Routes intersect	No perception of none STM compliant ship	Information overload
Routes intersect	Route negation ship to ship	Ships do agree on new routes
Routes intersect	Route negation ship to ship	No structure/hierarchy in route negotiation
Routes intersect	Over reliance in STCC route	Other navigational means not used to control route
Routes intersect	Ships position not displayed on route	Fault in warning system
Routes to close	Margins to small	Misinterpret distances in system
Routes to close	Margins to small	Over reliance in suggested routes
Routes to close	Margins to small	Over reliance in other ships intentions

Intermediate event:
COLREG violation, meaning that ship manoeuvres caused by breaking COLREG results in collision. The intermediate event of **COLREG violation** is followed by the events that COLREG violation is **Intentional** or **Unintentional.**

*Table 21: List of events, Top event **Collision**, Intermediate event **COLREG violation**, Primary events* **Intentional** and **Unintentional**

Primary event	Secondary event(s)	Basic event
COLREG violation intentional	Route negotiation	Negotiating at short distances
COLREG violation intentional	Route negotiation	Creates situation for other ships
COLREG violation intentional	Not willing to leave route	Time pressure
COLREG violation unintentional	-	Over reliance in route system
COLREG violation unintentional	-	Not observing none STM compliant ship(s).
COLREG violation unintentional	Ships sends inaccurate dynamic AIS data	No visual confirmation

5.1.3.2 Grounding

Top event: Grounding. The event of that the draught of the ship exceeds the current deep. Grounding can have more or less severe consequences.

Intermediate event The intermediate events, are events where and how the grounding would take place. **Ship hits ground in route**

*Table 22: List of events, Top event **Grounding**, Intermediate event **Ship hits ground in route***

Primary event	Secondary event(s)	Basic event
Loading conditions	Wrong draught reported	STCC suggest shallow route
OOW fails to observe depth in route	Over reliance in STCC route	Do not cross check route
OOW fails to observe depth in route	Workload	Route negotiation
Does not follow new safe route sent by STCC	Workload	Information overload
Wrong draught in ship parameters	-	Input error
STCC suggest shallow route	OOW do not crosscheck	Over reliance

Intermediate event The intermediate events, are events where and how the grounding would take place. **Ship hits ground outside route**

*Table 23: List of events, Top event **Grounding**, Intermediate event **Ship hits ground outside route,** Primary event **Ship leaves route intentionally** and **Ship leaves route unintentionally***

Primary event	Secondary event	Basic event
Ship leaves route intentionally	Traffic situation	Traffic flow not considering none STM ships

Ship leaves route intentionally	Traffic situation	ARPA and Route prediction deviates.
Ship leaves route intentionally	Disagreement with STCC on route	Insufficient training in system.
Ship leaves route unintentionally	Navigational error	Incorrect WPs in route
Ship leaves route unintentionally	Positional error	Not using all means to establish a correct position
Ship leaves route unintentionally	Warning system	No warning system/Fault settings

5.1.4 Risk assessment

Personnel
Personnel might get injured if accidents occur. Severity classified I to IV.
I - Death
II – Serious injury requiring hospital care, and full recovery might not be able
III – Less serious injury that requires medical attention and the person will be fully recovered.
IV – The injury is negligible and the person can return to duty after minor medical care.
Ship/system damage
The accidents might cause damages on property such as structural damages
Severity classified I to IV
I – Systems cannot be repaired. Ship sinks or is damaged beyond chance of repair.
II – Ship is affected in such a way that in cannot conduct its tasks in the system.
III – Ship or system is affected but still conducts it tasks in the system.
IV – No restrictions.
Environment
Accidents in the system might have effect on the surrounding environment. Severity classified I to IV
I – Serious effect on the environment that requires considerable efforts to restore. The natural effect to restore is heavily affected.
II – Serious effect. The environment will recover, considerable efforts required to assist the naturel recovery.
III – Less serious effect that requires small efforts to restore, the natural recover will be effective
IV – Small or less serious effect that do not require any recovery measures. The natural recovery is sufficient.
.
Table 1: Risk assessment matrix (Ericson 2005)

Severity	Probability
I. Catastrophic	A. Frequent
II. Critical	B. Probable
III. Marginal	C. Occasional
IV. Negligible	D. Remote
	E. Improbable

Table 24: Result of risk assessment

	Personnel	System/Ship	Environment
Collision	III C	II B	II B
Grounding	III D	II B	BI/II

5.1.5 Mitigation

The identified basic events that are the result of the FTA analysis are processed to find countermeasures to mitigate or eliminate the hazard.
The basic events are considered to have similarities with the effects of hazards identified in the PHA.

5.1.5.1 Countermeasures to Basic Events

Some Basic events share the same countermeasure. The result in this section is presented by a list of basic events and those countermeasures that may be effective to counter that the basic event initiated by the top event.

Table 25: Countermeasures to basic events, FTA

Basic event	**Countermeasure**
Time pressure	All actors in STM must comply STCC direction of traffic.
Insufficient training in system.	All operators must be certified
Fault in warning system	Back up systems. No over reliance in system
Error in receiving new route	Back up systems. No over reliance in system
Cultural hierarchy	Cultural awareness of all actors. Robust reporting and follow up routines.
Not observing none STM compliant ship(s).	Navigational and traffic situation must be controlled by all means at all times.
No warning system/Fault settings	Navigational and traffic situation must be controlled by all means at all times.
No visual confirmation	Navigational and traffic situation must be controlled by all means at all times.
ARPA and Route prediction deviates.	Navigational and traffic situation must be controlled by all means at all times.
Information overload	Only relevant data and information presented for system operators. Suppress irrelevant data at complex situations.
Information overload	Only relevant data and information presented for system operators. Suppress irrelevant data at complex situations.
Over reliance in system	Operators must be trained of handling the system with regard to its limitations, sources of error and restrains
Over reliance in suggested routes	Operators must be trained of handling the system with regard to its limitations, sources of error and restrains
Over reliance in route system	Operators must be trained of handling the system with regard to its limitations, sources of error and restrains

Over reliance in other ships intentions	Operators must be trained of handling the system with regard to its limitations, sources of error and restrains
Over reliance	Operators must be trained of handling the system with regard to its limitations, sources of error and restrains
Other navigational means not used to control route	Position and navigational progress must be confirmed with all available means
Not using all means to establish a correct position	Position and navigational progress must be confirmed with all available means
Misinterpret distances in system	Position and navigational progress must be confirmed with all available means
Incorrect WPs in route	Position and navigational progress must be confirmed with all available means
Route negotiation	Route negotiation must be conducted and confirmed at safe distance
No structure/hierarchy in route negotiation	Route negotiation must be conducted and confirmed at safe distance
STCC suggest shallow route	Routes must be cross checked by all actors before acceptance.
Do not cross check route	Routine of always compare route condition and ship parameters.
Ships do agree on new routes	Routine of prioritizing routes accepted and implemented by all actors.
Negotiating at short distances	Routine of prioritizing routes accepted and implemented by all actors.
Creates situation for other ships	Routine of prioritizing routes accepted and implemented by all actors.
Input error	Routine to control ship parameters before entered into system
Ship uses preferred ship instead of suggested speed by STCC	Ship parameters of preferred speed known and agreed upon with STCC.
Traffic flow not considering none STM ships	STCC and OOW must have awareness of the restrictions of route use since not all actors at sea are part of the system
Workload	System must be designed to ease up operations and smooth handle data. Warning systems to detect current and expected situations with overwhelming workload.

5.1.5.2 Mitigation/recommendations from PHL

Identified measures and recommendations to reduce hazards and avoid accidents are here compiled with the relevant results highlighted.

