

Methodology for Safety and Security Analysis

Deliverable D5.5 - Version Final – 2023-06-02



Advanced, Efficient and Green Intermodal Systems

<http://aegis.autonomous-ship.org/>



This project has received funding from the European Union's Horizon 2020 research and innovation program under Grant Agreement N° 859992.



Document information

Title	D5.5 Methodology for safety and security analysis
Classification	Public

Editors and main contributors	Company
Name (initials)	
Marianne Hagaseth (MH)	SINTEF Ocean
Per Håkon Meland (PHM)	SINTEF AS
Ørnulf Jan Rødseth (ØJR)	SINTEF Ocean
Egil Wille (EW)	SINTEF Ålesund
Dag Atle Nesheim (DAN)	SINTEF Ocean

Rev.	Who	Date	Comment
0.1	MH	2023.01.09	Document created
0.2	PHM	2023.05.12	Review version
0.3	SK	2023.05.16	Reviewed version
Final	MH	2023.06.02	Final revision to be submitted to EC

© 2020 AEGIS CONSORTIUM

This publication has been provided by members of the AEGIS consortium and is intended as input to the discussions on and development of new automated and autonomous waterborne transport systems. The content of the publication has been reviewed by the AEGIS participants but does not necessarily represent the views held or expressed by any individual member of the AEGIS consortium.

While the information contained in the document is believed to be accurate, AEGIS participants make no warranty of any kind with regard to this material including, but not limited to the implied warranties of merchantability and fitness for a particular purpose. None of AEGIS participants, their officers, employees, or agents shall be responsible, liable in negligence, or otherwise howsoever in respect of any inaccuracy or omission herein. Without derogating from the generality of the foregoing neither of AEGIS participants, their officers, employees or agents shall be liable for any direct, indirect, or consequential loss or damage caused by or arising from any information advice or inaccuracy or omission herein.

The material in this publication can be reproduced provided that a proper reference is made to the title of this publication and to the AEGIS project (<http://aegis.autonomous-ship.org/>).



Table of Contents

Executive Summary	4
Definitions and Abbreviations	6
1 Introduction.....	9
1.1 Scope	9
1.2 How this Work Covers AEGIS Specific Objectives	9
1.3 Main Scientific and Technical Contributions	10
1.4 Structure of the Document	10
2 Background Information	11
2.1 Autonomous Shipping Operations	11
2.2 Summary of Autonomy Concepts.....	11
2.3 Mission Phases, Ship Processes and Sub-Spaces of the OEnv.....	13
2.4 Risk Management in Shipping	16
2.4.1 Safety Risks	16
2.4.2 Cybersecurity Risks.....	17
3 Methodology Overview.....	19
4 Big Picture of Mission Example: Rotterdam-Ghent	21
5 Context	22
6 Actors	23
7 Ship Particulars and Processes	24
7.1 Ship Processes	25
8 Mission Phases and Mission Phase Patterns.....	27
8.1 Description of Mission Phases.....	27
8.2 Description of Mission Phase Patterns.....	31
9 System Control Tasks	38
9.1 Parametrization of Operational Envelope, SCT and State Variables.....	38
10 UML Diagrams	41
10.1 Introduction.....	41
10.2 UML Model Structure in Enterprise Architecture	42
10.3 UML Top-Level Use Case Diagram for IWW Scenario	44
10.4 UML Top-Level Activity Diagram for IWW Scenario.....	45
10.4.1 Next Level UML Activity Diagrams	46
10.4.2 UML Diagrams for some SCTs.....	49



- 10.5 Diagram Components..... 55
 - 10.5.1 UML Activity Diagram Components 55
 - 10.5.2 UML Collaboration Diagram Components 57
 - 10.5.3 UML Sequence Diagram Components..... 61
- 11 Safety and Security Analysis..... 65
 - 11.1 Exploring potential hazards..... 65
 - 11.2 Top-level Misuse Case 68
 - 11.3 Mission Phase Pattern Threats..... 68
 - 11.3.1 Approaching Lock 69
 - 11.3.2 Approaching Bridge 69
 - 11.3.3 Passing Bridge..... 70
 - 11.3.4 Passing Lock Chamber 71
 - 11.3.5 Complex IWW Sailing 71
 - 11.3.6 Simple IWW Sailing..... 74
 - 11.3.7 Cargo Operation in Terminal 75
 - 11.3.8 Cargo Operation outside Main Terminals (foreseen)..... 75
 - 11.3.9 Deberthing/Berthing 75
 - 11.3.10 Port Departure/Arrival 76
 - 11.4 Likelihood Estimations..... 76
 - 11.5 Overall Result of the Analysis 82
- 12 Discussion and Conclusions..... 85
- References..... 86

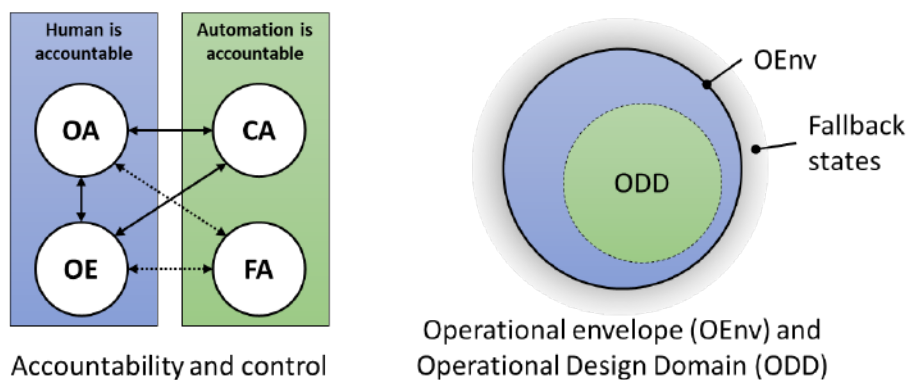


Executive Summary

This document describes a safety and security analysis method based on the work done in the Seatonomy project, the Autoship project, and previous work done in AEGIS WP5. The work is documented in the modelling tool Enterprise Architect.

This deliverable has four parts:

First, we give a summary of concepts used regarding the description of autonomous shipping operations, the handover between humans and automation in a maritime autonomous ship system, and the methodology that we have used in this work. The most important point here is the definition of the cooperation between autonomy and human, as shown in the following, where FA (Fully Autonomous) means that the autonomous system is approved for operation without any human intervention, while CA (Constrained Autonomy) means that the automation is accountable and will also notify the human in time for him to get situational awareness, do some action and for the ship to react. During OA (Operator and Automation) and OE (Operator Exclusive), the human is accountable but get assistance from the automation or the automation can control the system within certain limits.



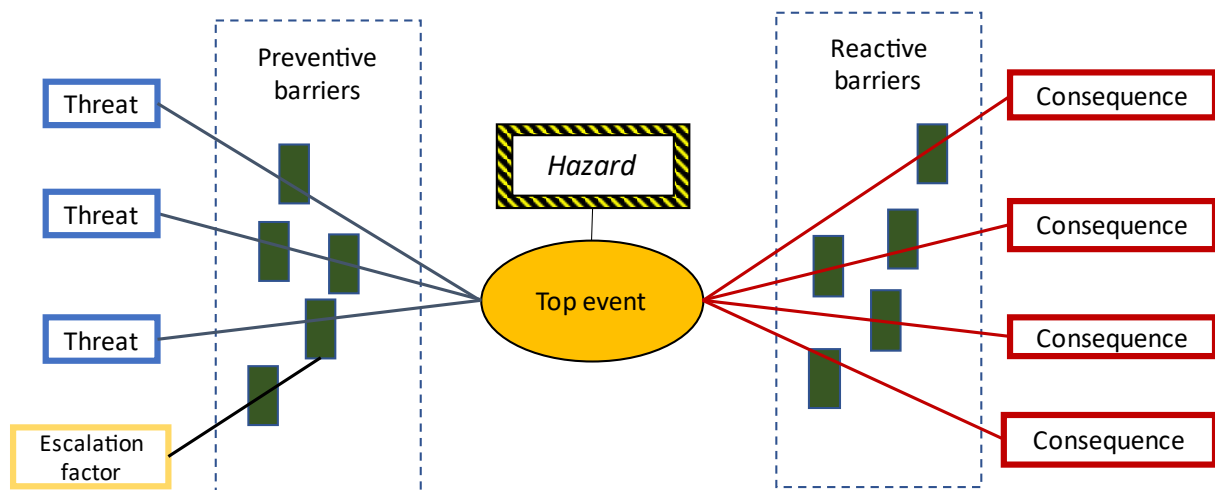
Secondly, the inland water way case covering sailing from Rotterdam to Ghent is described regarding the big picture, context, actors, ship particulars and processes, mission phases and mission phase patters, and also the System Control Tasks (SCTs). The reason why we selected this use case, is that it showcases several aspects that are important when describing the operation of an IWW barge, as for instance:

- This is an inland waterway route passing through a number of locks and bridges.
- The route goes from one country to another (Netherlands - Belgium).
- The waterways have varying degrees of traffic that requires manoeuvring in a narrow space. This includes leisure boats of varying sizes.
- Blocking or congestions may introduce serious delays to the other vessels and ports, as well as hinterland operations.
- The barges operating along these routes are heavy and slow-moving.
- The terminals will have reserved space for RoRo barges, extending the autonomous operations to landside operations.
- It is easy for a threat agent to be in the physical vicinity of the vessels even from ashore. The same applies for the landside infrastructure.



Part three consists of a set of UML diagrams describing some of the SCTs to give examples of how the methodology is used. During this work, we found it useful to define a set of UML components covering some activity diagrams, collaboration diagrams and sequence diagrams that can be reused when setting up the UML diagrams for System Control Tasks. Reuse of UML diagrams is useful since several of the System Control Tasks are similar. Also, the UML diagrams, especially the one for the sequences, are useful when doing safety and security analysis.

The last part covers the safety and security analysis, where we focus on finding critical situations where cyber-attacks threaten the different modes of autonomous operations, especially related to the interplay between the automation and human operators. The threat and consequence analysis is done according to the bow-tie methodology as shown in the following:



Further, the various attacks are modelled using the UML Diagrams and misuse case diagrams. The purpose of using UML diagrams for the analysis is to support the design of operational envelopes that can tackle situations out of the ordinary. The goal is that the analysis will reduce the frequency of resource demanding fallbacks and safety incidents. The methodology is particularly useful when analysing autonomous ship systems at an early concept stage where implementation details are still undecided. This also means that the risk assessment should be continuously updated along with the progress of the design, the technological development and decisions, and the changing threats in the operating environment.



Definitions and Abbreviations

Definitions are primarily taken from ISO/TS 23860 [1] and secondarily from deliverable D3.1 from the AUTOSHIP project [2]. Other references are also used and marked appropriately in the text.

Accountability: The responsibility for carrying out a control function. This can be performed by an automation system or a human, but only one party should be accountable at any time.

Accountable: The party that is responsible for executing safe and efficient control over the ship system. This will be a human onboard or in the RCC, or the automation system. This is included in the SCT description.

AEGIS Use Case A: The Trondheimsfjord case from WP8 was used as an example of how the CONOPS methodology can be applied in Deliverable D5.3

AEGIS Use Case B: The IWW case from WP9 is used as an example of how the methodology can be applied in this deliverable.

AEGIS Use Case C: Increased automation of cargo handling is also a relevant scenario to apply this methodology on, however, this is not covered in the current deliverable.

AGV: Automated Guided Vehicle.

AOC: Autonomous Onboard Controller [1].

Automatic: Process or equipment that, under specified conditions, can function without human control [1].

Autonomous controller: This is a control function that, under certain circumstances, are allowed to make operational decisions without human confirmation (see definition of autonomy in [1]).

Autonomy: One or more of a ship system's processes or equipment, under certain conditions, is designed and verified to be controlled by automation, without human assistance [1].

CONOPS: Concept of Operation. This is a document describing the characteristics of a proposed system from the viewpoint of an individual who will use that system. This is a mostly prose type description commonly used as part of the required documentation for approval of autonomous ship systems.

Context: This is the description of actors that are outside the autonomous ship system, that the ship system needs to interact with.

FSA: Formal Safety Assessment.

GNSS: Global Navigation Satellite System, a collective term for satellite navigation systems such as Galileo, GPS, GLONASS and BeiDou.

HAI: Human-Automation Interface.

IMO: International Maritime Organization

ISM: International Safety Management (ISM Code by IMO)

ISPS: International Ship and Port facility Security (code). Now in SOLAS Ch. XI.

MASS: Maritime Autonomous Surface Ship, a ship which can operate intermittently or continuously without human interaction. Can also be used to mean: Maritime Autonomous Ship System.



Mission: This is the description of the overall operation that the autonomous ship system performs, typically with a limitation, e.g., to the ship itself and its direct interfaces.

Mission phase: These are distinct parts of the mission that can be characterized by being delimited by specific operational and environmental parameter values. Some possible phases would be cargo loading and discharge, berth departure, port departure, and normal sailing.

Mission phase pattern: This is a generalization of one or more mission phases into one common operational pattern. Typically, normal sailing will be divided into several legs where the geographic location, course and/or speed will be different between the legs. However, if geographic location, course, and speed are generalized into categories or characterized by less specific parameters, collections of several legs can normally be described by one single mission phase pattern.

MSC: Maritime Safety Committee (in IMO)

O: Operational envelope state space.

Operational envelope (OEnv): The conditions and related operator control modes under which an autonomous ship system is designed to operate, including all tolerable events ([1]).

Process/Ship Process: The autonomous ship system requires many more or less independent processes to function. Some examples can be navigation, power generation, stability and ballasting, fire protection etc. Annex A of [2] contains a longer and more complete list of ship processes broken down to two or three sub-levels.

RCC: Remote Control Centre, site remote from the ship that can control some or all of the autonomous ship system processes [1].

RCO: Risk Control Option.

RoRo: Roll-on/Roll-off. Type of cargo/operation where cargo units (e.g. containers) are loaded and unloaded on wheels.

System Control Task (SCT): The specific implementation of the control of one or more processes in one or more mission phase patterns is called a SCT [1].

System components and actors: This is the identification of the actors (human, automation, or physical infrastructure) that need to be incorporated into the description of how the autonomous ship system is controlled.

State variable: This is a parameter that is part of the characterization of a mission phase or a use case. This can be external, e.g., wind direction and strength, a dynamic property of the ship, e.g., speed or course, or a more static property of the ship, e.g., loading condition or technical status.

$U_{i,j}$: State space for SCT(i,j) where i is the process number and j is the sequence number for the SCT.

UML: Unified modelling language [3].

UML Diagram: A diagram written using UML to describe structural or behavioural information. Several different types of UML diagrams exist, for instance use case diagram, activity diagram, sequence diagram, state diagram, collaboration diagram and class diagram.

UML Description of SCT (System Control Task): The description of a SCT, that is, how one or more ship processes is implemented in one or more mission phase patterns, can be described by use of UML. An SCT is then described by a set of UML diagrams of different types, for instance, UML activity diagrams,



UML state diagrams, UML sequence diagrams, UML collaboration diagrams, UML class diagrams, and UML use case diagrams. As an example, an overall UML use case diagram for a SCT can be used to describe central actors and their main activities. Each SCT may also span over several mission phase patterns.

VTS: Vessel Traffic Service



1 Introduction

1.1 Scope

This report describes a refinement and further development of the safety and security analysis method described in deliverable D5.3 *Safety and security analysis and remedial measures* [4]. Similar to D5.3, the method described in this report employs UML diagrams to describe the target system and mission, and this is based on methods described in the AUTOSHIP project [2], [5] and Seatonomy [6], [7].

While D5.3 used the daughter vessels of AEGIS Use Case A as a basis for its analysis, this report will illustrate the refined methodology by applying it to an example mission based on AEGIS Use Case B, specifically a RoRo barge route between Rotterdam and Ghent. Based on this example mission, a set of System Control Tasks and Mission Phases have been defined, and these are subject to a generic safety and security analysis where activities, threats and risks are described and assessed with the help of various UML diagrams. The analysis is not exhaustive, but rather an example of how the methodology can be used.

1.2 How this Work Covers AEGIS Specific Objectives

The AEGIS project has specific objectives (SO) as described in Table 1. This report is mainly relevant to SO2 covering resilience, safety and cyber security in highly physically and digitally integrated transport systems. However, it also identifies and highlights limitations and considerations which are relevant to the other specific objectives, with some examples below:

- SO1: One of the likely purposes and goals for a cyberattack is business disruption, which can be achieved e.g. by attacking autonomous systems and causing blockage of a high-traffic waterway. This would also lead to increased emissions, pollution and noise, which negatively impacts the fulfilment of SO1.
- SO3: There are various ways to deteriorate timeliness and frequency of shipments through cyberattacks, e.g. by disrupting cargo operations while the autonomous vessel is in a terminal (as described in 11.3.7).
- SO4, SO5, SO6: This is relevant as the methodology can be used to analysis autonomous ship systems which utilizes small terminals outside of large terminals to reduce the length of the last mile.

Table 1: Specific Objectives (SO) in AEGIS

SO	AEGIS Specific Objectives
SO1	Minimum GHG emissions, pollution and noise from ship transport and terminals: Green transport.
SO2	Resilience, safety and cyber security in highly physically and digitally integrated transport systems: Robust transport systems.
SO3	More flexible ship transport by combining smaller and automatic lightweight shuttle vessels with faster medium to long distance ships: Higher speed, timeliness and frequency.
SO4	Transport to smaller quays and ports, also outside ISPS areas: Rural connectivity.
SO5	Automated short distance transport from terminals to end users where possible: Last mile automation.
SO6	Enabling ship transport into city centres with no terminal storage space by using small lightweight automated shuttle vessels and just in time arrival: Urban connectivity.
SO7	Improved access to waterborne transport for all transport users, minimum administrative hassle, more efficient security controls: User-centered services.



1.3 Main Scientific and Technical Contributions

This report documents work performed in Task 5.4 in the AEGIS project. The main contributions from this work are:

1. Improvements in the overall description of autonomous ship systems in an operational envelope.
2. Further developments and example cases of the UML methodology based on the work reported in D5.3.
3. A method for determining the likelihood of hostile attacks on the system.
4. A joint consolidation of safety and security considerations
5. Description of Diagram Components in Enterprise Architect that can be reused when setting up activity diagrams, collaboration diagrams and sequence diagrams for other scenarios.