- Algorithm used in Flow Optimisation should have routine to over time improve the performance in order to work as most efficient.
- Awareness must be raised that not all ships are part of STM and that might cause traffic situations due to unawareness of such ships.
- Back up functions in route exchange system and for supporting sub-systems such as AIS and GPS.
- Warning systems that detect deviation from route for ships and STCC.
- Warnings systems that alert if route conditions conflict with ship characteristics such as draught and Rate of turn.
- Sufficient training in handling the system. All operators should be certified to increase level of correct use of system.
- Use of all navigational means to navigate and establish a correct position to counter act over reliance in the system.
- Routine to verify input and reporting of ship parameters and characteristics.
- Keeping safety distances at all situations, and not relying of route data of keeping safe distances to other vessels for safe navigation.
- Routines of crosschecking routes. All actors should have established routine to control that route and ship characteristics comply.
- Routine to verify performance of route exchange system with all available means and navigational equipment such as radar and visual methods.
- Ships preferred speed must be known and considered by STCC when suggesting routes.
- The effect of external factors such as wind, waves and current must be considered both to ensure safe navigation and calculate reliable ETAs.

6 Discussion

The aim of this chapter is to present and discuss the major finding as well as discuss the methodology used in the thesis. The chapter is divided into different sections to keep it easier to follow the discussions. The order of the discussions is: results from the system safety analysis, the system safety methodology and finally research methodology.

6.1 Results from the System safety analysis.

The system safety analysis had the aim of answering the first research question i.e. *What are the major safety issues in the STM concept and what are suitable measures to mitigate risks and thereby enhance safety*? The discussion below discusses how well that was achieved.

The general result of the system safety process indicates a number of areas and functions in the system that may be subject to development. This is to improve and enhance the objective of safer shipping with the implementation of the system. Considering the route exchange function as the core function of the system. That is that the actors in the system have the ability to send and receive information that display ships routes as well as suggestions to change routes. The route exchange function is considered to have the ability to enhance safety at sea by providing an improved situational awareness. This function is also the main source of the hazards that have been identified in the system safety process.

The major findings are discussed and presented in the same order as the system safety was done i.e. hazard identification, risk assessment and risk mitigation.

Hazards

As mentioned the system relies on the accurate exchange of routes between the actors in the system. This will enhance situational awareness, optimize traffic flow and enable functions such as precise just in time arrivals to port. A number of factors might have the effect of hampering the efficiency of reaching those objectives.

Being part of the system is voluntarily and there seems to be a lack of hierarchy in the system to handle conflicting interest e.g. change of requested ETAs, right of certain routes and handling disagreements in ship-to-ship route negotiating.

Another factor that might contradict the function is the right of the ships Master to always have the final call of the actions taken by the ship. The Master can instantly, at any moment, reject route suggestions and route negotiating. This combined that COLREG always is in force may hamper the effectiveness or contradict the route exchange function. The system relies on that ships voluntarily comply, which may be functional, but the presence of ships not taken part in the system must be considered.

None STM compliant ships will more or less interact with the system and hamper the system performance.

Route parameters such as draught, air draught, width and radius of curves in the channel will have affect. The route parameters must fit the ship characteristics in order not produce hazards and accidents. The number of hazards identified from that concern in the process are several. E.g. the route parameters are not crosschecked by the OOW due to over reliance in the system. Ship characteristics are incorrect in the way that inaccurate values have been entered into the system or interpreted incorrectly. Further might route negotiation between ships during time pressure result in that the route not is checked and confirmed to fit ship characteristics.

The system performance relies on a number of sub-systems such as AIS, GPS, interfaces and communication equipment. Not working correct or submitting incorrect information will have impact on the performance of the system. Routes with incorrect data might be presented or not presented at all. The hazard indicates that ships due to this will deviate or use wrong route and the probability of accidents increases.
Identified hazards indicates that the use of the system leads to that other navigational means are put aside or used less frequently e.g. use of radar and visual methods i.e. the use of all available means to perform correct and safe navigation. Relevant and important examples of this are route acceptance without crosschecking due to over reliance, workload, information overload and cultural hierarchy. And over reliance of that the actions of none STM compliant ships are considered in the traffic management. The system may present too much irrelevant information leading to heavy workload that hampers decision-making especially in complex traffic situations.

Risk assessment
All operations at sea involves some kind of risk, as previous stated is risk the probability of an accident to occur times the consequence of the outcome of the accident. In the system safety work conducted a number of top-level-accidents, TLAs and Safety Critical Functions, SCFs where derived. The probability and consequences of the accident where assessed. The evaluation was done qualitative and based on the writers experience and knowledge as well as the information gained from the process of collecting and assessing data to be used. No statistical data was used to evaluate the probability of the accidents. Evaluating the risks using relevant statistics is recommended for further studies when data from the STM validation project are available. Concerning the accidents that have the most severe consequence are unmistakably Collision and Grounding, The consequences are structural damages, high risk of injuring personnel and discharge of harmful substances.
The accidents Grounding and Collision are ever present at sea and they cannot be isolated to be the product of hazards that especially occurs in the STM concept.

Mitigation
The system safety process also aims of finding measures to mitigate the hazards that are identified. Measures are identified in the techniques PHA and FTA, though named differently countermeasures derived from Basic events and Recommendations derived from the PHA serve the same purpose.
The mitigation measures are compiled as to correspond to the discussed issues in the result chapter section 5.1.5. In order to mitigate the present risk of that the ship would be let to sail in a route where hazards are present robust routines should be implemented, routines to cross check all routes, both own generated and suggested routes. Routines to prioritize routes and ships coordinated with the ships desired ETA, this is a function that STM is based on but in the event of frictions and disagreements between actors an agreed prioritizing process should take place. Close – quarter situations should be predicted and last minute manoeuvring according to COLREG should then be avoided. The role of the master should be discussed to guarantee compliance and acceptance of route directions and traffic management. Traffic optimisation must also consider and have an active data exchange concerning optimised speed for traffic flow and ships preferred speed.
To mitigate the hazards that the route parameter does not fit the ship characteristics a number of actions are possible. Routines to cross check routes by all actors must be

established. Strict routines of how and when route negotiation is allowed. Introduce active measures that verify that all actors have controlled the route parameters and compared with the characteristics of the ship.
Robust warning systems are essential that verifies the operating status of the system. All actors and operator must be properly trained to distinguish fault data/information. Ship position and navigational progress must be verified and controlled by all means. As in all systems one vital component is the operator that handles, interpret information, supervise, make decisions and carry out the actions. As stated by Reason (Reason 2000) it is easy to blame the human when error occur instead of investigating if the system is causing the error.
The STM concept is a complex system with many components ranging from human operator to technical equipment. Hazards identified in the process are in many ways connected to human error both as the hazard itself as well as the cause and effect of the hazard that might to lead to the release of an accident. The results indicates that it is important that the system is designed in such a way that the work load is kept at a minimum and that irrelevant information is suppressed or vital data highlighted at certain occasion such during complex traffic situations. Over reliance of the system is also a hazard repeatedly identified. Over reliance can be counter measured by robust routines that remind the operator to use all available means for navigation.
The hazard that ships do not change routes due to cultural hierarchy is a complex issue and it might be difficult to find countermeasures in a systems analysis. The counter measure to that hazard is probably best identified during the education process of becoming an officer on board.