1.4 Structure of the Document

This deliverable is structured as follows:

- Chapter 2 describes the concepts we use related to autonomous ship systems, operational envelopes and the different levels of autonomy.
- Chapter 3 gives an overview of the methodology, that is, how the descriptions of the Context, Actors, Ship particulars, Ship processes, Mission phases, Mission phase patterns and System Control Tasks (SCTs) relate to various UML diagrams.
- Chapter 4 gives the overview of the inland water ways (IWW) scenario from Rotterdam to Ghent.
- Chapter 5 describes the context of the scenario
- Chapter 6 describes the actors of the scenario
- Chapter 7 describes the ship particulars and the ship processes
- Chapter 8 describes the mission phases and generalizes these to mission phases patterns for the IWW scenario from Rotterdam to Ghent.
- Chapter 9 describes the System Control Tasks (SCTs) that are needed to describe the relevant mission phase patterns.
- Chapter 10 describes the UML activity, collaboration and sequence diagrams for some of the activities and SCTs in the IWW scenario. It also describes some reusable diagram components that can be used as building blocks for setting up similar activity diagrams, collaboration diagrams and sequence diagrams.
- Chapter 11 contains the safety and security analysis including bow-tie diagrams.
- Chapter 12 concludes the deliverable with some discussions on the results.



2 Background Information

2.1 Autonomous Shipping Operations

Ever since the MUNIN project [8] started in 2012, the international interest in autonomous shipping has been growing, and the *International Maritime Organization* (IMO) is currently working on a new code for autonomous ships in international trade with a target completion year of 2025 [9]. The realization of an autonomous ship system can take many forms and the community has not even agreed on a common definition of a *Maritime Autonomous Surface Ship* (MASS) [9]. However, it is understood that autonomous ships differ from other autonomous vehicles such as cars or aerial vehicles in many ways. Ships are much more costly, move more slowly, and operates in environments that generally have fewer obstacles than cars [10]. This also provides opportunities: Ships are costly enough to make the use of remote supervision and intervention cost effective compared to developing full autonomy for the ships. A fully uncrewed ship sails with an *autonomous onboard controller* (AOC) that can operate the ship without human assistance most of the time, while a manned *Remote Control Centre* (RCC) will intervene at the request of the AOC to handle situations beyond the AOC's capabilities [11]. This requires that the AOC can issue warnings in time for the operator to gain sufficient situational awareness to take safe actions.

Autonomy will also create new possibilities for cyber-attacks as coordination between AOC and crew becomes critical. Thus, the hand-over of control between human and automation via a communication link becomes important. There can also be cases where the crew fails to take over control after an alert from the AOC. If the general rule is just stopping the ship in all cases of communication loss, simple jamming of the communication link can effectively stop the ship from doing anything useful.

2.2 Summary of Autonomy Concepts

There are many different definitions of autonomy and levels of autonomy [12], but in this document we will use a simplified definition taken from [13] which is the same as that given in ISO/TS 23860 [1]:

“In the context of ships, autonomy means that one or more of a ship system's processes or equipment, under certain conditions, is designed and verified to be controlled by automation, without human assistance” . This definition uses the term *control* which can be understood as having the full responsibility for safe operation of the processes or equipment. This in turn implies that the responsibility of *control* can reside either with the human in the RCC or on the ship, or with the automation. Furthermore, this also implies that when the automation has control, the human is relieved, and can do other things than monitoring or operating the ship. This understanding of control can also be expressed as the concept of *accountability* [14], i.e. what party is at any particular point in time responsible for monitoring and doing necessary interventions to safely operate the equipment or the process.

As the definition of autonomy also states *“under certain conditions”*, it should be clear that the accountability may change between human and automation, dependent on the conditions. For a ship, this may mean that the automation is fully capable of controlling the navigation in open sea and calm weather, but that human assistance is required, e.g., in port approaches and during berthing. In addition, we assume that most autonomous ship systems will be designed with the possibility for continuous monitoring from an RCC and with the possibility for operator to intervene, even when automation is fully capable of controlling the ship. This can be illustrated as in Figure 1.

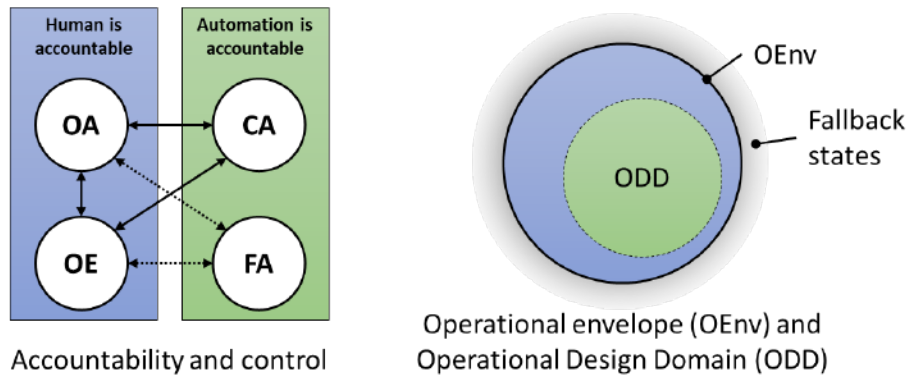


Figure 1: Autonomy and human cooperation

Here, we introduce several concepts that will be referred to in this document (figure to the right):

- **Operational Envelope (OEnv):** This is the overall capabilities of the system, including both automation and human. This can be seen as a state space over, e.g. weather, traffic conditions, ship state etc [15].
- **Operational Design Domain (ODD):** This term is taken from SAE J3016 [16] and represents the part of the OEnv where the automation is capable of controlling the system, i.e. may be accountable. Following the ODD taxonomy of PAS 1883:2020 [17], the ODD shall be classified into the top level attributes; *a) scenery* (non-movable elements of the operating environment), *b) environmental conditions* (weather, atmospheric conditions, connectivity), and *c) dynamic elements* (movable elements of the ODD, e.g. traffic or subject).
- **Fallback states:** This is a collection of "designed states" outside the OEnv that can be entered through a fallback function when the OEnv is in some way exceeded. These states are outside the OEnv but should still represent a tolerable risk for the system and its environment. Fallback states are defined during the design of the system and is, thus, "designed".

One should keep in mind that "the system", as used here, most often represents a sub-set of the full autonomous ship system capabilities, e.g., energy production, stability, fire protection or navigation. While the OEnv should be what the full ship system is able to operate in, the ODD will normally be dependent on the specific function that is discussed. This is discussed in section 2.3.

With the above definitions, we can define four main operational modes or classes of autonomous operation that are indicated to the left in the figure:

- **Fully autonomous (FA):** A fully autonomous system that is approved for operation completely without operators within the OEnv. Operators may still monitor or intervene in the system, but they should not be required to do so (dashed arrow). This means that OEnv is the same as ODD. The automation can be accountable in the full OEnv.
- **Constrained Autonomy (CA):** The automation can safely control the systems within the specified ODD. In addition, to allow accountability for the automation, the automation must be able to detect when human control will be needed, and to warn the operator sufficiently before control is transferred to allow the operator to gain the necessary level of situational awareness to safely handle the situation. This allows the operator to do other things than monitoring the system, until the automation issues an alert to take over control. This also allows the automation to be accountable in the ODD.



- **Operator and automation (OA):** The automation can control the systems within certain constraints, but it is not possible for the automation to detect early enough the need for control transfer. This may be because the ODD is not fully known or because the transition out of ODD is too fast to alert the operator in time. This means that the operator can leave control to automation, but he or she must continuously supervise the system to take over control on short notice. The operator is accountable.
- **Operator exclusive (OE):** Automation may still give some assistance, e.g., through autopilot control rather than direct thruster and rudder control, but the operator needs to be continuously in control of the system. The operator is accountable.

Transitions are indicated by arrows. Note that with the above definitions, all transitions will be initiated by the human operator. Fallbacks will be activated by the automation system when a human fails to respond to a critical situation fast enough or as a last resort emergency shutdown. Normally, a human operator is needed to restore the ship system to normal operation after a fallback. This means that even fully autonomous ships may need some form of RCC.

2.3 Mission Phases, Ship Processes and Sub-Spaces of the OEnv

Mission phases and ship processes were originally defined in deliverable D3.1 *Design standards* from the AUTOSHIP project [2]. A brief definition of the concepts is summarised below.

Different part of a ship's mission or voyage will require different performance from the ship systems. Thus, it is useful to define **mission phases** that can be used in analysis of the system. An example of some possible mission phases related to ship departure from port is illustrated in Figure 2. At the end of the sequence, one will have similar phases, but as arrival instead of departure.

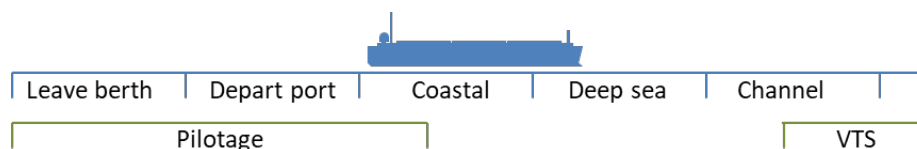


Figure 2: Example of mission phases

The figure also illustrates that there may be different external constraints that sub-divide the mission phases differently, e.g., related to pilotage or VTS communication requirements. In addition to geographically constrained definitions of mission phases, one may also need to consider weather, visibility and other non-geographic parameters.

The degree of autonomy will vary between the different operations and functions a ship system performs. One may, e.g., expect that energy production may be more automated than navigation. Figure 3 shows three groups of operations, each with a number of distinct functions associated with them. The figure divides the functions into operations that are performed on the ship, those related to ports, and those related to ship management. The latter will as example include shore-based ISPS and ISM management. An example of a possible three-level breakdown of operations is included in Annex A of AUTOSHIP Deliverable D3.1.

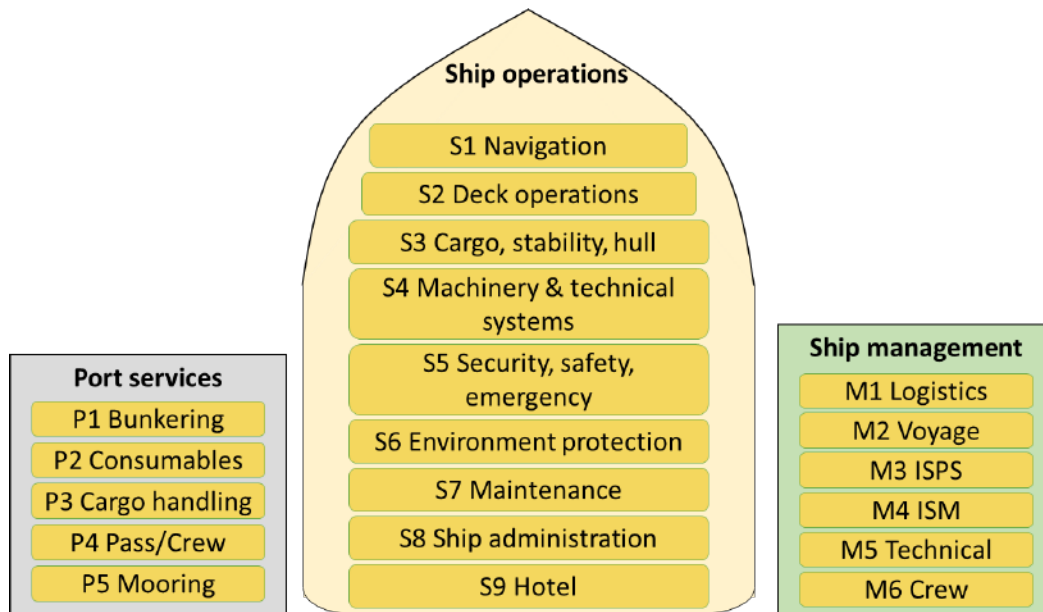


Figure 3: Main functional breakdown [Source: AUTOSHIP]

The AUTOSHIP example creates a tree-structured breakdown for all **processes** in the system. There are also other ways to do this and other ways to decompose the individual elements into lower-level primitives. However, a sub-set of the AUTOSHIP structure is illustrated in Figure 4.

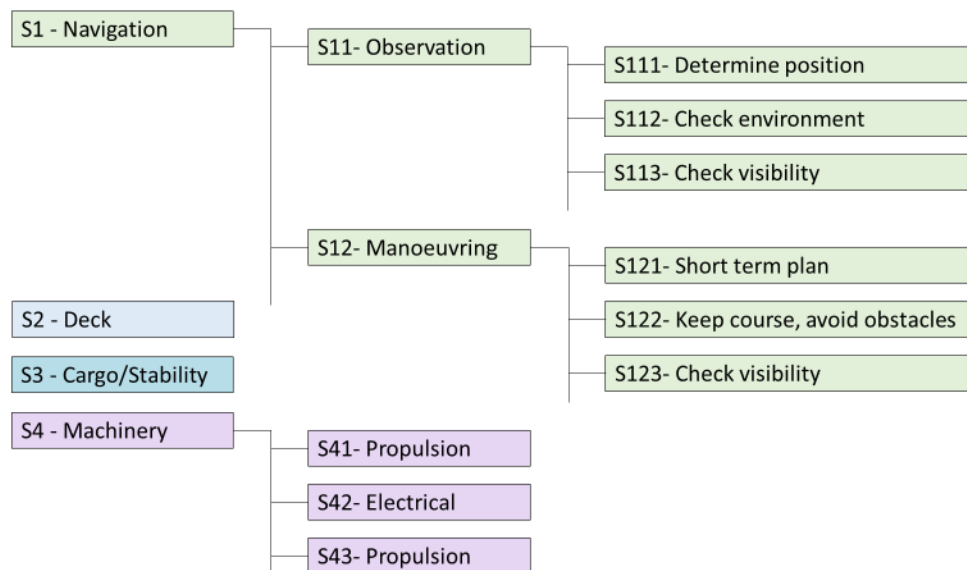


Figure 4: A small sub-set of the AUTOSHIP breakdown

The **operational envelope** is defined as “conditions and related operator control modes under which an autonomous ship system is designed to operate, including all tolerable events” [1]. Thus, the operational envelope must capture the system objectives and the constraints under which these should be reached, while also describing the division of responsibilities between human operators and automation. The operational envelope will form a state space where dimensions may be environmental factors (geography, visibility), operational conditions such as traffic density, ship state such as engine and propeller condition and so on. This state space is in the following denoted \mathcal{O} . The operation envelope is further divided into several "sub-envelopes", mainly based on:



- *Mission phases:* These define the temporal perspective of the system objectives. Different complexity of functionality and automation will normally be required in different phases of the mission. As an example, automated sailing on high seas is normally “easier” than in congested fairways close to shore or on inland waterways (fjords, rivers or canals).
- *Processes:* The different ship processes may have different degrees of automation in one mission phase. As an example, the ship engine and other technical systems are already approved for continuous unattended operation on many ships while navigation is still a process mainly performed by humans.

This is illustrated in Figure 5 where a selection of mission phases and processes have been put into a matrix and colour coded to show different parts of the operational envelope: The darker the colour, the more complex the operation. This is only an example, but it illustrates how O can be divided into different regions, here from O_1 to O_9 .

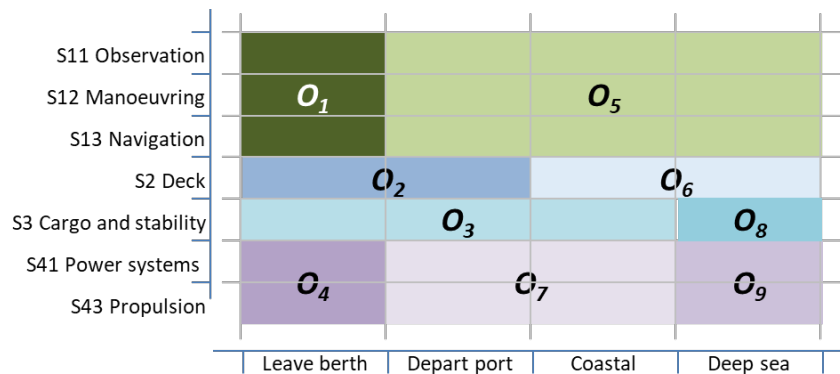


Figure 5: Examples of sub-envelopes

The example shows a subdivision according to the following main principles:

- Navigation, observation and manoeuvring are closely connected, and requirements will differ quite substantially during the voyage, with complexity (darker colour) mostly associated with nearness to other objects and geographic features (O_1 and O_5).
- Deck operations will be important close to port where mooring, tug assistance and pilot disembarkation may have to be handled. During normal passage, these operations are rarely needed (O_2 and O_6).
- Cargo and stability functions are about the same when the ship is sailing. There may be some additional complexity related to severe sea states in the deep-sea phase (O_3 and O_8).
- Power generation and propulsion are also closely linked and are mostly independent of voyage phase, except during approaching or leaving berth (O_4), where complexity may be higher. Also, in deep sea, adverse weather may increase complexity of operations (O_9).

The distinction between O_3 and O_8 as well as between O_7 and O_9 is intentionally exaggerated. One can normally merge these states and just add another state parameter representing the sea state.

In each of the sub-spaces one or more processes have been combined with one or more mission phases to form a state space where the same set of processes are performed under similar conditions. This is called a **system control task (SCT)** and is the basis for the transition from a textual description of the ships operation to UML (further described in Chapter 3).



2.4 Risk Management in Shipping

Risk can generally be defined as the product of the assumed occurrence frequency or likelihood and the impact or consequence of hazardous incidents. In this document we will differentiate between safety and security risks. Generally, both types of risk are caused by the same types of hazardous incidents, but there is a significant difference in the likelihood as will be discussed in the following.

2.4.1 Safety Risks

In the shipping industry one has traditionally considered risk as the product of the hazard incident's consequence and its occurrence frequency [18]. When consequence and frequency are plotted in a log-log axis system, one will typically get a diagram as shown in Figure 6.

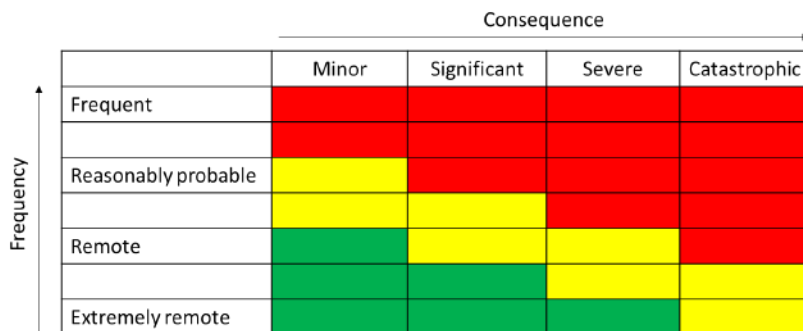


Figure 6: Example of risk diagram

Here, the cells are color-coded according to the general assessment of risk:

- **Green:** Generally acceptable risk, no risk-reduction measures are needed.
- **Yellow:** As Low As Reasonably Practicable (ALARP), risk should be reduced as much as is practically possible. Normally, this includes some form of cost-benefit analysis of the risk reduction measures.
- **Red:** Unacceptable risk. Risk-reduction is required.

The diagram in Figure 6 is generalized, and the actual classification into categories and exactly how to calculate the risk varies. Even for conventional shipping, the frequency is difficult to estimate, particularly for special ships with small crews or new hazards that have little statistical data. In this case one may use, e.g., Delphi methods or Bayesian belief networks. These and several other methods are suggested in the FSA guidelines [18].

The FSA guidelines are quantitative in their approach and put much emphasis on the ALARP region and the cost-effectiveness of various risk control options. If the risk estimates are very uncertain, this may not be possible. In such cases one may need other approaches, e.g., based on qualitative assessment of risk control options. This can be based on a bow-tie diagram as shown in Figure 7. In this variant, a *hazard* is something with a potential to cause harm, but also being necessary for performing the operation. The *top event* is an unwanted event that represents what will happen if one loses control over a hazard. The top event can have one or multiple causes denoted as *threats*, and one or more possible *consequences*. We have two types of *barriers*, *preventive* which aim to interrupt causes of top events, and *reactive* that makes it possible to react or recover from the top event without causing severe consequences. An *escalation factor* is anything that may cause a barrier to fail, and it is also possible to add barriers to these. An overview of the development of bow-ties is presented by Aust



and Pons [19], who also point out there is no standard way of doing this, and variations of this structure occur.

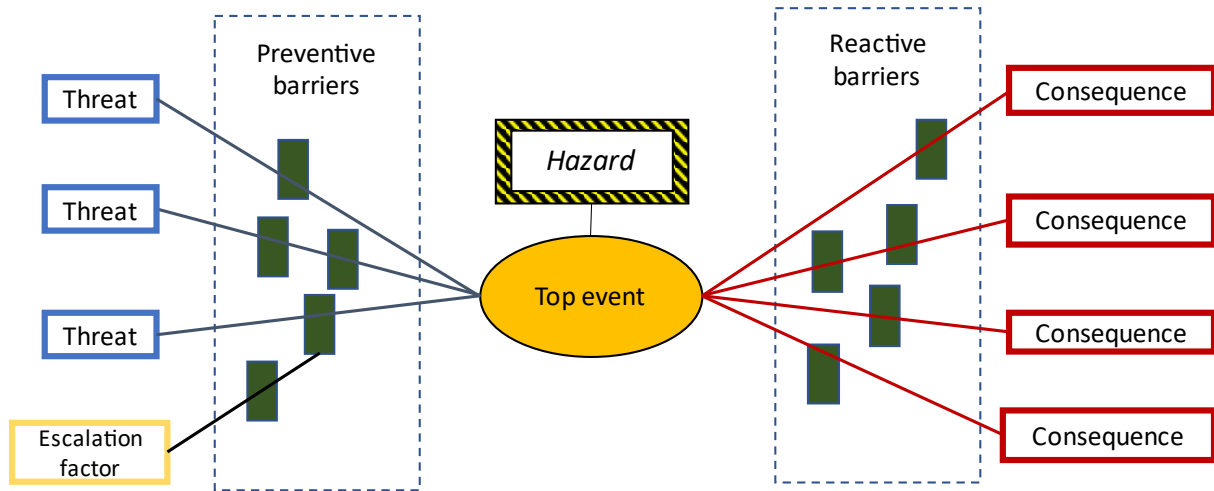


Figure 7: Typical structure of a bow-tie diagram

Another alternative to quantitative assessments is to first do a qualitative assessment of all risks and classify them as either acceptable or unacceptable, based on the nature of the consequence and a qualitative estimate of probability. An example of a possible classification is illustrated as in Figure 8.

		Consequence			
		Minor	Significant	Severe	Catastrophic
Frequency	Frequent				
	Reasonably probable				
	Remote				
	Extremely remote				
	Extremely remote				

Figure 8: Qualitative risk assessment

For all unacceptable risks, one can then use, e.g., a bow-tie approach to assess if there are sufficient barriers in place to avoid the consequence. Again, the assessment must be qualitative.

2.4.2 Cybersecurity Risks

Though the shipping industry has had a long tradition of considering risks from a safety perspective, the cyber security elements are often insufficiently considered [20]. One can argue that the hazards and the consequences generally are the same for both safety and cyber security related risk, but that the likelihood or frequency distribution is the main difference. As cyber-attacks often have a conscious and antagonistic motivation behind them, one cannot use general probability distributions based on historical occurrences. Instead, we should follow the principle defined by Anderson [21] that “we assume a hostile opponent who can cause some of the components of our system to fail at the least convenient time and in the most damaging way possible”. In order to evaluate and rank for autonomous shipping operations, Meland et al. [22] argue that we need to identify and assess threats based on the best data available. This paper also provides an overview of risk management frameworks



for the maritime domain, similarly to Svilicic *et al.* [23], Mraković and Vojinović [24], Bolbot *et al.* [25], Tusher *et al.* [26], Grigoriadis *et al.* [27] and Park *et al.* [28]. As pointed out by Tam and Jones [29], many of the existing frameworks do not adequately address cyberthreats for autonomous vessels. Therefore, our methodology builds upon the concept of assessing *storyless systems* [30] to address the novelty of autonomous shipping. Also, our methodology addresses the dynamic nature of the mission, acknowledging that the risk will vary according to the location and type of operation.



3 Methodology Overview

This chapter gives a short overview of the methodology. The methodology is used to describe the operation of autonomous ship systems, using a more systematic and structured approach than prose text. The purpose of doing this is to ensure that the structured description can be reused for cases where the autonomous ship system is changed or when the ship is operating in a different area. Further, the resulting description can be used as a starting point for safety and security analysis of the system.

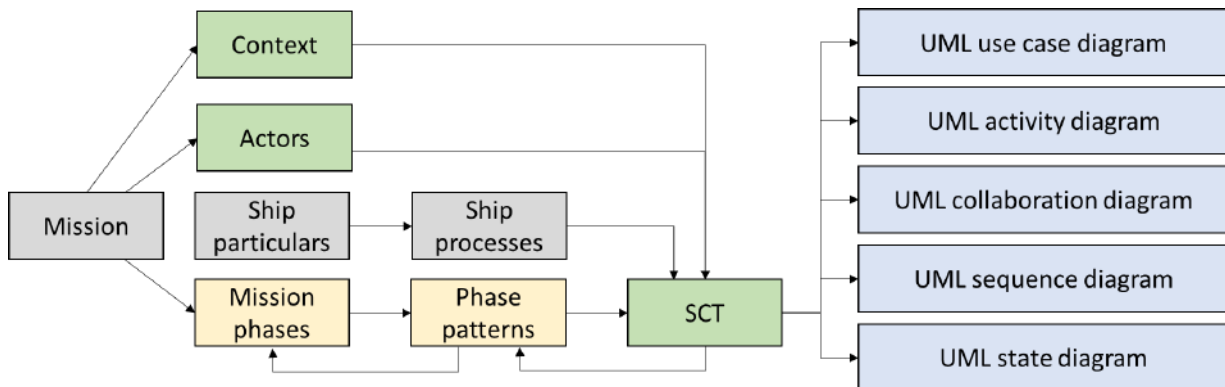


Figure 9: Summary of methodology for analysis of autonomous ship system operation

Figure 9 shows the different parts of the methodology (left part) and indicates that the operational description of the autonomous ship system can be formalized by a set of UML diagrams (blue boxes to the right).

The methodology starts with a textual and high-level description of the *mission*, which may for instance be a certain voyage with port calls and cargo operations. The mission is further detailed in the textual descriptions as follows:

- *Context*: The external entities and systems that the ship system cannot directly control. This includes other ships, traffic services as VTS and MRS (ship reporting areas), pilots, fairway information (Maritime Safety Information, aids to navigation), port services related to cargo handling and mooring, fairway services related to tugs and anchorage, river services related to locks and bridges, among others.
- *Actors*: These are the actors that are part of the autonomous ship system. This includes the autonomous ship itself with the autonomous onboard controller, and also the RCC operators, automatic cranes and mooring systems, location positioning systems, among others.
- *Mission phases*: The mission is broken down in a set of mission phases which is characterised by a set of geographic and operational parameters, also called state variables. One example is a parameter describing the attention needed by the RCC operator, whether it is high, medium, low or direct, for each phase of the mission, for instance covering various legs of a voyage. The mission can be described as a set of specific phases, for instance automatic or supervised sailing through a specified part of the voyage, and cargo operation, port navigation, berthing and de-berthing related to a specific port call.
- *Phase patterns*: Each mission phase must be generalised into a mission phase pattern. This may be an iterative process, meaning that the initial definition of the mission phase may need to be changed after the mission phase pattern has been defined (the arrow from Phase



patterns to Mission phases in Figure 9). Examples of generalized mission phases are automatic sailing, supervised sailing, cargo operation, port navigation, berthing and de-berthing.

Ship particulars is the description of the capabilities of the autonomous ship. These capabilities are often tailored for repetitive mission, but general-purpose ships may also contain capabilities not relevant for the mission at hand. *Ship processes* are the different processes that the autonomous ship system must handle to implement a given mission. Examples of processes are energy production, cargo handling, and navigation.

System Control Tasks (SCTs) describe the safe operation of a certain component in a certain mission phase and ship process. The SCT and their prose definitions are developed based on the context, actors, ship processes and phase patterns. One SCT can span several system processes and possibly several mission phases. Each SCT is described by an associated state space that defines the parameter ranges over which the respective component can safely function. Examples of state variables/parameters are:

- Geographic parameters (depth, width of fairway, traffic separation schemes etc.)
- Weather parameters (wind, current, waves, etc.)
- Traffic parameters (number of ships in vicinity, their speed and heading etc.)
- Sensor quality parameters (day/night, rain/snow, sea clutter etc.)
- Ship system parameters (power available, equipment defects, cybersecurity breach, etc.)
- Communication parameters (RCC data link, data links to other ships etc.)
- Remaining supplies on board (fuel, electric energy etc.)
- Ship condition (trim, heel, list, draught etc.)

The SCT definitions can be represented by suitable UML diagrams. There are different types of such diagrams, e.g., UML activity diagrams, UML state diagrams, UML sequence diagrams, UML collaboration diagrams, UML class diagrams, and UML use case diagrams. As part of this methodology, the resulting UML diagrams can be used as a basis to systematically perform safety and security analysis.



4 Big Picture of Mission Example: Rotterdam-Ghent

The mission we use to illustrate the methodology is based on AEGIS Use Case B, which is a planned autonomous RoRo barge route that runs out of the DFDS terminal in the Rotterdam Port (Vlaardingen) towards the DFDS terminal in Ghent which is part of North Sea Port.

What makes this example interesting from an analysis point of view is that we have to consider the following factors:

- This is an inland waterway route passing through a number of locks and bridges.
- The route goes from one country to another (Netherlands - Belgium).
- The waterways have varying degrees of traffic that requires manoeuvring in a narrow space. This includes leisure boats of varying sizes.
- Blocking or congestions may introduce serious delays to the other vessels and ports, as well as hinterland operations.
- The barges operating along these routes are heavy and slow-moving.
- The terminals will have reserved space for RoRo barges, extending the autonomous operations to landside operations.
- It is easy for a threat agent to be in the physical vicinity of the vessels even from ashore. The same applies for the landside infrastructure.

The vessels will depend on sensors onboard and interact with lock and bridge services. In addition, communication is needed for remote control fallback with an RCC, monitoring and inform about changes in operational variables.



5 Context

The context of inland waterway sailing can be divided into what is done today and what is foreseen with autonomous systems in the future. Parts of today's context systems are likely to be automated as well, or at least be upgraded to support the autonomous operations of the barges. The most relevant external entities and systems are as follows:

Today's situation:

- Locks are directly manually operated or locally controlled from centres in the vicinity of the locks. While inside the locks, the barges need to do mooring while being raised/lowered.
- Bridges will need to be raised when the barges do not have sufficient clearing.
- Signalling systems are used for controlling traffic, for instance related to entering/exiting locks or for waterway intersections.
- Terminals contain berthing equipment and cranes for cargo operations. Also, trucks may be used for trailer-based cargo operations.
- Other ships (commercial and leisure crafts) sail in the vicinity of the barges. Traffic operations such as yielding, overtaking and turning is something that the barges must be aware of. Queuing before entry to locks is also very typical for these operations.
- Different kinds of inland aids to navigation (AtoN), such as buoys, beacons, fog signals, are located in the water or onshore.
- In addition to VHF radio, different kinds of land-based communication systems are available, in particular 4G/5G cellular networks.
- Inland AIS (iAIS) base stations on shore can track and exchange information with the barges. This includes static (e.g. ship number, call sign, name), dynamic (e.g. position, speed, course) and voyage-related (e.g. draught loaded, destination, estimated time of arrival) data.

Foreseen situation:

- Remote Control Centres (RCC) can either directly take control of an autonomous barge or provide tactical instructions.
- Locks and bridges become more automated, with little or no human presence. Remote control centres for operating these can be located far away.
- The locks can provide infrastructure for automatic mooring outside or inside the locks.
- Automated guided vehicle (AGV) will be used to unload trailers from the barges.
- Signalling systems and AtoNs become more virtual.
- Smart infrastructure technologies along the waterways, including sensors, CCTVs, transponders, etc.
- Other ships become more autonomous and cannot be hailed directly. Traffic can take place 24/7.
- Cargo operations can take place outside of the terminals, e.g., during the voyage.
- Barges become more electrified and may need to recharge or replace batteries during the voyage (outside the terminals).



6 Actors

Actors that are part of the Autonomous Ship System:

- AOC: Autonomous onboard controller (AOC): The AOC is a high-level controller which supervises all relevant ship systems and gains situational awareness based on data from onboard sensors as well as external sources such as weather data and navigational aids. Based on its control algorithms and situational awareness, the AOC continually makes necessary adjustments to the command signals which are sent to the various ship systems to ensure operation within the desired limits.
- RCC: (aka shore control center)

Actors external to the system:

- River Information Services (RIS): Support traffic and transport management in inland navigation.
- Remote Control Centres for locks and bridges.
- Manual or autonomous trucks.
- Manual or autonomous cranes.
- External boatmasters or other autonomous vessels.



7 Ship Particulars and Processes

For the chosen mission example, i.e., sailing between Rotterdam and Ghent, we have chosen a fictitious example vessel based on typical main dimensions for existing conventional vessels sailing this route. The example vessel will have a RoRo capacity of 48 TEU, but can alternatively support LoLo operation with stacked containers and a capacity of 144 TEU. For RoRo operation, the vessel has both a bow ramp and a small side ramp, to allow for cargo operations on smaller ports/terminals between Rotterdam and Ghent. The amount of "side loadable" cargo is not specified in this example, since such details are more relevant for optimizing operation than for security analysis. Table 2 presents a summary of the main dimensions and other specifications for the example vessel. Some of the specifications may be of limited relevance for the security analysis, but are included to give a comprehensive and realistic example vessel description:

Table 2: Ship particulars and key systems/functions for example vessel

Category	Specifications/description
Main dimensions	<ul style="list-style-type: none"> - Length: 110.0 m - Width: 12.50 m - Draught: 3.55 m
Machinery	<ul style="list-style-type: none"> - 2 x 12 cylinder diesel engines (900 kW each) - 2 x fixed propellers - 1 x bow thruster (500 kW) - Speed: 12,5 kn
Navigation	<ul style="list-style-type: none"> - Cameras (visible and infrared) - Radar - GNSS - Lidar? - Local positioning systems
Autonomous/remote control	<ul style="list-style-type: none"> - Autonomous onboard controller (AOC) to conduct autonomous sailing (with support from RCC) - Automatic mooring system, for use at compatible terminals and quays
Communication (vessel)	<ul style="list-style-type: none"> - 4G/5G - Line-of-sight (LoS) / WiFi
Communication (RCC)	<ul style="list-style-type: none"> - VHF - 4G/5G - Internet
Cargo capacity	<ul style="list-style-type: none"> - 48 TEU (RoRo), or - 144 TEU (LoLo)
Cargo equipment	<ul style="list-style-type: none"> - 1 x bow ramp - 1 x side ramp

Figure 10 shows a real vessel ("POLYBOTES", IMO:9280392), upon which the fictitious example vessel is based.



Figure 10: IWW vessel "POLYBOTES" (IMO: 9280392) [31] main inspiration when defining the particulars of the fictitious example vessel.

7.1 Ship Processes

The example vessel will perform various processes, and below is a selection of the most important ship processes for this assessment, based on the processes and tasks defined in the Autoship project [2]:

- S1 Navigation: Ship operation that includes sub-tasks related to:
 - S11 Situational awareness (Observation): Determine location, verify chart information, AtoN, observe weather and sea, determine visibility, detect and classify objects and obstacles, assess own ship and traffic situation.
 - S12 Ship control (Manoeuvring): Do short term planning for safe operations, keep track and course, avoid obstacles and grounding, operate dynamic positioning, semi-stationary or special operations.
 - S13 Voyage management (Navigation): Especially plan and replan voyage (communicate with management) and monitor voyage (act on deviations).
 - S14 Nautical communication: Communicate with other ships, RIS, VTS and similar digitally and operate other communication devices, light, lanterns, sound, etc.
- S2 Deck operation (Navigation support)
 - S21 Cargo and ship supplies operations: Including perform RORO operations, operate cranes, do lashing/unlashing in cargo hold or container stacks, operate hatches.



- S22 Mooring and anchoring: Moor and unmoor ship, drop and lift anchor.