6.2 System safety process

Has the second question been answered i.e. *Is system safety a suitable methodology to identify safety issues in STM or similar concepts?*

How and what parts to include in the system safety process was determined by studying relevant literature and discussions with a person that has conducted such analysis in an industrial context. The interviewee and literature review suggested that relevant literature to conduct the process could be retrieved from manuals and books used in a military and military industrial context as well as literature with a broader perspective on several areas where system safety is an accepted process.
An objective of the thesis was to learn more about system safety work, which is fulfilled by the studying the theoretical background as well as the literature that describes how to conduct the process.
The literature review did not indicate or found any approaches to conduct a system safety analysis on a system like the STM concept. That strengthens the research question of assessing if the process is suitable for systems like STM but is troublesome in the way that there is no conducted analysis to compare the results with. The impression is that the methodology used in the process is suitable and that system safety can be an appropriate way of finding and enhancing safety issues in systems like STM. The method should also be suitable to analyse parts of the system not only looking at the system as whole unit. That would probably lead to more detailed and specific identification of hazards and risks. Also as indicated in interviews that the result of the process often is applicable of how much resources are put into the process concerning number of people and time. The analysis has been carried out by a single person, the writer, without previous experience of conducting

system safety work as defined in the literature. To verify the divergence of that factor perhaps the work has to be done with a team with experience to have relevant data to compare with. The system safety process might be very long and comprehensive, in this case a number of suitable methods and techniques have been chosen. Even if the process in the thesis might be considered shallow and short, it is considered sufficient to fulfil the objective of the thesis. Even if only parts of the process are used and presented in the thesis the whole process has been studied and understood as part of the learning process of writing the thesis. It might be the fact that in order to design the process in a proper way a thorough understanding of all parts is required.
The process is considered to fulfil the requirements of transferability since it is clearly described and presented. The results might be difficult to confirm since no other system safety process in the areas have been identified. The methods used are generally accepted but factors such as experience and the delimitations must be considered if the process fulfils relevant requirements of conformability.

6.3 Research methodology

This section primary discuss the methods used to collect the data used in the thesis. Both secondary and primary data has been collected in order to conduct the system safety process as well as presenting the background and theoretical background of the subjects in the thesis.

6.3.1 Literature review

The literature review is considered to be a collection of secondary data. The secondary data has been used to achieve an understanding of the subjects and the underlying theoretical framework. Issues to regard when colleting secondary data is that the data initially not was produced for the purposes they are used for in the thesis. A critical stand must be taken when assessing how the data can come into use and the relevance of it. I.e. can the data be used to answer the research questions (Vaus & Vaus 2001)? Factors that support if the process is done correct and what strengthens and weakens it must be considered (Höst et al. 2006). The literature review is considered to have found relevant data covering the major concerns of preparing the system safety analysis, constructing a solid background and understanding the theoretical framework. It has certainly not covered all available data in the field but the structure of the review, as described in chapter 3 section 3.2, gives confidence that enough relevant data has been found and studied supporting the reliability of the data collection. When finding data for the theoretical framework the “authorities” in the field are considered to have been identified and articles of those have been used. Concerning data for deepening the understanding of the Sea Traffic Management concept, STM, the data is mainly extracted from literature authored by persons involved in the project and with dependability that the project is successful. Even so the data is considered to be reliable since the authors hold high scientifically credibility.

6.3.2 Interviews

Interviews are often a valuable source of information, but as with any other data it should be critically estimated. Interviews are in one way a fact seeking process but the facts that are delivered may be affected by different sources. The interviewees might be affected to provide a positive picture of the interview topic having a dependability

being involved in the work or development. As the STM expert wants to enhance to positive effects and the interviewee with systems safety experience wants to highlight it as an effective process. As discussed by (Czarniawska 2004) if the interviewee is delivering facts or is the interview and exchange of the persons views of the topic. Either way the interviews were considered to add valuable data to the thesis and there are no concerns that invalid data was given. The most interviews are reliable since there is often no gain of distorting or making up incorrect data (Czarniawska 2004).

7 Conclusion

The process of writing the thesis has certainly reached the objective of enhancing the writer's knowledge of Sea Traffic Management and System safety. However if the thesis reached the other objectives and answered the research questions follows below.

The STM concept is considered in many ways to have a firm stand in the development of the shipping industry, digitization and information sharing are areas developing in a fast pace in society and industry. That shipping is taking those steps seems logical and natural. The implementation of the STM concept brings a lot of benefits, but as the system analysis indicates the system will have hazards that should be dealt with. Identifying these hazards has been the major effort of the thesis. The hazards and risks considered most relevant for further analysis are those linked to how the information is handled and the use of the system. This since the results indicates that if the information in the system is inaccurate or interpreted incorrectly the risk in the system for accidents rise considerably. It is also vital for the safety in the system that the operators understand the limitations of the system, are able to deal with uncertainties and use all means to monitor and control the systems performance.

The system safety process is assessed to be useful to identify hazards and finding ways of enhancing safety in the system. This is considered to be the main contributions for further safety work in the STM concept. Even though system safety is a process that can be used in many ways, the skilfulness of the performer is probably more important of achieving relevant results then following a specific process. Most fair is to consider the result as an indicator of what could be done to improve the system and not as hard facts. The overall conclusion might be that the implementation of new systems must be the subject of thorough analysis processes to detect safety concerns not accounted for.

It might be considered if a more thorough and detailed system safety analysis of all parts of STM could be beneficial. An analysis conducted by those involved in the development of STM and experts in system safety would perhaps identify a wide range of improvements in the concept.

8 References

Andersson, A. & Forsman, B., 2015. *FSA – Formal Safety Assessment of the STM concept*,

Czarniawska, B., 2004. Czarniawska, Barbara. Narratives in Social Science Research. London, GBR: SAGE Publications Ltd. (UK), 2004. ProQuest ebrary. Web. 8 January 2016. Copyright © 2004. SAGE Publications Ltd. (UK). All rights reserved. , (January).

DoD, 1993. MIL-STD-882C. , (MIL - STD -882C). Available at: http://www.fmv.se/Global/Dokument/Verksamhet/Systemsäkerhet/MIL-STD-882C.pdf.

Ericson, C., 2011. *Concise Encyclopedia of System Safety*, Hoboken, US: Wiley. Available at: ProQuest ebrary. Web. 20 January 2016.

Ericson, C.A., 2005. *Hazard analysis techniques for system safety*,

Falnes, S.T., 2015. The Strategic Voyage Management Description. *MONALISA 2.0*, 0_D2.3.1-4, pp.1–20. Available at: http://stmvalidation.eu/wp-content/uploads/ML2-D2.3.1-4.1-Strategic-Voyage-Management-Description.pdf.

FMV, 2015a. *Checklist of Hazards and hazardous conditions*, Available at: http://www.fmv.se/Global/Dokument/Verksamhet/Systemsäkerhet/HSystSäk/PHL-mall-template_ver.2.0_Sv-Eng.docx.

FMV, 2015b. Systemsäkerhetsplan (SSPP) för leverantör. Available at: http://www.fmv.se/Global/Dokument/Verksamhet/Systems?kerhet/HSystS?k/121101/Systems?kerhetsplan (SSPP).f?r leverant?r.doc.

FMV, 2015c. *Systemsäkerhetsplan för SSWG-2*, Available at: http://www.fmv.se/Global/Dokument/Verksamhet/Systemsäkerhet/Stöddokument för systemsäkerhet/Systemsäkerhetsplan (SSPP) för arbetsgrupp.doc.

Gustafsson, E. & Åding, P., 2014. *Taktiskt ruttutbyte ship-to-ship och dess relation till COLREG*. Chalmers University of Technology. Available at: http://studentarbeten.chalmers.se/publication/212717-taktiskt-ruttutbyte-ship-to-ship-och-dess-relation-till-colreg [Accessed April 27, 2016].

Heurlin, H., 2015. STM Onboard Systems.

Hägg, M., 2015. *Concept of operation and standard operating procedures for Sea Traffic Management Services*,

Hägg, M. & Ferrús Clari, G., 2015. Flow management Description. *MONALISA 2.0*, 0_D2.3.1-4, pp.1–18. Available at: http://stmvalidation.eu/wp-content/uploads/ML2-D2.3.1-4.3-Flow-Managment-Description.pdf.

Hägg, M. & Lind, M., 2015. Sea Traffic Managment A Holistic View. *MONALISA 2.O*, ML2-D2.3.1. Available at: http://stmvalidation.eu/wp-content/uploads/ML2-D2.3.1-4.0-Sea-Traffic-Managment-A-Holistic-View.pdf.

Höst, M., Regnell, B. & Runeson, P., 2006. *Att genomföra examensarbete*, Studentlitteratur.