In addition to these processes related to ship operations, there are other processes that the ship will need to interact with, such as:

- I IWW Operations
 - I1 Lock and bridge control: Including manage local bridge and locks, perform central bridge and lock management.
 - I2 River information system: Monitor traffic and inform ships, provide information to ships, receive ship reports.
- P Port Operations
 - P3 Cargo handling
 - P5 Mooring/Berthing - automated or manual services.
 - P6 Local Sensor Systems

However, these processes are outside of the ship or RCC control, and have a static location, so they are not modelled as dedicated control tasks for the ship in this assessment.



8 Mission Phases and Mission Phase Patterns

8.1 Description of Mission Phases

The foreseen route for the barge from Vlaardingen just outside Rotterdam and the DFDS terminal in Ghent, is found in the EuRIS-portal [32].



Figure 11: Distinct bodies of water for the route between Rotterdam and Ghent

The route is shown on the map in Figure 11 as coloured lines with red circles indicating the location of the four locks along the route. Table 3 lists all the mission phases that have been identified on the inland waterway route from Vlaardingen (Rotterdam) to the DFDS terminal in Ghent. This table only lists the mission phase pattern that each of the mission phase can be generalized to. The column *Characteristics* describes more details on each of the legs. The decision on which mission phase pattern to be used as a generalization of which mission phase, is based on the level attention that is needed



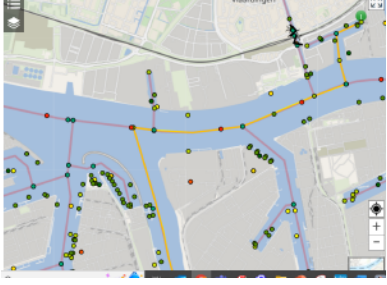
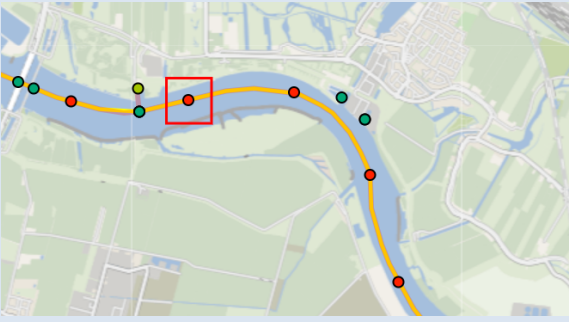
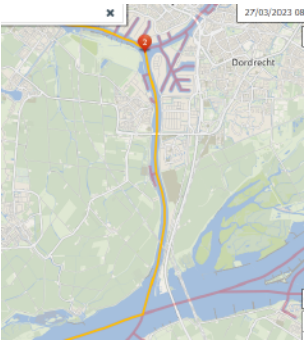
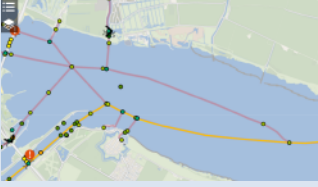
by the RCC operator during the leg and operation. Further, the level of attention by the RCC operation is dependent on several parameters:

- The traffic density, for instance described as the number and type of ships in the area. Using AIS density maps for the actual area, we see that the traffic is overall dense, and that the big locks often have heavy traffic with queues of barges waiting to pass in both directions.
- The traffic complexity, for instance, frequent speed change and course change that is done on this leg, the course that the vessel has relative to the traffic, crossing traffic or parallel traffic.
- Fairway complexity, for instance curves, sight, how narrow the fairway is, current, tides, wind, whether it is canal or river. For this case, the whole fairway, except for the short distance when leaving the terminal in Vlaardingen and entering the main fairway, is classified as CEMT VIc. In some cases, specific visual signals are used by a barge to signal that the barge needs to deviate from standard navigational rules due to for instance the current (different current in the outer curves, or close to shallow areas)
- Communication possibilities, including the infrastructure on the shore-side.
- The complexity of the task, for instance passing a large lock with several chambers or difficult navigation under narrow bridges with marginal clearance.
- All the locks on this route are manually operated, however, in the further descriptions, we have added remotely operated locks and automatically operated locks to be able to cover future cases. For instance, for the remotely operated and automatic locks, the operation will be dependent on more sensors (cameras) and communication systems between the sensors at the lock and the operator or RCC for the lock. Some of the locks are large systems with several chambers meaning that the operator or lock control system must decide which chamber to use for each ship.
- Within the lock chamber, there might be some kind of flexible (height-adaptable) mooring system.
- Also, a lock passing will typically require the barge to be moored some time before being cleared for passage to the lock chamber. This may be done autonomous or with support from shore.
- Bridge passing: Theoretically, the bridges in this case have sufficient clearance for the vessel described in Chapter 7 to pass without requesting bridge opening. However, bridge opening is described as one of the mission phase patterns to make the description more complete. There might also be two other scenarios for passing a bridge without raising it:
 - 1) ballasting with water to lower the total height over water.
 - 2) If there is a height-adjustable bridge on the vessel, lower the bridge to pass underneath critical heights.

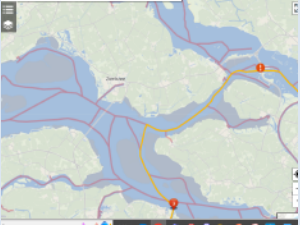
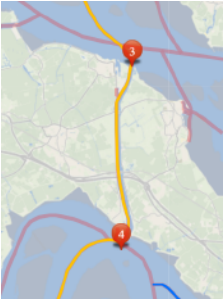
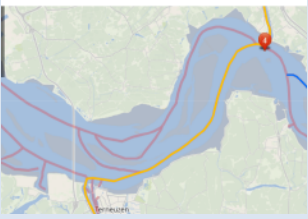
Table 3: Description of Mission Phases on the Rotterdam-Ghent IWW Route

Mission Phase	Mission Phase Pattern	Characteristics
Cargo operation Vlaardingen (Rotterdam)	Cargo Operation	
Deberthing Vlaardingen	Deberthing/Berthing	
Departure Vlaardingen: Sailing from berth in the terminal in Vlaardingen and into the river Nieuwe Maas, near the junction Nieuwe Maas - Toeloop close to Koningin Wilhelminahaven.	Port departure/arrival	The barge is leaving the port area in Vlaardingen and entering the fairway to Rotterdam, sailing west.
Sailing west-bound on river Nieuwe Maas from outside the terminal in Vlaardingen to junction Het Scheur - Oude Maas.	Complex IWW sailing	At the end of this leg, the barge must cross the traffic towards Rotterdam to enter the river Oude Maas to go south.

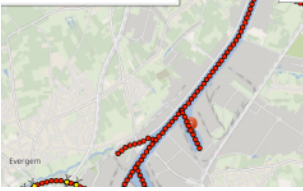


Mission Phase	Mission Phase Pattern	Characteristics
		
<p>Sailing southbound from junction Het Scheur-Oude Maas on river Oude Maas to the bridge Botlekbrug</p>	Simple IWW sailing	
<p>Sailing under bridge Botlekbrug</p>	Approaching bridge / Bridge passing	
<p>Sailing from bridge Botlekbrug to bridge Spijkenisserbrug</p>	Simple IWW sailing	
<p>Sailing under bridge Spijkenisserbrug</p>	Approaching bridge / Bridge passing	
<p>Sailing on river Oude Maas from bridge Spijkenisserbrug to junction Dordtsche Kil-Oude Maas in Dordrecht</p> 	Simple IWW sailing	
<p>Sailing on river Dordtsche Kil from junction Dordtsche Kil-Oude Maas in Dordrecht to junction : Hollandsch Diep, Zuid Hollandsch Diep - Hollandsch Diep, Dordtsche. Entering the fairway going east-bound to Oosterhout, Eindhoven, and other places.</p> 	Complex IWW sailing	Narrow canal
<p>Sailing on Hollandsch Diep from previous junction til the point when turning south towards Volkerak Lock.</p> 	Simple IWW sailing	
<p>Lock passing: Volkerak Lock including a bridge over the lock.</p>	Approaching lock / Passing lock chamber	Heavy traffic in locks



Mission Phase	Mission Phase Pattern	Characteristics
Sailing westbound from Volkerak lock and bridge to Krammer lock and bridge.	Simple IWW sailing	
Lock passing: Krammer Lock	Approaching lock / Passing lock chamber	Heavy traffic in locks
Sailing: from Krammer Lock to Wemeldinge including some strict turns en route: 	Complex IWW sailing	One sharp course change needed, Several areas with shallow water in this area.
Sailing south bound on canal through Zuid-Beveland From Wemeldinge to Hansweert 	Simple IWW sailing	
Passing bridge Vlakebrug	Approaching bridge / Bridge passing	
Continue sailing south bound on the canal from Vlakebrug till entrance of Hansweert Lock.	Simple IWW sailing	
Lock passing: Hansweert Lock (tide-dependent)	Approaching lock / Passing lock chamber	Heavy traffic in locks
Leaving the Hansweert lock and exit the canal at Hansweert, and entering Westerschelde.	Complex IWW sailing	
Sailing: Westerschelde (Western Scheldt): From Hansweert to Terneuzen. Passing through the fairway leading to Antwerp. 	Complex IWW sailing	High traffic density as the route is crossing the fairway in and out of Antwerp. Also, this leg goes through a large area with shallow waters.
Lock passing: Terneuzen Lock	Approaching lock / Passing lock chamber	Heavy traffic in locks
Sailing: Canal Ghent-Terneuzen: From Terneuzen to bridge Sluiskil, towards Ghent	Simple IWW sailing	
Passing bridge Sluiskil.	Approaching bridge / Bridge passing	
Continue sailing: Canal Ghent-Terneuzen: From bridge Sluiskil to bridge Sas van Gent towards Ghent	Simple IWW sailing	
Arrival DFDS Terminal in Ghent	Port departure/arrival	



Mission Phase	Mission Phase Pattern	Characteristics
		
Berthing at DFDS terminal in Ghent	Deberthing/Berthing	
Cargo operation at DFDS terminal in Ghent	Cargo operation at terminal	

8.2 Description of Mission Phase Patterns

Each mission phase pattern has been subject to an autonomous job analysis (AJA) as proposed by the Seatonomy project [6], [7]. This analysis includes the following characteristics:

- **Mission phase pattern description:** What are we trying to accomplish? What is the relationship to other sub-operations?
- **Communication:** What key information needs to be communicated? What are the communication restrictions and limitations? What communication infrastructure can be used?
- **Perception:** Which information about the environment and the system itself must be present?
- **Success criteria:** What are the criteria for successfully executing the sub-operation? How are the criteria quantified?
- **What can go wrong:** Which external and internal events should be planned for? What should the system do in case of undesirable events?
- **Operational safe state:** What should the system do in case of failure/damage?
- **Human Machine Interaction (HMI):** What type of user interaction is needed? What information does the operator need? What is the role of the human?
- **Other possible inputs:** Additional premises/requirements relevant for the analysis.

The Autonomous Job Analysis consists of the following steps [6]:

1. Describe the main goal of the operation.
2. Divide into sub-goals, based on e.g. sequence, parallel behaviour or choices.
3. Answer the list of AJA questions in AJA Table (page 9 in[6]).
4. For each sub-goal, go to step 2 and repeat until goals become trivial tasks.

The following mission phase patterns are identified for the IWW sailing from Rotterdam to Ghent, where also some foreseen phase patterns that are currently not part of this sailing, are added (the word "foreseen" added to the name), Table 4:

Table 4: List of Mission Phase Patterns in IWW Scenario

Mission Phase Patterns
1. Approaching Lock
2. Approaching bridge



3. Passing Bridge
4. Passing Lock Chamber
5. Complex IWW Sailing
6. Simple IWW Sailing
7. Cargo operation in terminal
8. Cargo operation outside main terminals (foreseen)
9. Deberthing/berthing
10. Port departure/arrival

Mission phase pattern description	1. Approaching lock
Description	The barge approaches the lock and queues when necessary. Queuing includes mooring before the lock. Enters when the lock is available. Commercial ships may overtake leisure boats.
Communication	Barge/RCC operator – Lock operator: Request passing, clearance to enter, queuing position. Provide static information: Call sign, type of ship, dimensions. Communication infrastructure: Marine-band VHF, 4G/5G, Internet, iAIS Limitations: Need available RCC operator and Lock operator (local, remote, automatic).
Perception	Barge: Traffic, queue position, signalling system, gate state Lock system: Barge autonomy level, position of the vessels
Success criteria	Efficient passing of the lock, minimize queuing before the lock
What can go wrong	Collision (damage) Wrong interpretation of the bridge clearance due to the chart references or tidal effects. (damage) Not able to enter (delay, blocking) Not able to do mooring before the lock (unsafe state) No communication with remote lock operator (lock disruption)
Operational safe state	Halt ship, mooring of ship, request manual takeover
Human Machine Interaction (HMI)	RCC Operator should be able to monitor the position, sensor data and status of the autonomous ship. RCC Operator should be able to control or take control of the autonomous ship.
Other possible inputs	

Mission phase pattern description	2. Approaching bridge
Description	Similar to mission phase pattern 1. Before approaching the bridge, clarify whether bridge opening is needed or not. If not needed, sailing as usual within speed limits (5. Complex IWW Sailing). If needed, then do the following: Request bridge opening. Moor if needed to wait for the opening of the bridge. When ready, the barge approaches the bridge, making sure that it follows the speed limit in the bridge area. There could be queuing before the bridge, which could require mooring.
Communication	Need information on barge air draft, bridge clearance (at mean high water/middle water?), tide affecting the bridge clearance, opening hours for the bridge, speed limits. RCC Operator/Barge – Bridge system (Send announcement of the approach to the bridge. Receive bridge status to know when to prepare for bridge passing and when to pass the bridge. Provide static information: Call sign, type of ship, dimensions, bridge clearing, bridge status (raised/lowered) Communication infrastructure: iAIS, 4G/5G, Internet, Marine-band VHF Limitation: In case of remotely controlled bridge, no fallback to traditional verbal communication



Perception	Barge: Traffic, queue position, bridge state, signalling system Bridge system: Barge autonomy level, number of ships waiting to pass, size of ships.
Success criteria	Minimize queuing before the bridge, no human intervention
What can go wrong	Collision (damage) Not able to moor (unsafe state)
Operational safe state	Halt ship, back ship, mooring of ship, give alert.
Human Machine Interaction (HMI)	RCC Operator should be able to monitor the position, sensor data and status of the autonomous ship. RCC Operator should be able to control or take control of the autonomous ship.
Other possible inputs	

Mission phase pattern description	3. Passing bridge
Description	If the bridge does not need to be raised, this is similar to mission phase 5. Complex IWW Sailing. The barge will then sail under the bridge, but there could be queuing of ships waiting for the bridge to be raised. There could be several bridge pass areas. In cases where the bridge must be raised, the barge sail when the signal gives clearance or by clearance from direct communication.
Communication	Barge/RCC operator – Bridge system: Request passing, clearance to enter, queuing position. Provide static information: Call sign, type of ship, dimensions. Communication infrastructure: Marine-band VHF, 4G/5G, Internet, iAIS Limitations: May need available RCC operator and bridge system operator (local, remote, automatic).
Perception	Barge: Traffic, queue position, bridge state, signalling system, barge air draft, actual bridge clearance, position of the highest bridge clearance, current tide, bridge opening hours, speed limits. Bridge system: Barge autonomy level, ships passing, size of ships, speed of ships (flow).
Success criteria	Efficient passing of the bridge, no intervention needed from RCC Operator
What can go wrong	When passing the bridge without opening, the passing is done at a place with not enough clearance. (damage) Hitting the bridge constructions (damage) Bridge lowered while ship is beneath it (not enough clearing) (damage) Collisions with other ships (damage) Problems with the navigation due to currents and winds close to the bridge (damage, blocking, delays) Unnecessary bridge opening (delays)
Operational safe state	Halt ship, back ship, give alert, request manual takeover of the barge
Human Machine Interaction (HMI)	RCC Operator should be able to monitor the position, sensor data and status of the autonomous ship. RCC Operator should be able to control or take control of the autonomous ship.
Other possible inputs	Depends on mission phase pattern 2. Approaching bridge

Mission phase pattern description	4. Passing lock chamber
Description	The barge enters the lock chamber based on signal and/or direct communication. The Lock system detects that the barge has entered the lock chamber. The barge is automatically or manually moored and raised or lowered in the lock chamber, usually with other vessels at the same time. The barge exits when the lock gate opens and signal is given.
Communication	Barge/RCC operator – Lock operator: Ready for lock operations. Provide static information: Call sign.



	Communication infrastructure: Marine-band VHF, 4G/5G, Internet, (iAIS) Limitations: Need available RCC operator and Lock operator (local, remote, automatic).
Perception	Barge: Signalling system, state of gates, other vessels. Lock system: Position of the vessels, state of gates, state of valves
Success criteria	Safe passing of lock, no unnecessary delays.
What can go wrong	Collision (damage) Not able to enter (delay, blocking) Not able to do mooring in the lock chamber (unsafe state) No communication with remote lock operator (lock disruption) Not able to exit (delay)
Operational safe state	Halt ship, mooring of ship, give alert. Lock system closes the gates if a dangerous situation is detected. Human intervention is needed to restart the lock system, after confirmation of the situation being OK.
Human Machine Interaction (HMI)	RCC Operator should be able to monitor ship and lock state. RCC Operator should be able to request control over the ship.
Other possible inputs	

Mission phase pattern description	5. Complex IWW sailing
Description	The barge is sailing in a canal or river where close attention (OA, OE) by the RCC Operator is needed due to heavy traffic, difficult navigation or other situations with limited reaction time.
Communication	Barge – RCC: Get status information from barge RCC-Barge: Switch to manual control of barge Communication infrastructure: 4G/5G, general high bandwidth with short delay and high uptime.
Perception	Barge/RCC Operator: Situational awareness during the sailing. Visual sensors, beacons, proximity sensors (radar/lidar data), iAIS data, traffic data, signalling systems, speed limits.
Success criteria	Safe and efficient sailing in complex waters
What can go wrong	Loss of communication (OA/OE not possible) Inefficient (slow) sailing, bottleneck (delays) Collision (damage) Unavailable resources (RCC overload) Resource demanding (fatigue)
Operational safe state	Halt ship, emergency manoeuvre (e.g., hard starboard turn), give alert
Human Machine Interaction (HMI)	RCC Operator should be able to monitor ship and bridge state. RCC Operator should be able to control the ship.
Other possible inputs	

Mission phase pattern description	6. Simple IWW sailing
Description	The barge is sailing in a canal or river where only attention from the RCC Operator is needed (FA, CA). If a situation occurs that requires RCC Operator attention, shift to 5. Complex IWW sailing.
Communication	Barge – RCC: Get status information from barge RCC-Barge: Switch to manual control of barge Communication infrastructure: Marine-band VHF, 4G/5G



Perception	Barge: Visual sensors, beacons, proximity sensors (radar/lidar data), iAIS data, signalling systems, speed limits. RCC Operator: Situational awareness during the sailing
Success criteria	Successful sailing according to the voyage plan from start to end on the leg. Switch to 5. Complex IWW sailing in time for the RCC operator to assess the situation, decide on the action needed, to perform the action, and the barge to do the manoeuvring or other action requested.
What can go wrong	The AOC (Autonomous Onboard Controller) fails to warn the RCC operator about a critical situation, or the warning comes too late for the RCC operator to be able to react and the barge to perform the required action. Loss of communication (CA, OA not possible) Inefficient (slow) sailing, bottleneck (delays) Collision (damage)
Operational safe state	Shift to 5. Complex IWW sailing.
Human Machine Interaction (HMI)	RCC Operator should be able to monitor ship and environment. RCC should be able to request control of the ship.
Other possible inputs	

Mission phase pattern description	7. Cargo Operation in terminal
Description	Unloading/loading of cargo while moored in a designated quay area. Cranes could be onboard the ship or onshore, and may be manually controlled, remotely controlled or automated. Ramps should be in position for RoRo-transshipment (automated operation of the ramps or remote control operation should be possible). AGVs could deliver and fetch trailers directly to/from the ship.
Communication	Barge – Crane: Operational information Barge -Truck: Operational information Barge – Automatic mooring system: Position data, status. Communication infrastructure: Marine-band VHF, 4G/5G, Internet (WiFi), Bluetooth, iAIS
Perception	The position of the ship, visual sensors on the ongoing cargo operation
Success criteria	Safe and efficient loading/unloading of cargo.
What can go wrong	Cargo placed in wrong position (unstable ship) Wrong cargo picked (economic impact) Damage to cargo or environment (economic, safety) Slow operation (delay, economic) Theft of cargo (illegal) Smuggling of illegal goods (illegal)
Operational safe state	Halt cargo operations, give alert, notify terminal crew
Human Machine Interaction (HMI)	The RCC Operator should be able to monitor the cargo operations.
Other possible inputs	The level of automation of the cargo operation may be indifferent to the ship.

Mission phase pattern description	8. Cargo Operation outside main terminals
Description	Unloading/loading of cargo while moored in an area along the voyage. The assumption is little infrastructure onshore, and RoRo only.
Communication	Barge/RCC Operator – Truck: Status of ship, clearance, instructions Communication infrastructure: 4G/5G, Bluetooth



Perception	Position of the ship, beacons and/or visual sensors.
Success criteria	Safe and efficient loading/unloading of cargo.
What can go wrong	Cargo placed in wrong position (unstable ship) Wrong cargo picked (economic impact) Damage to cargo or environment (economic, safety) Theft of cargo (illegal) Smuggling of illegal goods (illegal)
Operational safe state	Halt cargo operations, give alert, notify authorities
Human Machine Interaction (HMI)	The RCC Operator should be able to monitor the cargo operations.
Other possible inputs	This is a foreseen/wanted phase pattern with many unresolved issues. Some mooring infrastructure will probably be needed.

Mission phase pattern description	9. Deberthing/berthing
Description	The ship is navigated to a designated quay and moored or anchored securely.
Communication	RCC Operator/barge – Automatic mooring system: RCC Operator – River Information System: Navigational instructions Communication infrastructure: iAIS, 4G/5G, Internet
Perception	Local tides, wind conditions, depths, navigation aids, available berth length, distances to the vessel's forward and aft from the berth, size of the harbor basin, other ships.
Success criteria	Efficient and safe berthing/deberthing. Avoiding unnecessary human intervention.
What can go wrong	Inefficient (slow) berthing/deberthing, bottleneck (delays) Collision (damage) Unavailable resources (RCC overload) Resource demanding (fatigue)
Operational safe state	Halt ship, emergency manoeuvre, give alert
Human Machine Interaction (HMI)	RCC Operator should be able to monitor ship and environment. RCC Operator should be able to control the ship.
Other possible inputs	

Mission phase pattern description	10. Port departure/arrival
Description	Similar to complex IWW sailing, where close attention (OA, OE) by the RCC Operator is needed due to heavy traffic, difficult navigation or other situations with limited reaction time.
Communication	Barge – RCC: Get status information from barge RCC-Barge: Switch to manual control of barge Communication infrastructure: 4G/5G, general high bandwidth with short delay and high uptime. Communication infrastructure: iAIS, 4G/5G, Internet
Perception	Barge/RCC Operator: Situational awareness during the sailing. Visual sensors, beacons, proximity sensors (radar/lidar data), iAIS data, traffic data, signalling systems.
Success criteria	Arrival not too early or late, safe and efficient sailing when departing from /arriving to port. Good communication with port authorities.
What can go wrong	Loss of communication (OA/OE not possible) Inefficient (slow) sailing, bottleneck (delays)



	Collision (damage) Unavailable resources (RCC overload) Resource demanding (fatigue)
Operational safe state	Halt ship, emergency manoeuvre, give alert.
Human Machine Interaction (HMI)	RCC Operator should be able to monitor ship and environment. RCC Operator should be able to control the ship.
Other possible inputs	



9 System Control Tasks

Table 5 shows how the relevant ship processes can be mapped to relevant mission phase patterns for the mission at hand. Similar colour indicates same sub-envelope. The ship processes (leftmost column) are described in Section 7.1.

Table 5: Mapping between ship processes and mission phase patterns

	1. Approaching Lock	2. Approaching Bridge	3. Passing Bridge	4. Passing Lock Chamber	5. Complex IWW Sailing	6. Simple IWW Sailing	7. Cargo operation in terminal	8. Cargo operation outside main	9. Deberthing/berthing	10. Port departure/arrival
S1 Navigation S11-S14	SCT1	SCT2	SCT3	SCT4	SCT5	SCT6			SCT7	SCT8
S21 Cargo and ship supplies operations							SCT9	SCT10		
S22 Mooring and anchoring	SCT11	SCT12		SCT13					SCT14	

9.1 Parametrization of Operational Envelope, SCT and State Variables

Table 6 shows how we characterise each system control task within the operational envelope by different geographic and operational parameters or state variables. We also indicate which fallback states are relevant when the operational envelope is exceeded.

Table 6: Parameterization of the System Control Tasks

System Control Task	OEnv	Operational Design Domain	Fallback states/Outside of ODD
SCT1: Navigating when approaching lock	OA - OE	Automation not accountable. RCC Operator accountable. Scenery: Narrow area before lock. Signals and signs. Environment conditions: Shielded. Some current. High connectivity. Dynamic elements: High traffic volume, queuing, slow flow rate, presence of special vessel (e.g. small leisure boats)	Halt ship, mooring of ship. OA: Request manual takeover
SCT2: Navigating when approaching bridge	OA - OE	Automation not accountable. RCC Operator accountable. Scenery: Different bridge entry points. Signals and signs. Environment conditions: Shielded. Some current. High connectivity. Dynamic elements: High traffic volume, queuing, slow flow rate, presence of special vessel (e.g. small leisure boats)	Halt ship, back ship, mooring of ship. OA: Request manual takeover
SCT3: Navigating through/under bridge	OA - OE	Automation not accountable. RCC Operator accountable.	Halt ship, back ship, mooring of ship, give alert. OA: Request manual takeover



System Control Task	OEnv	Operational Design Domain	Fallback states/Outside of ODD
		<p>Scenery: Special structure (bridge) that is signalised. Narrow passage. Potentially low vertical clearing.</p> <p>Environment conditions: Shielded. Little current. High connectivity.</p> <p>Dynamic elements: High traffic volume, slow flow rate, potentially queuing, presence of special vessels (e.g. small leisure boats)</p>	
SCT4: Navigating through a Lock Chamber	OA - OE	<p>Automation not accountable. RCC Operator accountable.</p> <p>Scenery: Special structure (lock) that is signalised. Narrow passage.</p> <p>Environment conditions: Shielded. Little current. High connectivity.</p> <p>Dynamic elements: High traffic volume, slow flow rate, potentially queueing, presence of special vessels (e.g. small leisure boats)</p>	<p>Halt ship, mooring of ship.</p> <p>OA: Request manual takeover</p>
SCT5: Navigating complex IWW	OA - OE	<p>Automation not accountable. RCC Operator accountable.</p> <p>Scenery: Potentially sharp curves. Potentially junctions/intersections. Signals and signs.</p> <p>Environment conditions: Shielded. Little current. High connectivity.</p> <p>Dynamic elements: High traffic volume, crossing traffic, slow flow rate, presence of special vessel (e.g. small leisure boats)</p>	<p>Halt ship, mooring/anchoring of ship.</p> <p>OA: Request manual takeover</p>
SCT6: Navigating simple IWW	(OA – OE) - FA – CA (OA-OE: This is identical to SC5 navigating complex IWW)	<p>Automation accountable during FA – CA</p> <p>Scenery: few sharp curves, wide passage, few obstructionS, no junctions.</p> <p>Environmental conditions: Sensors have a clear view (good illumination), calm weather. High connectivity.</p> <p>Dynamic elements: few other moving objects in the surrounding (low traffic density), low speed sailing of the subject.</p>	<p>Halt ship, mooring/anchoring of ship.</p>
SCT7: Navigating during berthing/deberthing	OA - OE	<p>Automation not accountable. RCC Operator accountable.</p> <p>Scenery: Special structure (berth). Potentially sharp curves. Signals and signs.</p> <p>Environment conditions: Shielded. Little current. High connectivity.</p> <p>Dynamic elements: High traffic volume, slow flow rate, presence of special vessels (e.g. small leisure boats)</p>	<p>Halt ship, mooring/anchoring of ship.</p> <p>OA: Request manual takeover</p>
SCT8: Navigating during port arrival/departure	OA - OE	<p>Automation not accountable. RCC Operator accountable.</p> <p>Scenery: Potentially sharp curves. Signals and signs.</p> <p>Environment conditions: Shielded. Little current. High connectivity.</p> <p>Dynamic elements: High traffic volume, slow flow rate, presence of special vessels (e.g. small leisure boats)</p>	<p>Halt ship, mooring/anchoring of ship.</p> <p>OA: Request manual takeover</p>



System Control Task	OEnv	Operational Design Domain	Fallback states/Outside of ODD
SCT9: RoRo in terminal	OA - OE	Automation not accountable. RCC Operator accountable. Scenery: Special structure (terminal). Ship fixed by mooring. Environment conditions: Shielded. Little current. High connectivity. Dynamic elements: Small traffic volume on/off deck (RoRo), slow flow rate, potentially queueing. Containers/trailers lashing/unlashing and shifting.	Halt cargo operations, give alert, notify terminal crew.
SCT10: RoRo outside of terminal	OA - OE	Automation not accountable. RCC Operator accountable. Scenery: Special structure (ramp). Ship fixed by mooring. Environment conditions: Shielded. Little current. High connectivity. Dynamic elements: Small traffic volume on/off deck (RoRo), slow flow rate, potentially queueing. Containers/trailers lashing/unlashing and shifting.	Halt cargo operations, give alert, notify authorities.
SCT11: Lock queueing	OA - OE	Automation not accountable. RCC Operator accountable. Scenery: Special structure (lock) that is signalised. Narrow area. Environment conditions: Shielded. Little current. High connectivity. Dynamic elements: Mooring system.	Halt mooring, emergency release, notify lock operator. OA: Request manual takeover.
SCT12: Bridge queueing	OA - OE	Automation not accountable. RCC Operator accountable. Scenery: Special structure (bridge) that is signalised. Narrow area. Environment conditions: Shielded. Little current. High connectivity. Dynamic elements: Mooring system.	Halt mooring, emergency release. OA: Request manual takeover.
SCT13: Mooring within lock chamber	OA - OE	Automation not accountable. RCC Operator accountable Scenery: Special structure (berth) that is signalised. Narrow area. Environment conditions: Shielded. Strong currents. High connectivity. Dynamic elements: Lock gates.	Halt mooring, emergency release, notify lock RC operator. OA: Request manual takeover.
SCT14: Mooring/unmooring at berth	OA - OE	Automation not accountable. RCC Operator accountable Scenery: Special structure (berth) that is signalised. Narrow area. Environment conditions: Shielded. Little current. High connectivity. Dynamic elements: Mooring system.	Halt mooring, emergency release. OA: Request manual takeover



10 UML Diagrams

10.1 Introduction

Table 7 summarizes the properties of each level of autonomy related to the AOC and the RCC Operator, and it also summarizes what triggers the transition of control between the actors. The table is set up based on Section 2.2. Some highlights from this tables include:

- The AOC can be the accountable party only when the mode of operation is full or constrained autonomy (FA or CA).
- Handover of control between AOC and RCC Operator has to be described for the operational modes Constrained Autonomy (CA) and Operator and Automation (OA).
- When the system operates in the Constrained Autonomy (CA) mode, the system must detect and notify the RCC Operator about situations in time for the operator to react and respond to the situation.
- All System Control Tasks (SCTs) need to handle the operational modes Operator and Automation (OA) and Operator Exclusive (OE).
- The operational modes Fully and Constrained Autonomy (FA and CA) is only relevant for SCT6, which covers Complex IWW Sailing. This means that for SCT6, the RCC Operator might be idle for a period, since the operator can trust the AOC to notify him about situations that may arise.
- If the RCC Operator is notified by the AOC about a situation, the system might transfer to the OA mode (Operator and Automation) or the OE mode (Operator Exclusive), where the RCC Operator is in control or just monitoring. If the RCC Operator fails to respond in time, the system may enter a fallback state.

Table 7: Levels of Autonomy and relations to the Autonomous Ship System

Operational Mode	AOC			RCC Operator			Detect when human control is needed?	System Control Tasks
	Accountable	Control	State	Accountable	Control	State		
FA (Fully Autonomous)	Yes	Yes	In control	No	No	Idle, monitoring (optional)	Not needed	SCT6
CA (Constrained Autonomy)	Yes	Yes	In control	No	No	Idle, Monitoring (optional)	AOC notifies in time	SCT6
OA (Operator and Automation)	No	Yes/No	In control, Stand by	Yes	Yes/No	Monitoring, In control	Not possible	SCT1, SCT2, SCT3, SCT4, SCT5, SCT6, SCT7, SCT8, SCT9, SCT10, SCT11, SCT12, SCT13, SCT14
OE (Operator Exclusive)	No	No	Stand by	Yes	Yes	In control	Not possible	SCT1, SCT2, SCT3, SCT4, SCT5, SCT6, SCT7, SCT8, SCT9, SCT10, SCT11, SCT12, SCT13, SCT14



10.2 UML Model Structure in Enterprise Architecture

This section describes how the Enterprise Architect tool is used to structure the information and diagrams for the IWW scenario. Figure 12 shows the structure of the information related to the IWW scenario as it is structured in the Enterprise Architect tool in the following folders:

- Overview: Links to all information stored in the modelling of the IWW scenario.
- Context: A big picture describing the IWW scenario, the relevant actors and means of communication.
- Scenario: The mission described by a Top Level Use Case (Figure 15) and Top Level Misuse Case (Figure 52), and the System Control Tasks as described in Table 5.
- Diagram Components: This folder contains reusable UML components describing activities, collaboration and interactions as listed in Figure 14, and further described in the following diagrams:
 - Activity Components: Figure 34, Figure 29, Figure 36, Figure 37, Figure 38, and Figure 39,
 - Collaboration Components: Figure 40, Figure 41 and Figure 42,
 - Sequence Components: Figure 43, Figure 44, Figure 45, and Figure 46,
- UseCases: This folder contains the UML diagrams describing each of the 14 System Control Tasks (SCTs) in the IWW mission and also how these SCTs are used as building blocks for describing the activities, Figure 13.
 - High Level Activities: Figure 16 shows the top-level activity diagram for the IWW scenario. Figure 17, Figure 18, Figure 19, and Figure 20 show how four of the top-level activities are created by using activity diagrams for SCTs as building blocks. Figure 21 shows the activity diagram for complex sailing using activity diagrams from the *Diagram Components* folder.
 - Diagrams for each SCT: Each SCT are described by an activity diagram, a collaboration diagram and a sequence diagram. These diagrams can be based on the *Diagram Components*, as described earlier. This is shown for a few of the SCTs to show examples of how this can be done.
- SafetyAndSecurityAnalysis: This folder contains UML diagrams describing the safety and security analysis as reported in Chapter 10.5.

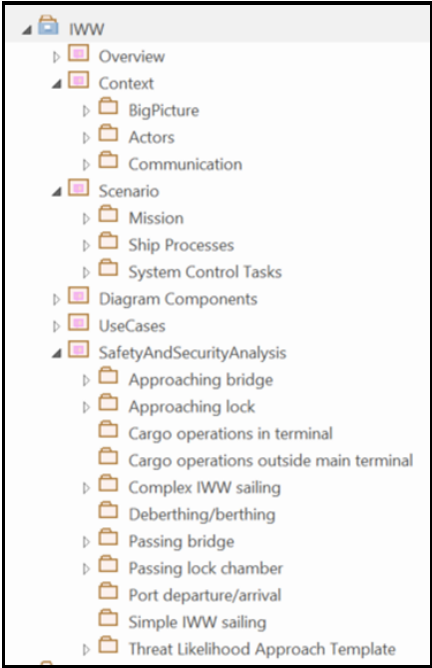


Figure 12: IWW Scenario Information in Enterprise Architect

Figure 13 shows the folder *UseCases* in the Enterprise Architect tool that contains the activity diagram, collaboration diagram and sequence diagram for each of the 14 Shore Control Tasks (SCTs). Currently, not all SCTs are fully described, however, a representative set of the STCs are handled to be able to show the methodology that we propose in this deliverable.