Kitchenham, B., 2004. Procedures for performing systematic reviews. *Keele, UK, Keele University*, 33(TR/SE-0401), p.28. Available at:

http://csnotes.upm.edu.my/kelasmaya/pgkm20910.nsf/0/715071a8011d4c2f482577a700386d3a/$FILE/10.1.1.122.3308[1].pdf\nhttp://tests-zingarelli.googlecode.com/svn-history/r336/trunk/2-Disciplinas/MetodPesquisa/kitchenham_2004.pdf.

Lantz, A., 2007. *Intervjumetodik*, Studentlitteratur.

LaPorte, T.R. & Consolini, P.M., 1991. Working in Practice but Not in Theory: Theoretical Challenges of "High-Reliability Organizations." *Journal of Public Administration Research and Theory: J-PART*, 1(1), pp.19 – 48.

Leveson, N., 2004. A new accident model for engineering safer systems. *Safety Science*, 42(4), pp.237–270. Available at: http://www.sciencedirect.com/science/article/pii/S092575350300047X [Accessed January 10, 2016].

Leveson, N. et al., 2009. Moving Beyond Normal Accidents and High Reliability Organizations: A Systems Approach to Safety in Complex Systems. *Organization Studies*, 30(2-3), pp.227–249.

Leveson, N., 2003. White paper on approaches to safety engineering. *Disponible en ligne sur le site de l'auteur (sunnyday. ...*. Available at: http://www.idc-online.com/technical_references/pdfs/mechanical_engineering/concepts.pdf [Accessed April 26, 2016].

Leveson, N.G., 2011. Applying systems thinking to analyze and learn from events. *Safety Science*, 49(1), pp.55–64. Available at: http://www.sciencedirect.com/science/article/pii/S0925753510000068 [Accessed February 24, 2016].

Lind, M. et al., 2014. Digital Infrastructures for enabling Sea Traffic Management. *The 10th International Symposium ISIS 2014 "Integrated Ship's Information Systems"*.

Lind, M. et al., 2015. Service and communication infrastructure for Sea Traffic Management. *14th International Conference on Computer Applications and Information Technology in the Maritime Industries*, pp.290–305. Available at: http://monalisaproject.eu/wp-content/uploads/Compit-2015-Service-and-Comm-Infra-Lind.pdf.

Lind, M. & Haraldsson, S., 2015. Port Collaborative Decision Making Description. *MONALISA 2.0*, 0_D2.3.1-4, pp.1–32. Available at: http://stmvalidation.eu/wp-content/uploads/ML2-D2.3.1-4.4-Port-Collaborative-Decision-Making-Description.pdf.

Mona Lisa 2.0, 2015. MONALISA 2.0. Available at: http://monalisaproject.eu/ [Accessed February 23, 2016].

Rasmussen, J., 1997. Risk management in a dynamic society: a modelling problem. *Safety Science*, 27(2-3), pp.183–213. Available at: http://www.sciencedirect.com/science/article/pii/S0925753597000520 [Accessed March 16, 2016].

Raviola, E., 2014. Lecture 5 in Research methods, qualitative methods strand.

Reason, J., 1990. *Human error*, Cambridge Univ. Press.

Reason, J., 2000. Human error: models and management. *BMJ (Clinical research*

ed.), 320(7237), pp.768–70. Available at: http://www.pubmedcentral.nih.gov/articlerender.fcgi?artid=1117770&tool=pmcentrez&rendertype=abstract [Accessed December 12, 2014].

Sagan, S.D., 1993. *The limits of safety*, Princeton Univ. Press.

Shahriari, M., 2013. Main concepts of risk in engineering. In M. Shahriari, ed. *Loss Prevention and Safety, A practical risk management handbook. Volume 1*. Göteborg: Chalmers University of Technology.

Siwe, U. et al., 2015. Sea Traffic Management – Concepts and Components. *14th International Conference on Computer Applications and Information Technology in the Maritime Industries*, pp.281–289.

Sjöfartsverket, 2016. Grunden läggs för säkrare och effektivare handelssjöfart - Sjofartsverket. *2016-01-29*. Available at: http://www.sjofartsverket.se/sv/Press/Nu-ska-fartygen-borja-prata-med-varandra/ [Accessed February 24, 2016].

STM Masterplan, 2015. What is STM? | STM. Available at: http://stmmasterplan.com/what-is-stm/ [Accessed April 18, 2016].

STM Validation Project, 2016. Sea Traffic Management Validation Project. Available at: http://stmvalidation.eu/ [Accessed April 18, 2016].

STM Validation Project, 2015. STM Validation Project Description. *STM*. Available at: http://monalisaproject.eu/wp-content/uploads/STM-Project-Info-v-1-00.pdf.

Svedberg, U. & Andreasson, B., 2015. Dynamic Voyage Management Description. *MONALISA 2.0*, 0_D2.3.1-4, pp.1–18. Available at: http://stmvalidation.eu/wp-content/uploads/ML2-D2.3.1-4.2-Dynamic-Voyage-Management-Description.pdf.

Swedish Armed Forces, 2011a. *Armed Forces´Handbook on System Safety 2011 Part 1 - Common* M7739–3520th ed. M. Lundgren, ed., Stockholm: The Armed Forces' Security Inspectorate and Swedish Defence Materiel Administration. Available at: https://www.fmv.se/Global/Dokument/Engelska webben/Our activities/System Safety/ipm_h_systsak_e_2011_part_1.pdf.

Swedish Armed Forces, 2011b. *Armed Forces´Handbook on System Safety 2011 Part 2 - Methods* M7739–3520th ed. M. Lundgren, ed., Stockholm: The Armed Forces' Security Inspectorate and Swedish Defence Materiel Administration. Available at: https://www.fmv.se/Global/Dokument/Engelska webben/Our activities/System Safety/ipm_h_systsak_e_2011_part_2.pdf.

Vaus, D.A. De & Vaus, P.D. de, 2001. *Research Design in Social Research*, Available at: https://books.google.com/books?hl=sv&lr=&id=9yurQt7T65oC&pgis=1 [Accessed April 20, 2016].

Velásquez Correa, S.I. et al., 2015. *MONALISA 2.0 and the sea traffic management - a concept creating the need for new maritime information standards and software solutions*, Available at: http://upcommons.upc.edu/handle/2117/26997 [Accessed March 7, 2016].

Vincoli, J.W., 2014. *Basic guide to System Safety*, Hoboken, US: Wiley.

9 Appendix

9.1 Preliminary Hazard List

9.2 Preliminary Hazard Analysis

9.3 Fault tree analysis

9.1 Preliminary Hazard list

Number	System Item	Hazard	Hazard effects	Accident	TLA
PHA 1	AIS	Inaccurate dynamic data - Navigational status	COLREG deviation	Close - quarters	Close - quarter
PHA 2	AIS	Inaccurate dynamic data - Rate of turn	Deviation from route	Close - quarters	Close - quarter
PHA 3	AIS	Inaccurate dynamic data - position	Inaccurate position displayed	Deviation from route	Deviation from route
PHA 4	AIS	Inaccurate voyage data - UKC	Navigational danger	Grounding	Grounding
PHA 5	AIS	Ghost vessels	Traffic perplexity	Navigational danger	Navigational danger
PHA 6	AIS	Inaccurate dynamic data - COG, SOG	Traffic perplexity	Close - quarters	Close - quarter
PHA 7	GPS	Deviant geodetic datum	Inaccurate position displayed	Deviation from route	Deviation from route
PHA 8	GPS	Position error GPS	Inaccurate position displayed	Deviation from route	Deviation from route
PHA 9	Interconnection	Power failure	No route exchanged	Deviation from route	Deviation from route
PHA 10	Interconnection	Communication interference	No route displayed	Deviation from route	Deviation from route
PHA 11	Interconnection	Communication interruption	No route displayed	ETA deviation	ETA deviation
PHA 12	Interconnection	Communication interruption	No route displayed	Traffic perplexity	Congestion
PHA 13	Interconnection	Information overload - in communication equipment	No route displayed	Traffic perplexity	Congestion
PHA 14	Interconnection	Power failure	No route received	Deviation from route	Deviation from route
PHA 15	Interconnection	Power failure	No route sent	No route displayed	Congestion
PHA 16	Nav. Equip.	Compass displays incorrect course	Deviation from route	Deviation from route	Deviation from route
PHA 17	Nav. Equip.	Arpa and Route calculations deviates	Uncertain route	Navigational danger	Navigational danger
PHA 18	Nav. Equip.	Radar and ECDIS position deviates	Uncertain route	Deviation from route	Deviation from route