Figure 14 lists the diagram components that we have proposed to be used as building blocks when setting up the diagrams (activity, collaboration and sequence) for each SCT. The reason why we propose to use diagram components is that several of the SCTs are similar, meaning that reuse diagram components may ease the development of the UML diagrams.

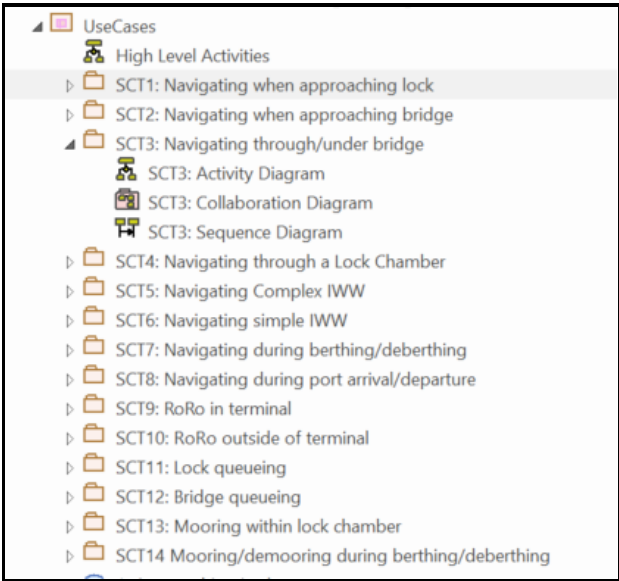


Figure 13: Enterprise Architect structure of the IWW UML models

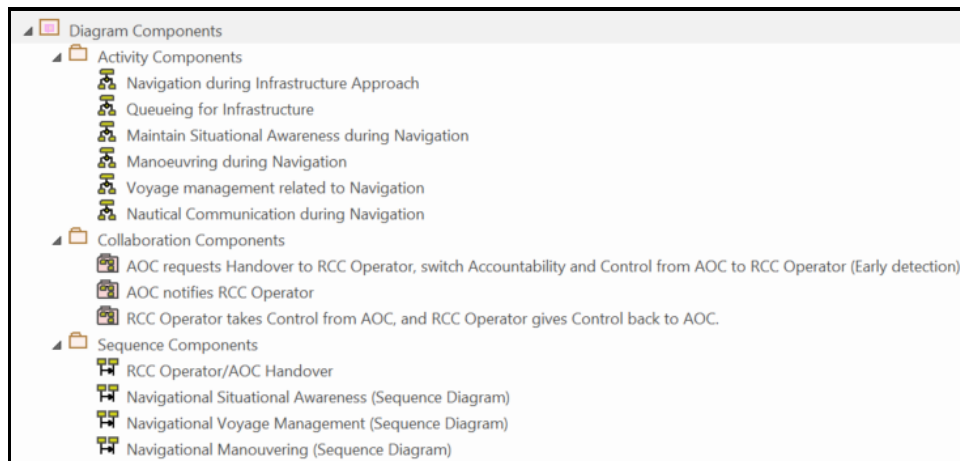


Figure 14: Enterprise Architect structure of reusable UML Components

10.3 UML Top-Level Use Case Diagram for IWW Scenario

Figure 15 shows the top-level activity diagram of the IWW scenario. Frames are drawn around several of the activities to make the relations to the actors easier to read: A relation from an actor to a frame, means that this actor is involved in all the activities inside this frame. Each of the activities corresponds to a *Mission Phase Pattern* as listed in Table 4.

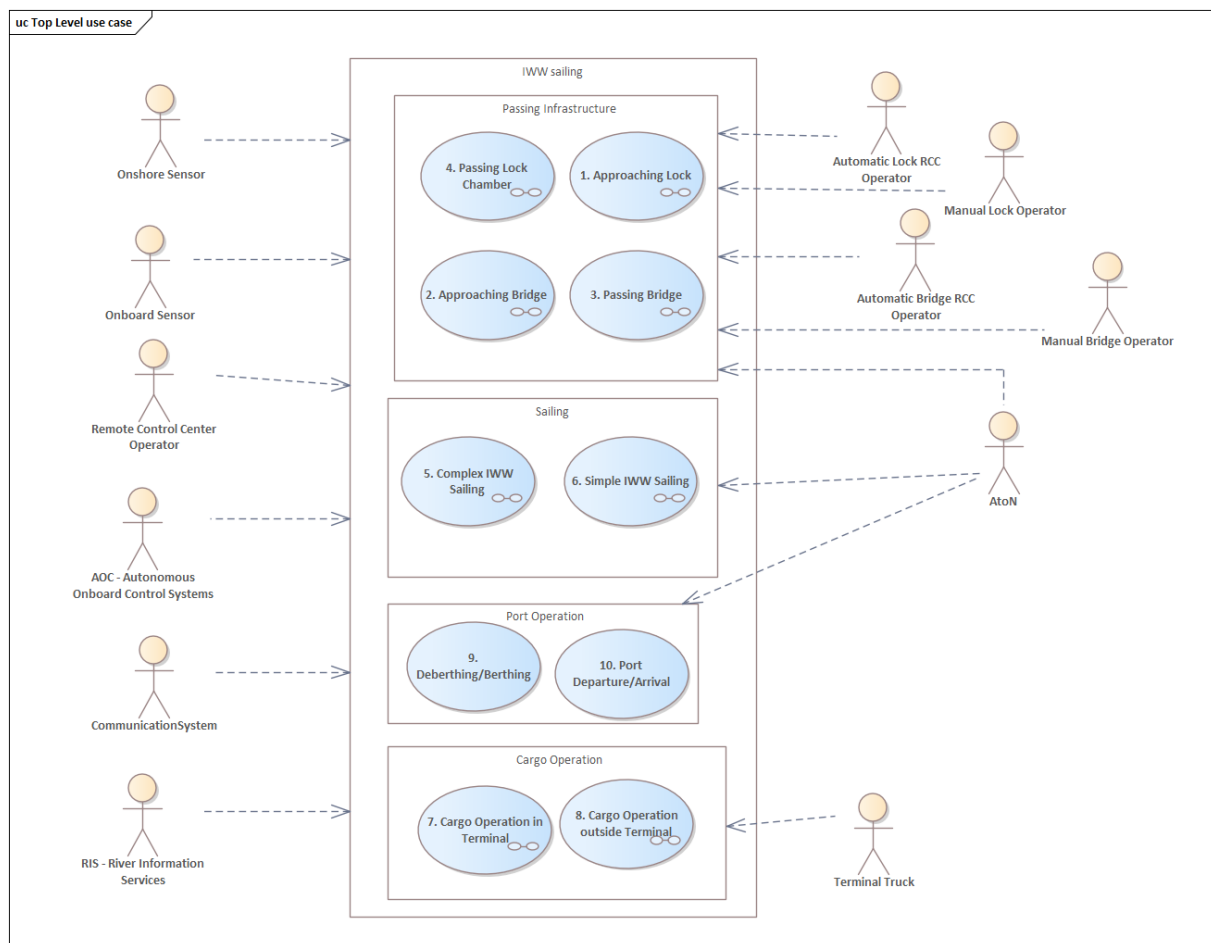


Figure 15: Top level use case diagram for the IWW scenario



10.4 UML Top-Level Activity Diagram for IWW Scenario

Figure 16 shows the high-level activity diagram for the IWW scenario. It shows that each of the phases related to port arrival/departure, deberthing/berthing, cargo operation, sailing, bridge- and lock passing can happen in any order. A ∞ in the activity means that a diagram exists, that further describes this activity. Examples of these activity diagrams are shown in Section 10.4.1, in Figure 17, Figure 18, Figure 19, Figure 20, and Figure 21 for the activities 1 through 5.

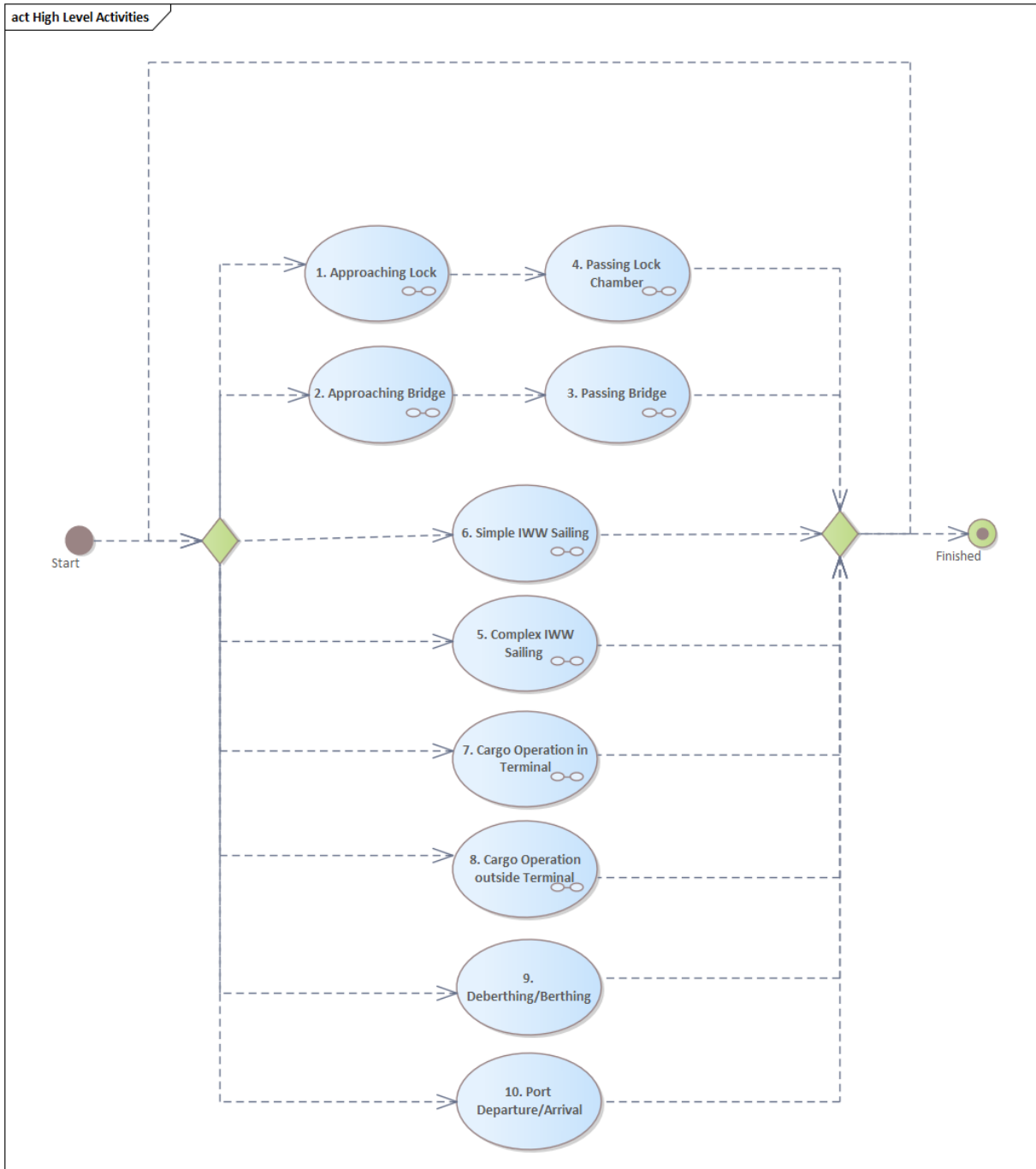


Figure 16: Top level activity diagram for the IWW scenario



10.4.1 Next Level UML Activity Diagrams

Figure 17 shows the activity diagram for Activity 1 Approaching Lock. This consists of two SCTs. First, SCT1 is to do navigation when approaching the lock, and then, SCT11 is to queue up before the lock, if that is necessary.

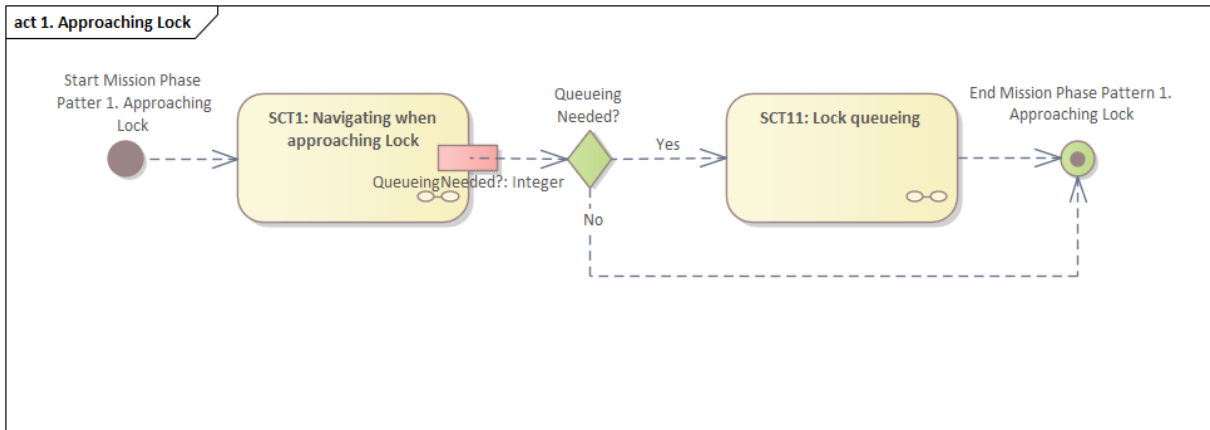


Figure 17: Activity 1 Approaching Lock

Figure 18 shows the activity diagram for Activity 2 Approaching Bridge, which contains the SCT2 Navigating when approaching bridge and then possibly followed by SCT12 bridge queueing, if that is needed.

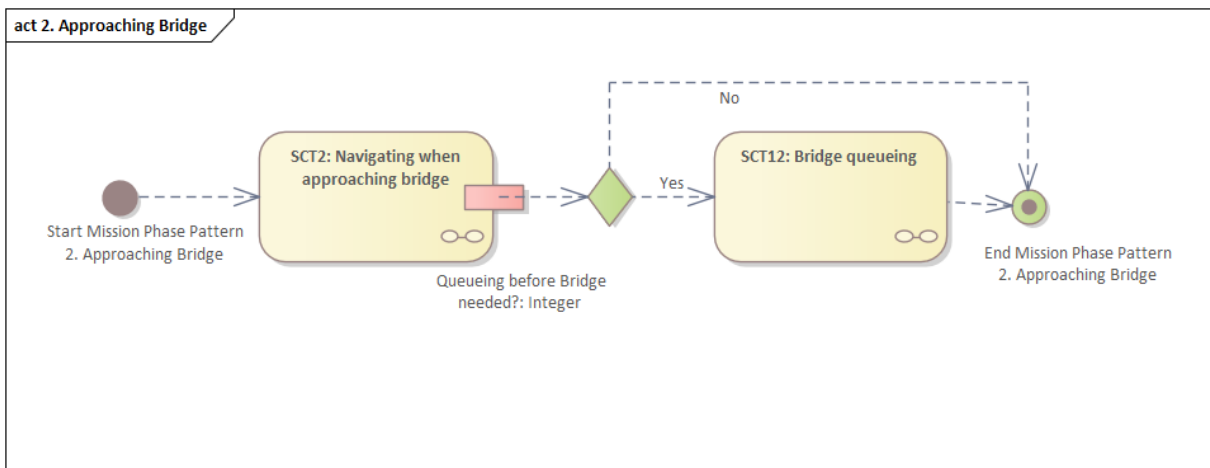


Figure 18: Activity 2 Approaching Bridge

The activity diagram for Passing Bridge (Activity 3, Figure 19) consists of just one SCT, namely SCT3 on Navigating through/under bridge.

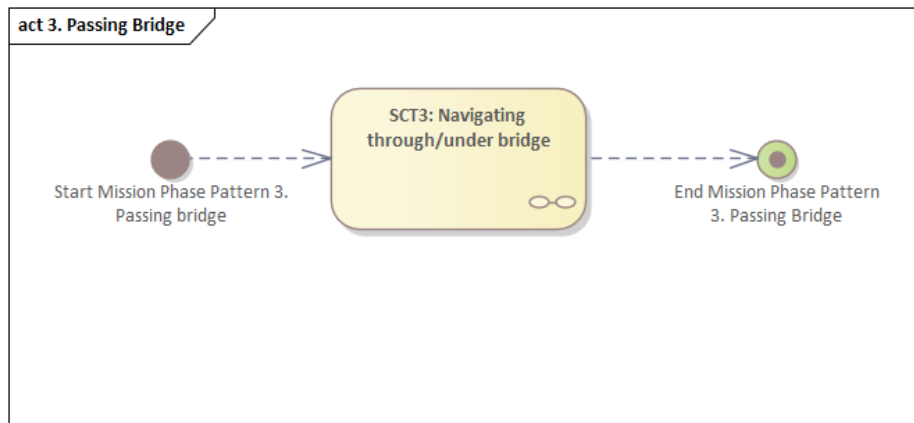


Figure 19: Activity 3 Passing Bridge

In Activity 4, Passing Lock Chamber (Figure 20), a possible mooring activity is added since, this may be needed inside the lock chamber (SCT13).

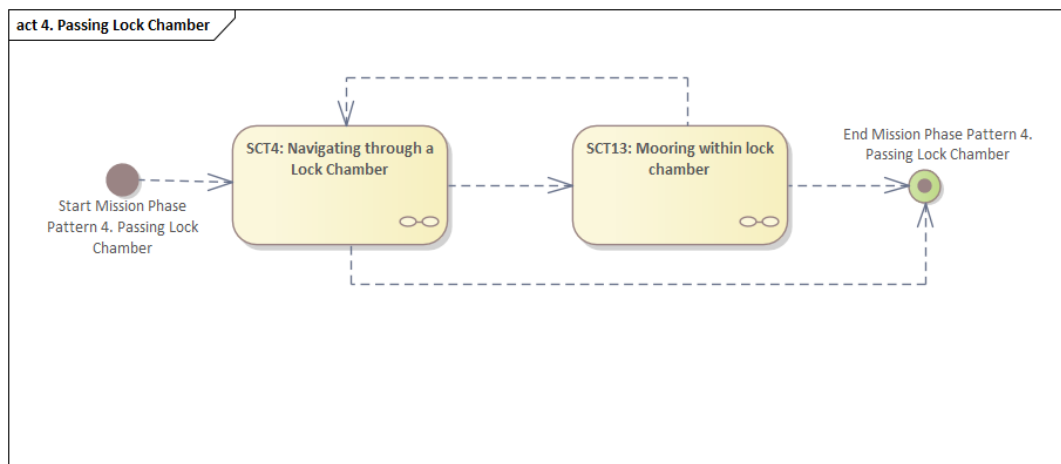


Figure 20: Activity 4 Passing Lock Chamber

Figure 21 shows the activity diagram for Activity 5 Complex Sailing, which consists of one SCT, namely the one for *SCT5 Navigating Complex IWW*. This shows that the diagram is built up using the diagram components for Maintain Situational Awareness during Navigation, Manoeuvring during Navigation, Voyage Management related to Navigation and Nautical Communication during Navigation. All these activities happen in parallel during complex sailing.