PHA 21	OOW	Information overload - Not observing all relevant ship routes	Close - quarters	Close - quarters	Close - quarter
PHA 22	OOW	Misconception of distances ship to ship	Close - quarters	Close - quarters	Close - quarter
PHA 23	OOW	Simultaneous change of route by ship to ship	Close - quarters	Close - quarters	Close - quarter
PHA 24	OOW	Simultaneous change of route by ships/shore centre	Close - quarters	Congestion	Congestion
PHA 25	OOW	WP/Route negotiation	Close - quarters	Close - quarters	Close - quarter
PHA 26	OOW	COLREG deviation agreed upon between ships	COLREG deviation	Close - quarters	Close - quarter
PHA 27	OOW	None STM compliant ship	Congestion	Close - quarters	Close - quarter
PHA 28	OOW	Incorrect WP data in route	Deviation from route	Close - quarters	Close - quarter
PHA 29	OOW	Not consider drifting due to wind and current.	Deviation from route	Deviation from route	Deviation from route
PHA 30	OOW	Not updating route after evasive manoeuvre	Deviation from route	Navigational danger	Navigational danger
PHA 31	OOW	Deviation from route not observed	ETA deviation	ETA deviation	ETA deviation
PHA 32	OOW	Over reliance	Inattentive	Close - quarters	Close - quarter
PHA 33	OOW	Over reliance	Navigational danger	Grounding	Grounding
PHA 34	OOW	Route not adapted to ship parameters	Navigational danger	Grounding	Grounding
PHA 35	OOW	Over reliance	No readiness of unexpected manoeuvres	Close - quarters	Close - quarter
PHA 36	OOW	Reduced visibility	No visual confirmation available	Deviation from route	Deviation from route
PHA 37	OOW	Information overload	Poor decision making	Navigational danger	Navigational danger
PHA 38	OOW	Information overload - Acoustic and visual pollution	Poor decision making	Navigational danger	Navigational danger
PHA 39	OOW	Information overload - blocks information	Poor decision making	Navigational danger	Navigational danger
PHA 40	OOW	Information overload - Override and block warnings	Poor decision making	Navigational danger	Navigational danger

PHA 41	OOW	Over reliance	Reduces safety margins	Close - quarters	Close - quarter
PHA 42	OOW	Cultural-hierarchic traditions	Ship do not change route	ETA deviation	ETA deviation
PHA 43	OOW	Cultural-hierarchic traditions	Ship do not change route	Close - quarters	Close - quarter
PHA 44	OOW	Disagreement on route negotiation	Ship do not change route	ETA deviation	ETA deviation
PHA 45	OOW	Cultural-hierarchic traditions	Ship do not follow route	ETA deviation	ETA deviation
PHA 46	OOW	Cultural-hierarchic traditions	Ship do not follow route	Close - quarters	Close - quarter
PHA 47	OOW	Disagreement on route negotiation	Ship do not follow route	ETA deviation	ETA deviation
PHA 48	OOW	Disagreement on route negotiation	Ship do not follow route	Close - quarters	Close - quarter
PHA 49	OOW	Not consider drifting due to wind and current.	Ship do not follow route	Close - quarters	Close - quarter
PHA 50	OOW	Not considering non STM compliant ship while altering route	Ship do not follow route	Close - quarters	Close - quarter
PHA 51	OOW	Over reliance of other ships route following	Ship do not follow route	Close - quarters	Close - quarter
PHA 52	OOW	Workload -decision making	Stress	Poor decision making	Navigational danger
PHA 53	OOW	Changing WP/route on short distances	Traffic perplexity	Close - quarters	Close - quarter
PHA 54	OOW	COLREG deviation agreed upon between ships	Traffic perplexity	Close - quarters	Close - quarter
PHA 55	OOW	Deviation from route not observed	Traffic perplexity	Traffic perplexity	Navigational danger
PHA 56	OOW	No visual or radar confirmation of changed route	Traffic perplexity	Navigational danger	Navigational danger
PHA 57	OOW	None STM compliant ship	Traffic perplexity	Close - quarters	Close - quarter
PHA 58	OOW	Insufficient training in system	Uncertain route	Navigational danger	Navigational danger
PHA 59	OOW	Insufficient training in system	Uncertain route	Navigational danger	Navigational danger
PHA 60	Route receiving	No ship to ship exchange	No route displayed	Deviation from route	Deviation from route
PHA 61	Route receiving	No ship to shore exchange	No route displayed	Deviation from route	Deviation from route
PHA 62	Route receiving	No transmission of route	No route displayed	ETA deviation	ETA deviation
PHA 63	Route receiving	No transmission of route	No route displayed	Deviation from route	Deviation from route
PHA 64	Route receiving	No transmission of route	No route displayed	Traffic perplexity	Congestion

PHA 65	Route sending	No ship to ship exchange	No route displayed	Deviation from route	Deviation from route
PHA 66	Route sending	No ship to shore exchange	No route displayed	Deviation from route	Deviation from route
PHA 67	Route sending	No transmission of route	No route displayed	ETA deviation	ETA deviation
PHA 68	Route sending	No transmission of route	No route displayed	Deviation from route	Deviation from route
PHA 69	Route sending	No transmission of route	No route displayed	Traffic perplexity	Congestion
PHA 70	Ship	Icing	Change of Rate of turn	Deviation from route	Deviation from route
PHA 71	Ship	Icing	Change of Rate of turn	Close - quarters	Close - quarter
PHA 72	Ship	Loss of propulsion	Deviation from route	Close - quarters	Close - quarter
PHA 73	Ship	Preferred ship speed	Deviation from route	ETA deviation	ETA deviation
PHA 74	Ship	Preferred ship speed	Deviation from route	Time separation error	Congestion
PHA 75	Ship	Rate of turn not in accordance to route/WPs	Deviation from route	Deviation from route	Deviation from route
PHA 76	Ship	Wind	Deviation from route	Deviation from route	Deviation from route
PHA 77	Ship	Loss of propulsion	Navigational danger	Close - quarters	Close - quarter
PHA 78	Ship	Loss of propulsion	Speed decline	ETA deviation	ETA deviation
PHA 79	STCC	Deviation from route not observed	Close - quarters	Close - quarters	Close - quarter
PHA 80	STCC	Misconception of distances ship to ship	Close - quarters	Close - quarters	Close - quarter
PHA 81	STCC	None STM compliant ship	Congestion	Close - quarters	Close - quarter
PHA 82	STCC	No route updating between different Shore centres	Decline in flow optimisation	Inefficiency	ETA deviation
PHA 83	STCC	No route updating between different Shore centres	Decline in flow optimisation	ETA deviation	ETA deviation
PHA 84	STCC	Incorrect WP data in route	Deviation from route	Close - quarters	Close - quarter
PHA 85	STCC	Deviation from route not observed	ETA deviation	ETA deviation	ETA deviation
PHA 86	STCC	Incorrect WP data in route	Incorrect route	ETA deviation	ETA deviation
PHA 87	STCC	Route not adapted to ship parameters	Navigational danger	Collision	Collision