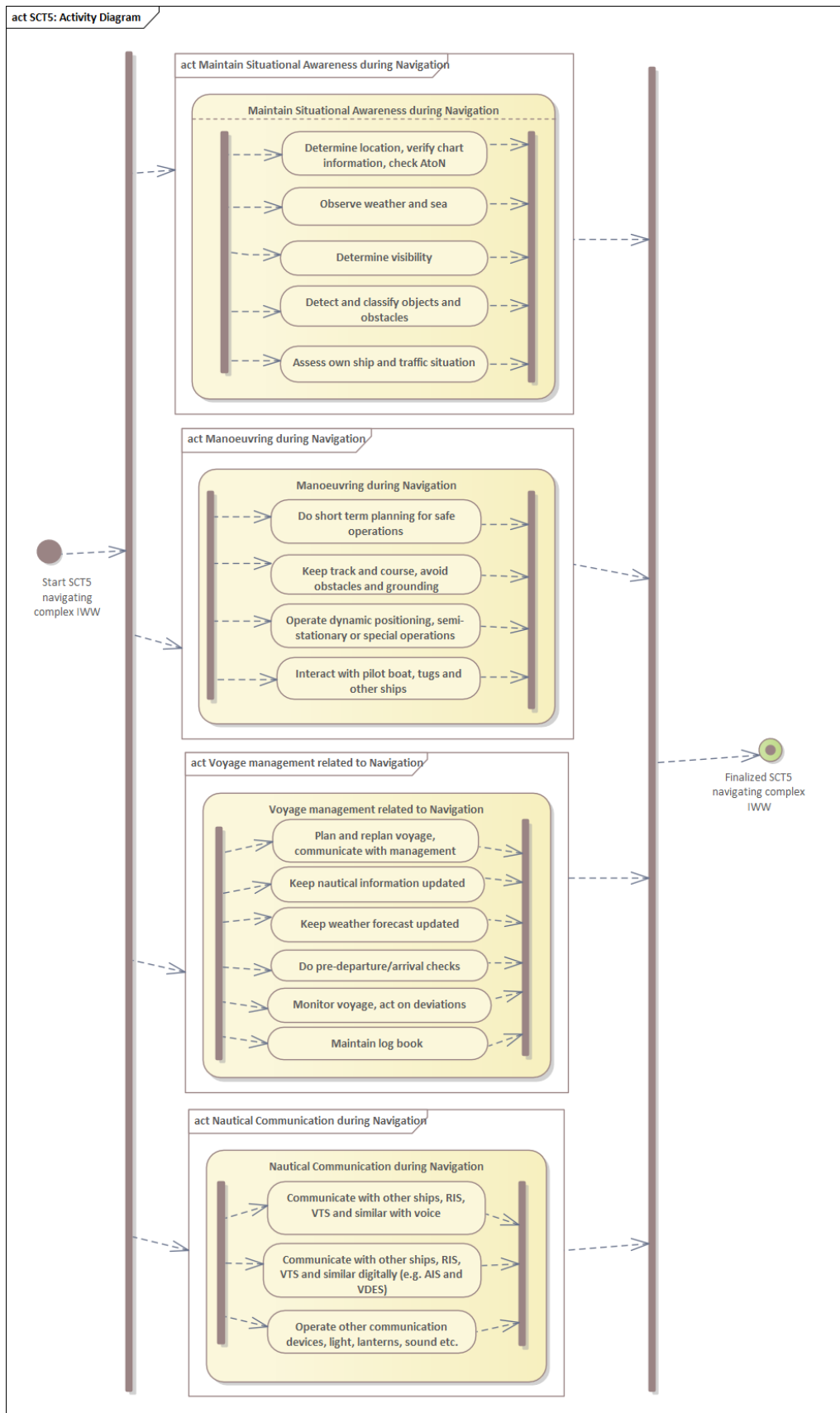


Figure 21: Activity 5 Complex Sailing



10.4.2 UML Diagrams for some SCTs

This section lists the UML activity diagrams, collaboration diagrams and sequence diagrams for some of the SCTs in the scenario.

10.4.2.1 UML Diagrams for SCT1 Navigating when Approaching Lock

This section contains UML diagrams for SCT1 Navigating when Approaching Lock. Figure 22 describes the UML activity diagram for SCT1. We see that in this diagram, the activity diagram component for Navigation during Infrastructure Approach (Figure 34) is reused.

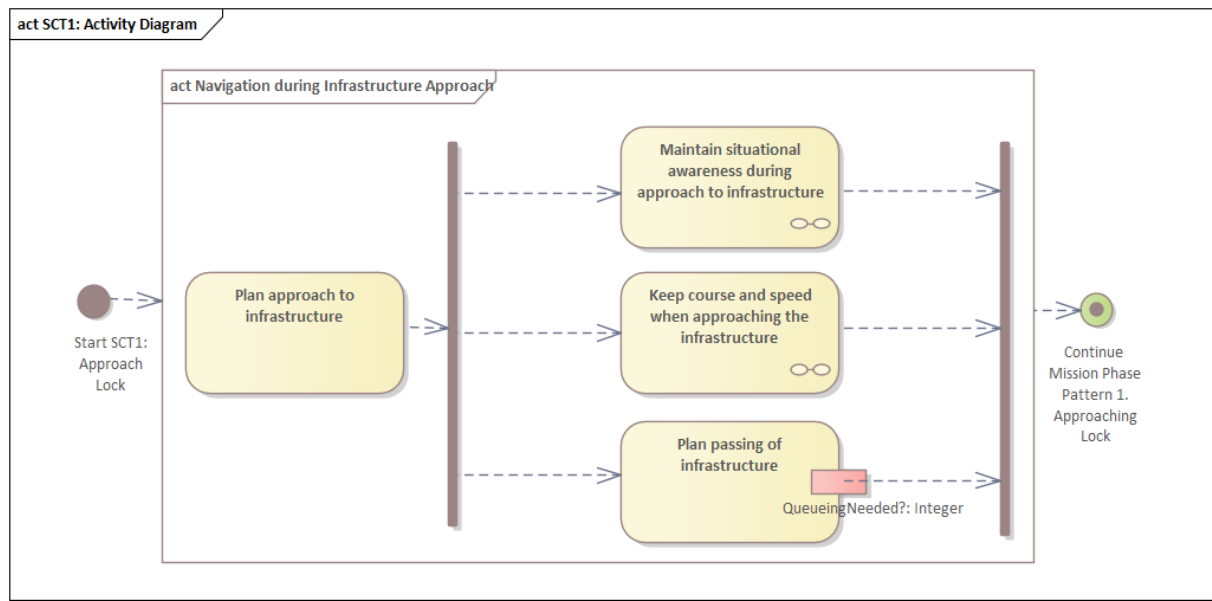


Figure 22: Activity Diagram for SCT1: Navigation during Infrastructure Approach

Figure 23 shows that the collaboration diagram for SCT1 consists of the two diagram components *RCC Operator takes Control from AOC, and RCC Operator gives Control back to AOC* (Figure 42) and *AOC notifies RCC Operator* (Figure 41).

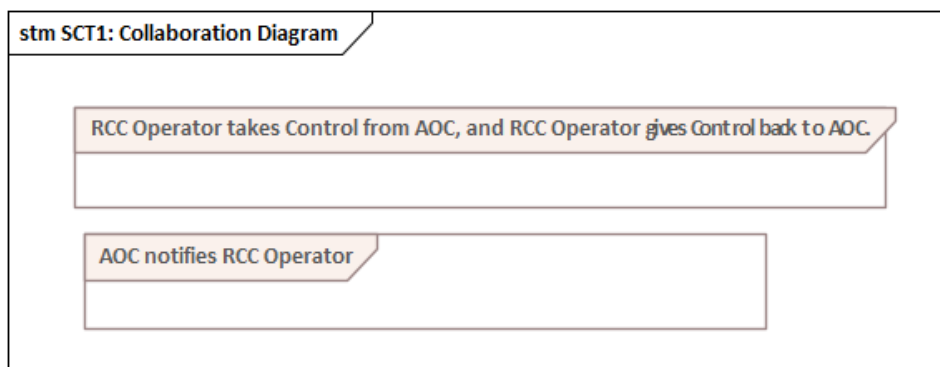


Figure 23: Collaboration Diagram for SCT1: Navigation during Infrastructure Approach

Figure 24 shows the sequence diagram for SCT1 Navigation during Infrastructure Approach. The first part of the sequence diagram shows a request to do the lock passing, then a confirmation is sent back. Further, the diagram components for *Navigational Situational Awareness* (Figure 44), *Navigational Manoeuvring* (Figure 46) and *RCC Operator/AOC Handover* (Figure 43) are reused.

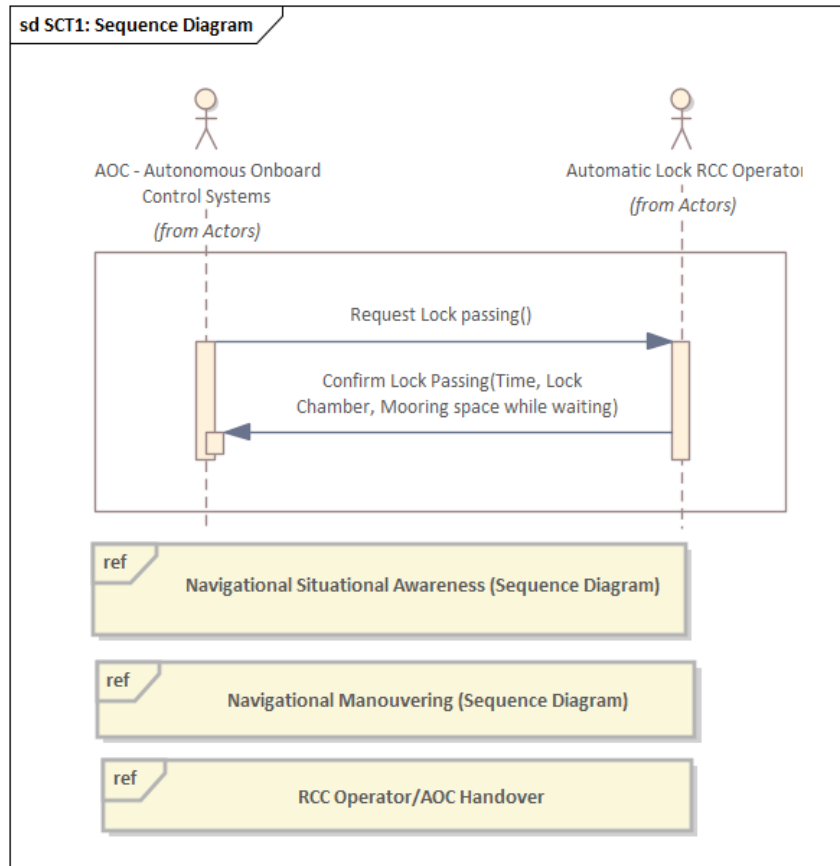


Figure 24: Sequence Diagram for SCT1: Navigation during Infrastructure Approach

10.4.2.2 UML Diagrams for SCT2 Navigating when Approaching Bridge

Figure 25 shows that the activity diagram for SCT2 on Navigating when approaching bridge uses the same activity diagram component as SCT1, namely the one for Navigation during Infrastructure Approach (Figure 34).

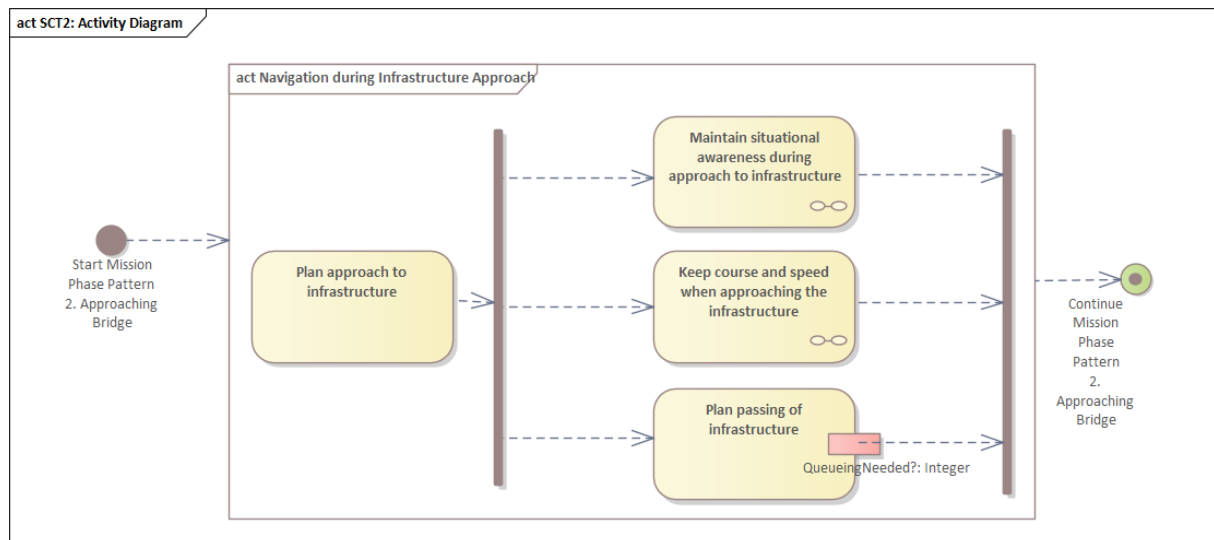


Figure 25: Activity Diagram for SCT2: Navigating when approaching bridge

The collaboration diagram for SCT2 is the same as that for SCT1, while the sequence diagram for SCT2 is shown in Figure 26.

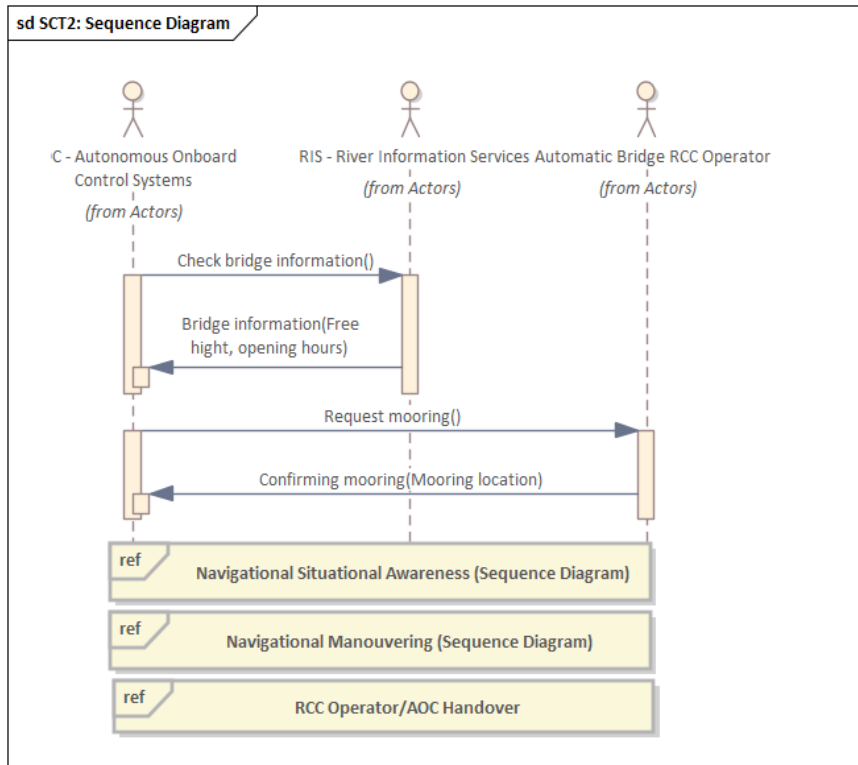


Figure 26: Sequence Diagram for SCT2: Navigating when approaching bridge

10.4.2.3 UML Diagrams for SCT5 Navigating Complex IWW

The UML activity diagram for SCT5 Navigating Complex IWW is shown in Figure 21. Figure 27 shows the collaboration diagram for SCT5 which consists of the diagram components for *RCC Operator takes Control from AOS, and RCC Operator gives Control back to AOC* (Figure 42), and *AOC notifies RCC Operator* (Figure 41).

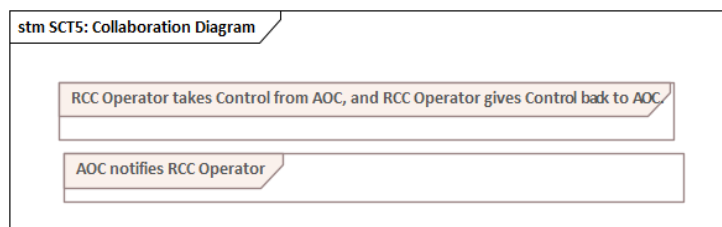


Figure 27: Collaboration Diagram for SCT5 Navigating complex IWW

Figure 28 shows the sequence diagram components that are chosen for SCT5.