PHA 88	STCC	No visual or radar confirmation of changed route	No confirmation of changed route	Deviation from route	Deviation from route
PHA 89	STCC	Disagreement on route negotiation	Ship do not change route	ETA deviation	ETA deviation
PHA 90	STCC	Disagreement on route negotiation	Ship do not follow route	ETA deviation	ETA deviation
PHA 91	STCC	Workload -decision making	Stress	Poor decision making	Congestion
PHA 92	STCC	None STM compliant ship	Traffic perplexity	Close - quarters	Close - quarter
PHA 93	System	Route information disrupted intentionally	Congestion	Close - quarters	Close - quarter
PHA 94	System	Information overload	No route displayed	Traffic perplexity	Congestion
PHA 95	System	Route information disrupted intentionally	No route displayed	Navigational danger	Navigational danger
PHA 96	System	Constrained work area	Poor decision making	Navigational danger	Navigational danger
PHA 97	System	Ergonomic strain	Poor decision making	Navigational danger	Navigational danger
PHA 98	System	Important information hidden/ placed under sub functions	Poor decision making	Navigational danger	Navigational danger
PHA 99	System	Information expressed in foreign language or in unfamiliar terms	Poor decision making	Navigational danger	Navigational danger
PHA 100	System	Route information disrupted intentionally	Ship do not follow route	Close - quarters	Close - quarter

9.2 Preliminary Hazard Analysis

Number	Item	Top level accident	Hazards with potential to cause TLA	Cause	Effect	Mitigation/ recommendation
PHL 1	AIS	Close - quarter	AIS sends incorrect position	GPS error, Error in input settings e.g. geodetic datum	Collision	Back up and warning systems. Confirm position with all means
PHL 2	AIS	Collision	AIS sends incorrect position	GPS error, Error in input settings e.g. geodetic datum	Collision	Back up and warning systems. Confirm position with all means
PHL 3	AIS	Deviation from route	Wrong AIS information from other ship/STCC	Error in route transmission	Route negotiate error	Back up and warning systems. Confirm position with all means
PHL 4	AIS	Grounding	Wrong draught in Voyage specific data	Error in draught calculations or input	Ship may sail on route without acquired depth	Routines to confirm calculations and correct input to AIS
PHL 5	AIS	ETA deviation	AIS sends incorrect position to route	GPS error, Error in input settings e.g. geodetic datum	Ships position is wrong presented	Back up and warning systems. Confirm position with all means
PHL 6	AIS	Navigational danger	AIS sends incorrect position to route	GPS error, Error in input settings e.g. geodetic datum	Traffic perplexity	Back up and warning systems. Confirm position with all means
PHL 7	GPS	Grounding	Inaccurate position	Fault position sent to Navigational equipment and Route display	Grounding	Back up system, Confirm accurate position by all means

PHL 8	GPS	ETA deviation	Inaccurate position	Fault position sent to Navigational equipment and Route display	ETA delayed or miscalculated	Back up system, Confirm accurate position by all means
PHL 9	GPS	Navigational danger	Inaccurate position	Fault position sent to Navigational equipment and Route display	Fault navigation	Back up system, Confirm accurate position by all means
PHL 10	GPS	Close - quarter	Inaccurate position	Fault position sent to Navigational equipment and Route display	Safety distances not kept	Back up system, Confirm accurate position by all means
PHL 11	GPS	Deviation from route	Inaccurate position	Fault position sent to Navigational equipment and Route display	Wrong position displayed on route	Back up system, Confirm accurate position by all means
PHL 12	Interconnection	ETA deviation	No route exchange	Error in transfer of route data	Delayed or disrupted ETA	Back up system. Readiness to calculate ETA with other means
PHL 13	Interconnection	Close - quarters	No route exchange	Error in transfer of route data	Ship routes not presented on own display	Back up system. Use all means to position surrounding traffic
PHL 14	Interconnection	Collision	No route exchange	Error in transfer of route data	Ship routes not presented on own display	Back up system. Use all means to position surrounding traffic
PHL 15	Interconnection	Deviation from route	No route exchange	Error in transfer of route data	Traffic perplexity	Navigate on route with all navigational means
PHL 16	Nav. Equip.	Collision	Radar and ECDIS position deviates	Uncertainty of position on route	Uncertainty of correct position	Routine to ensure reliable ECDIS function
PHL 17	Nav. Equip.	Deviation from route	Radar and route position deviates	Fault radar settings	Uncertainty of correct position	Routine to ensure reliable Radar function

PHL 18	Nav. Equip.	Close - quarter	ARPA and route prediction deviates	Error in route display or radar	Uncertainty of forthcoming traffic situation	Routine to ensure reliable ARPA function
PHL 19	OOW	ETA deviation	Not sailing at recommended speed to keep ETA	OOW uses ship preferred speed	ETA will not be accomplished	Ships preferred ship must be calculated with in Flow optimisation
PHL 20	OOW	Grounding	Do not control depth for suggested route	Draught exceeds depth in route	Grounding	Establish routines to check suggested routes before acceptance
PHL 21	OOW	Navigational danger	System functions leads to extensive workload	To much information presented to OOW	Increased risk of faulty navigation	Highlight relevant information and hide irrelevant information
PHL 22	OOW	Close - quarter	OOW do not keep distance to ensure freedom of manoeuvrability	Routes look safe on display, not using all navigational means or regarding external factors like and current	Ship might come into dangerous distance to other ship or obstacle	Control that safety distances are kept with all navigational means
PHL 23	OOW	Deviation from route	Not joining route after evasive manoeuver	Manoeuvring for other ship or obstacle	Ship not following route	Route deviation must be displayed on all ships/shore centres
PHL 24	Route receiving and Route sending	Close - quarter	Route exchange not conducted	Equipment malfunction, Operational incapability	Route not displayed	Back up system, Sufficient training of operators
PHL 25	Route receiving and Route sending	Collision	Route exchange not conducted	Equipment malfunction, Operational incapability	Route not displayed	Back up system, Sufficient training of operators

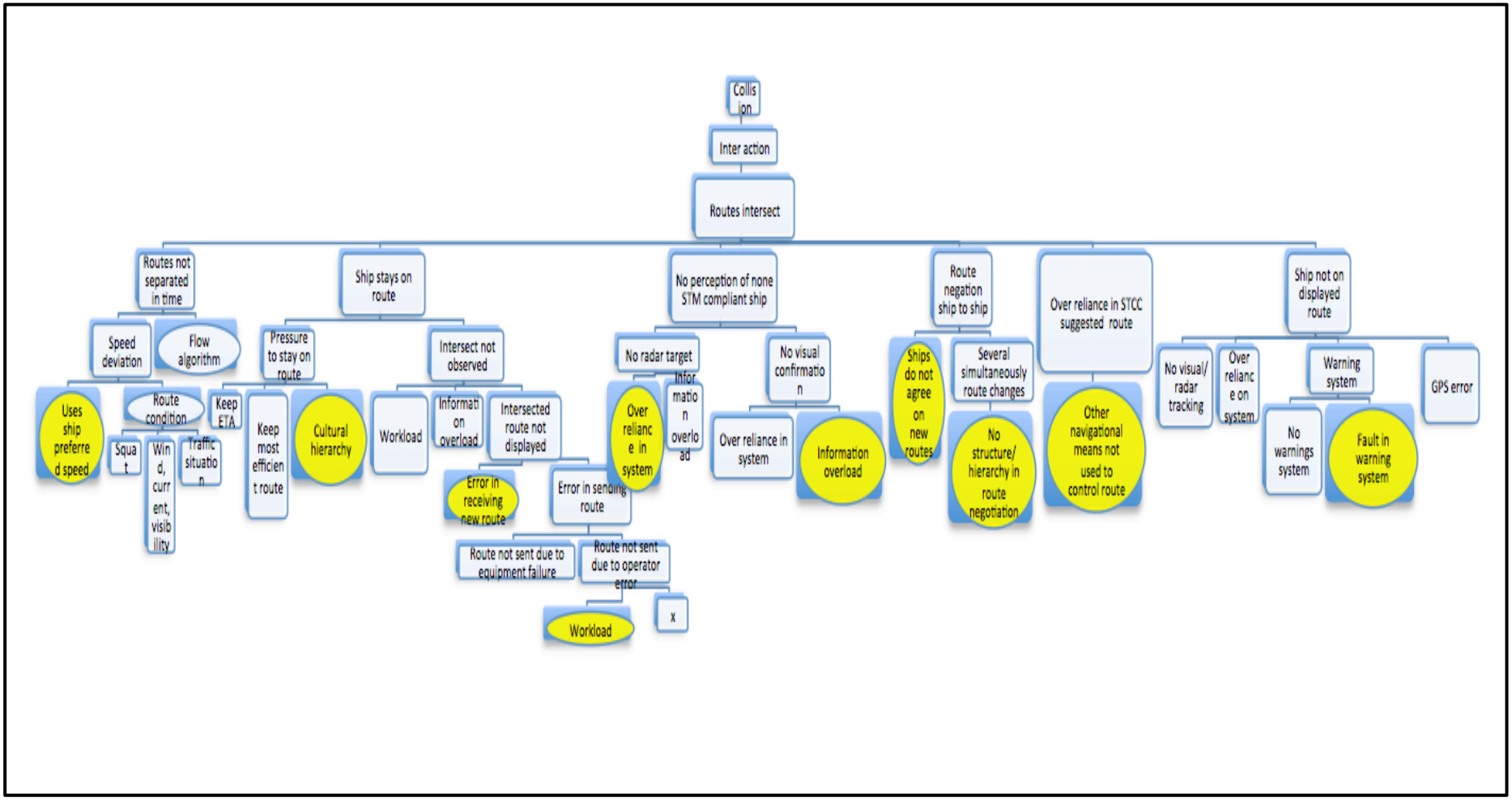
PHL 26	Route receiving and Route sending	Deviation from route	Route exchange not conducted	Equipment malfunction, Operational incapability	Route not displayed	Back up system, Sufficient training of operators
PHL 27	Route receiving and Route sending	ETA deviation	Route exchange not conducted	Equipment malfunction, Operational incapability	Route not displayed	Back up system, Sufficient training of operators
PHL 28	Route receiving and Route sending	Grounding	Route exchange not conducted	Equipment malfunction, Operational incapability	Route not displayed	Back up system, Sufficient training of operators
PHL 29	Route receiving and Route sending	Navigational danger	Route exchange not conducted	Equipment malfunction, Operational incapability	Route not displayed	Back up system, Sufficient training of operators
PHL 30	Ship	Close - quarter	Ship losses propulsion	Mechanical error.	Collision, grounding	Readiness to drop anchor in congested areas
PHL 31	Ship	Deviation from route	Rate of turn exceeds turns in route	Ships deviate rom route when altering course at WPs	Collision, grounding	Ship characteristics must be checked for all conditions
PHL 32	Ship	Grounding	Draught exceeds depth	Miscalculation of loading conditions	Route is to shallow for ship	Draught calculations must be coordinated with depth of route.
PHL 33	Ship	ETA deviation	External conditions hampers suggested speed	Wind, icing, current	Speed is reduced	Weather and other conditions must be calculated with when determining ETA

PHL 34	STCC	Grounding	Suggesting routes with not enough depth	Not regarding ship draught when distributing routes	Grounding	Routes must be cross checked
PHL 35	STCC	ETA deviation	Flow optimisation algorithm error	Fault in algorithm	Port calls delayed	Algorithm must be adjusted and performance monitored
PHL 36	STCC	Congestion	Flow optimisation algorithm error	Algorithm does not calculate with none STM compliant ships	Ship traffic will not flow	All ships STM compliant
PHL 37	STCC	Close - quarter	STCC suggests route with to small margins of navigational safety	In order of optimising traffic flow	Ships will come into unsafe distance	Routes must be separated according to relevant safety distances
PHL 38	STCC	Deviation from route	STCC does not observe ships deviating from routes	No alarm system, Error in flow algorithm	Traffic will not flow according to plan	Warning system and routine of checking route following
PHL 39	System	Deviation from route	System not configured to present ETA calculations	System does not present relevant information	Correct ETA not presented	System configured to requested task
PHL 40	System	Close - quarter	Information overload	Operator/OOW can not make proper decision based on the amount of information presented	Navigational danger	Suppress irrelevant information

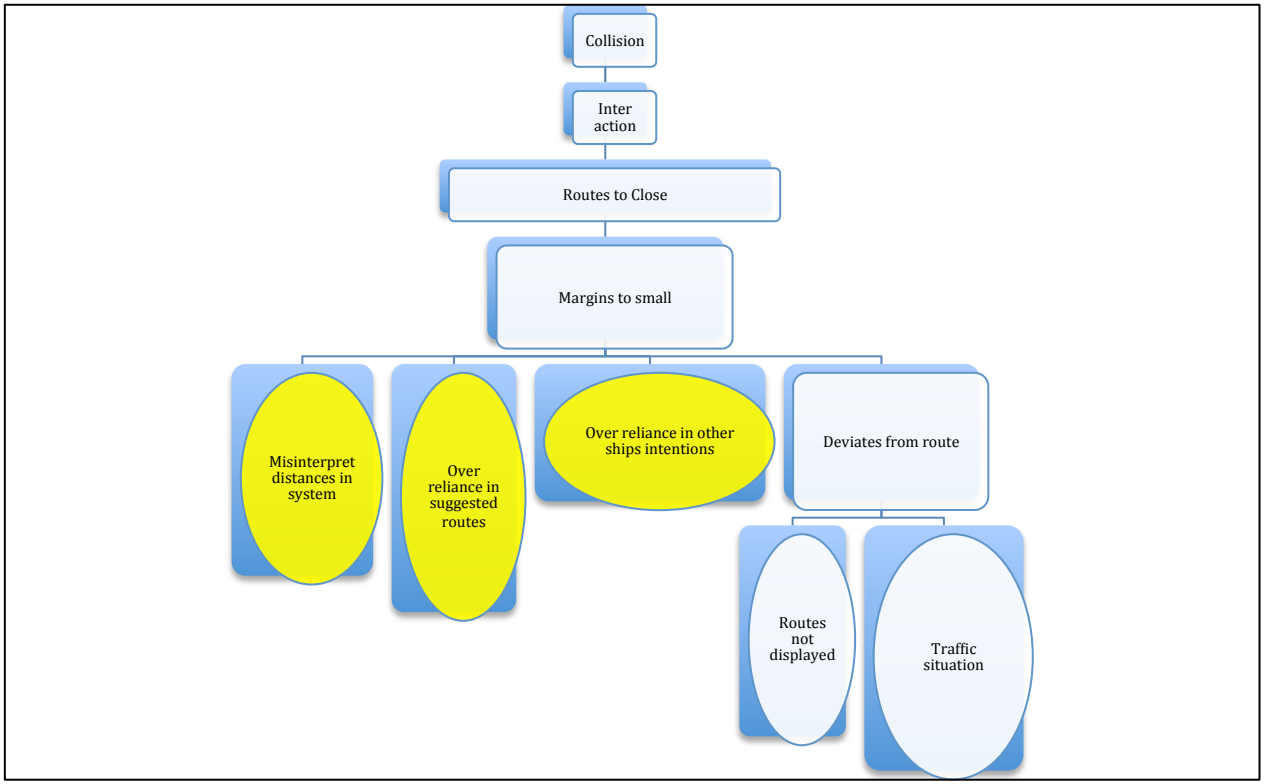
PHL 41	System	Collision	Workload	System is to complex to operate	Proper decision making is hampered	System design must enable efficient operating
PHL 42	System	Grounding	System parameters are incorrect	Incorrect ship parameters enter into system	Risk of grounding	Routine to control parameters and data entered into the system

9.3 Fault Tree Analysis -

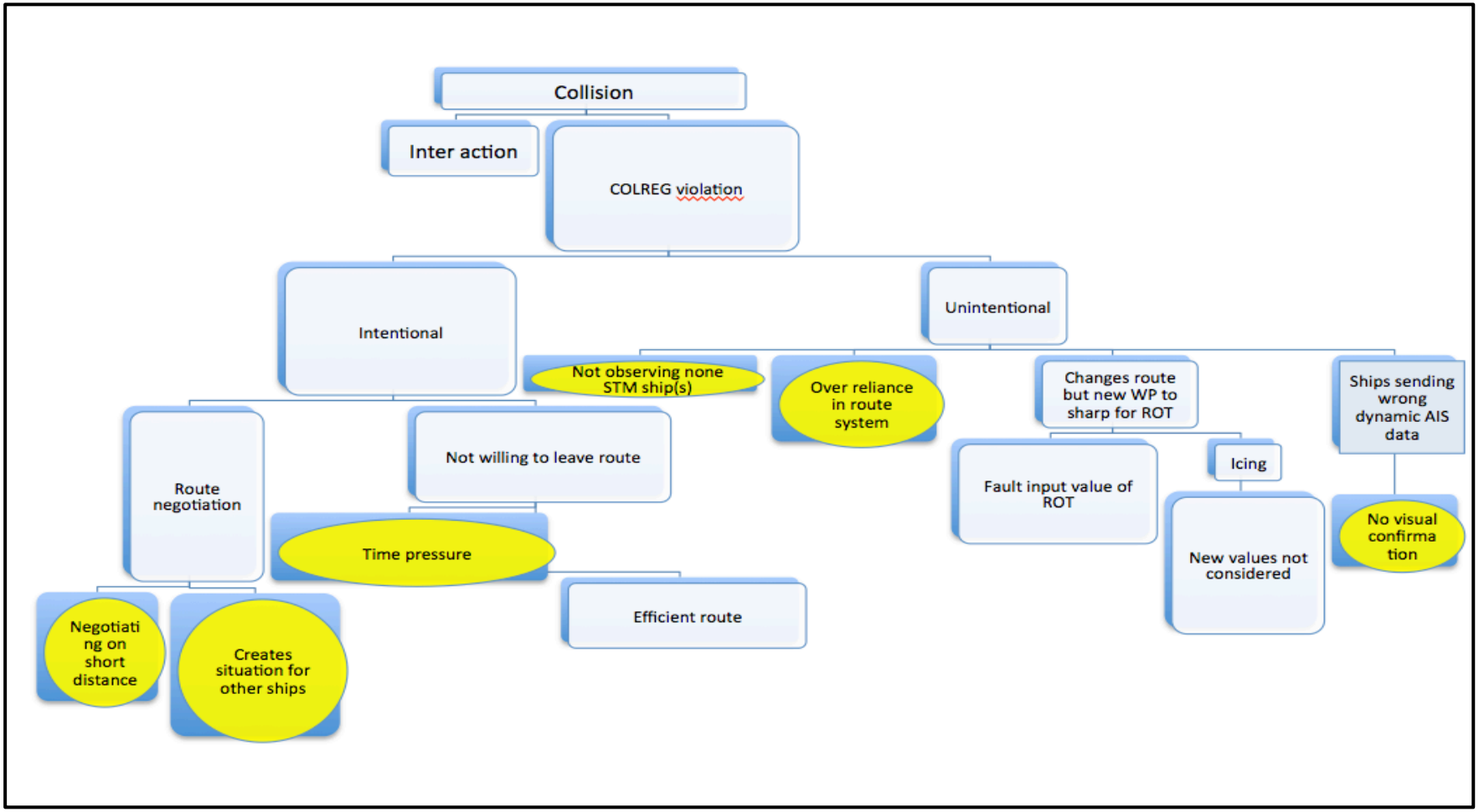
Fault Tree analysis - Collision- interaction – routes intersect



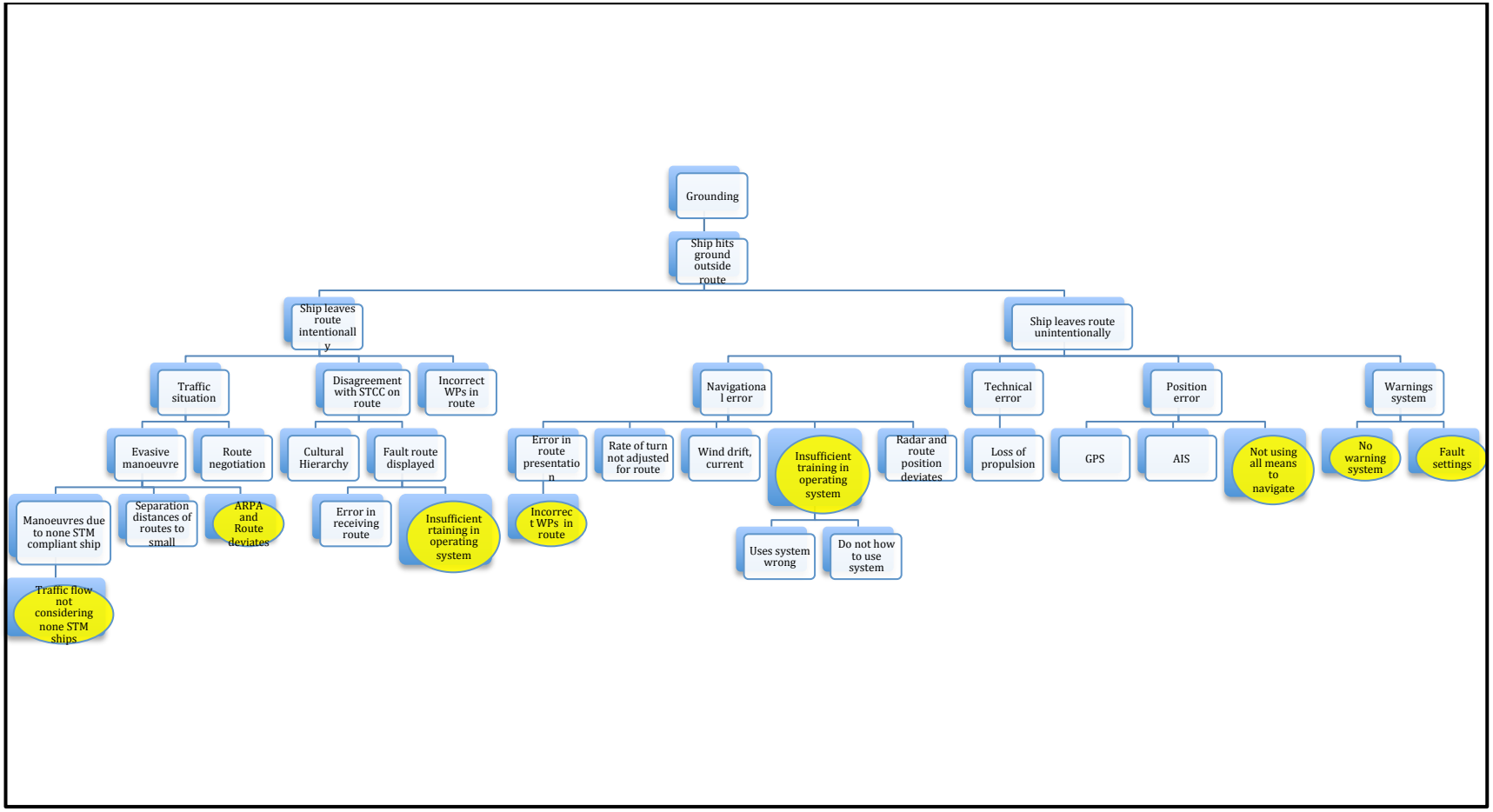
Fault Tree analysis - Collision- interaction – routes to close



Fault Tree Analysis - Collision – COLREG Violation



Fault Tree Analysis - Grounding ship hits ground outside route



Fault Tree Analysis - Grounding ship hits ground in route