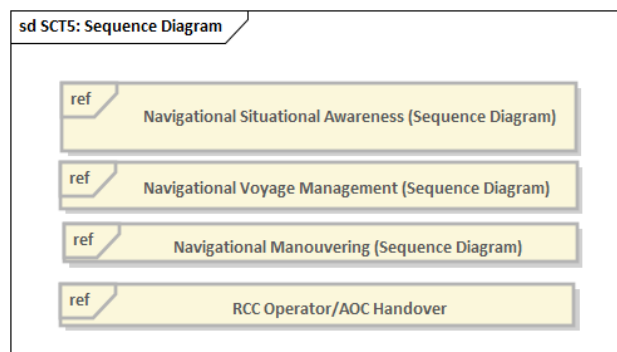


Figure 28: Sequence Diagram for SCT5 Navigating complex IWW



10.4.2.4 UML Diagrams for SCT6 Navigating Simple IWW

The collaboration diagram for SCT6 Navigating Simple IWW consists of three different collaboration diagram components, namely, for RCC Operator takes Control from AOC, and RCC Operator gives Control back to AOC (Figure 42), AOC notifies RCC Operator (Figure 41), and AOC requests Handover to RCC Operator, switch Accountability and Control from AOC to RCC Operator (Early detection) (Figure 40). Comparing this with Figure 27, shows that the difference between simple and complex sailing is that for the simple sailing, we also need to handle the case when the AOC requests the RCC Operator to take over control and accountability. This is because the autonomy level Constrained Autonomy (CA) in this scenario is only possible for SCT6 Navigating Simple IWW, and not for the SCT5 Navigating Complex IWW.

10.4.2.5 UML Diagrams for SCT11 Lock Queueing

Figure 29 describes activities related to lock queueing. For this description, the diagram component for *Queueing for Infrastructure* (Figure 35) is used.

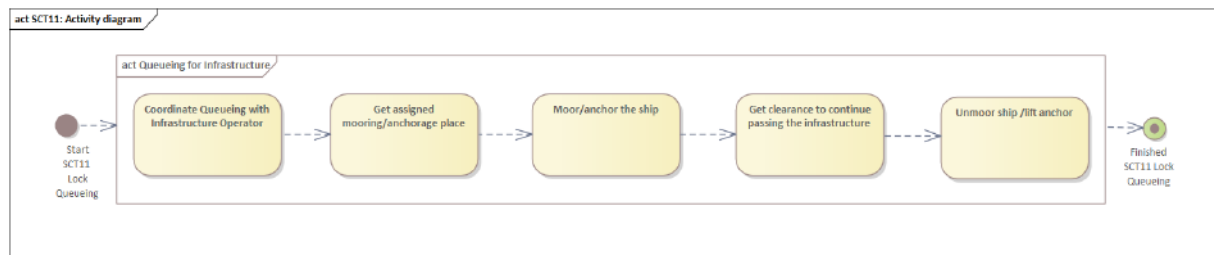


Figure 29: Activity diagram for SCT11: Lock Queueing

10.4.2.6 UML Diagrams for SCT12 Bridge Queueing

Figure 30 shows the activity diagram for bridge queueing based on the diagram component for queueing at an infrastructure (Figure 35).

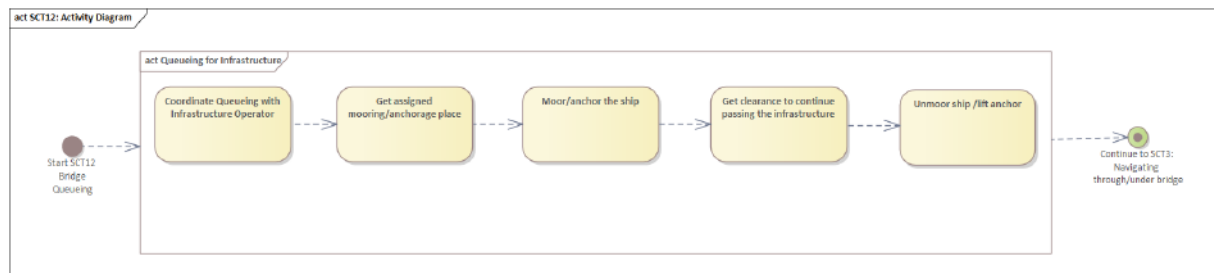


Figure 30: Activity diagram for SCT12: Bridge Queueing

10.4.2.7 UML Diagrams for SCT14 Mooring/Unmooring during Berthing/Deberthing

Figure 31, Figure 32, and Figure 33 from Deliverable D5.3 shows the activity diagram, collaboration and state diagram and sequence diagram for the mooring and unmooring SCT.

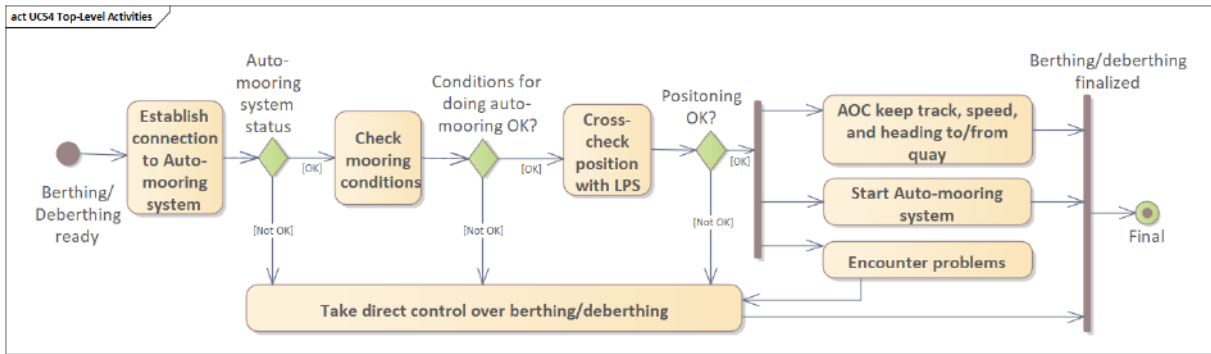


Figure 31: Activity diagram for SCT14: Mooring/Unmooring [from D5.3]

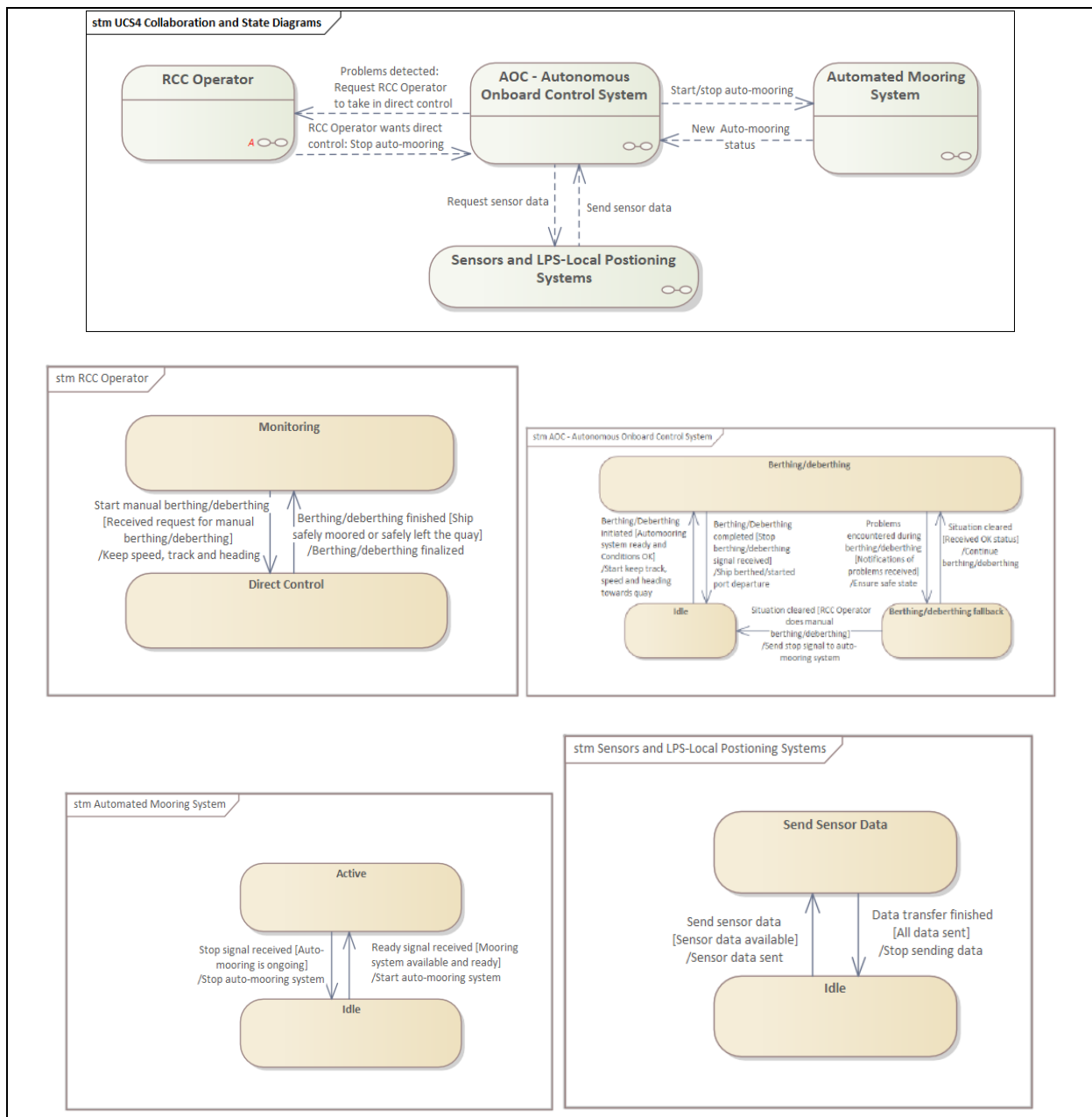


Figure 32: Collaboration and state diagrams for SCT14: Mooring/Unmooring [from D5.3]

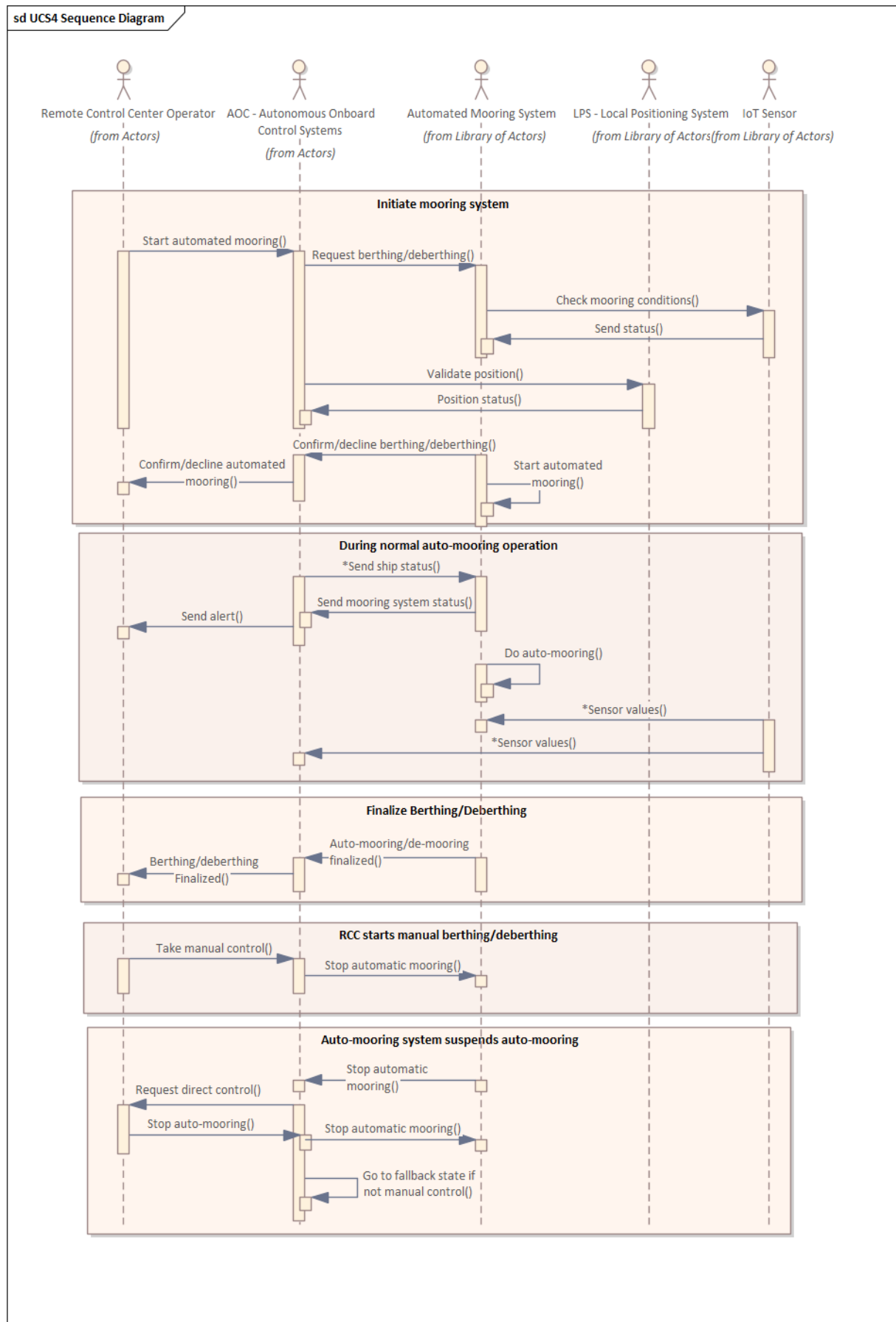


Figure 33: Sequence diagram for SCT14: Mooring/Unmooring [from D5.3]



10.5 Diagram Components

This section shows the diagram components that can be reused when setting up the UML diagrams for the specific activities and SCTs. The purpose of the diagram components is to capture behaviour that is common for several activities and SCTs. Section 10.5.1 shows UML activity diagram components, Section 10.5.2 shows collaboration diagram components, while Section 10.5.3 shows sequence diagram components.

10.5.1 UML Activity Diagram Components

The UML activity diagrams in Figure 34, Figure 35, Figure 36, Figure 37, Figure 38 and Figure 39 shows the diagram components that can be used as building blocks when setting up activity diagrams for the various System Control Tasks (SCTs).

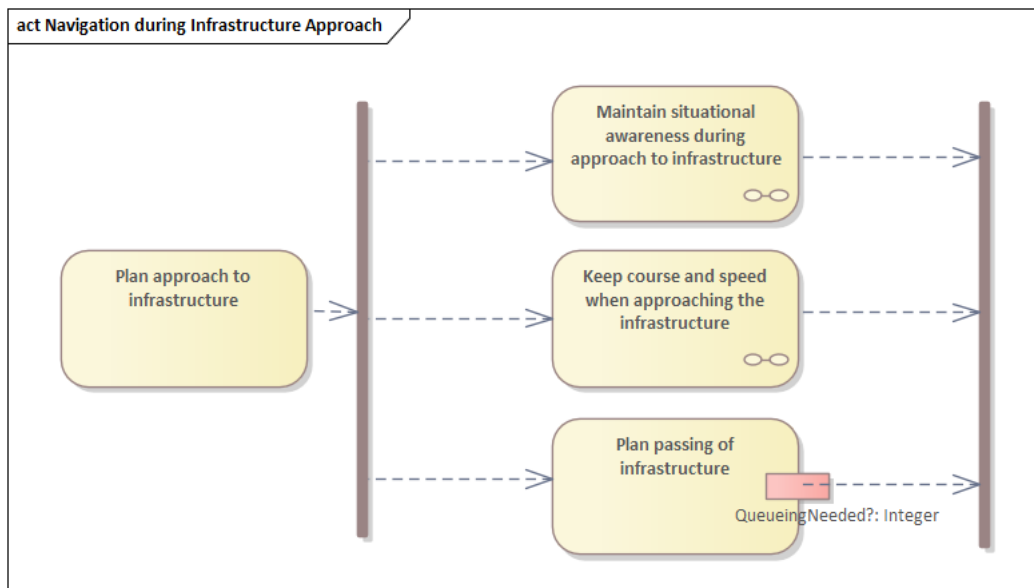


Figure 34: Diagram Component: Activity Diagram for Navigation during Infrastructure Approach

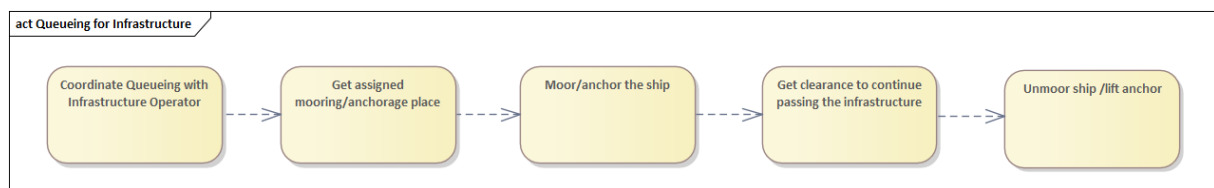


Figure 35: Diagram Component: Activity Diagram for Queueing for Infrastructure

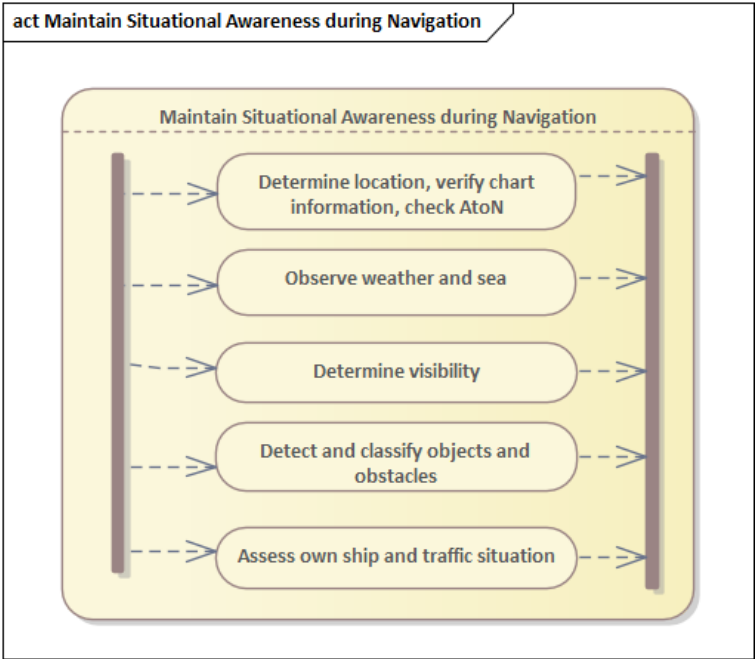


Figure 36: Diagram Component: Activity Diagram for Maintain Situational Awareness during Navigation

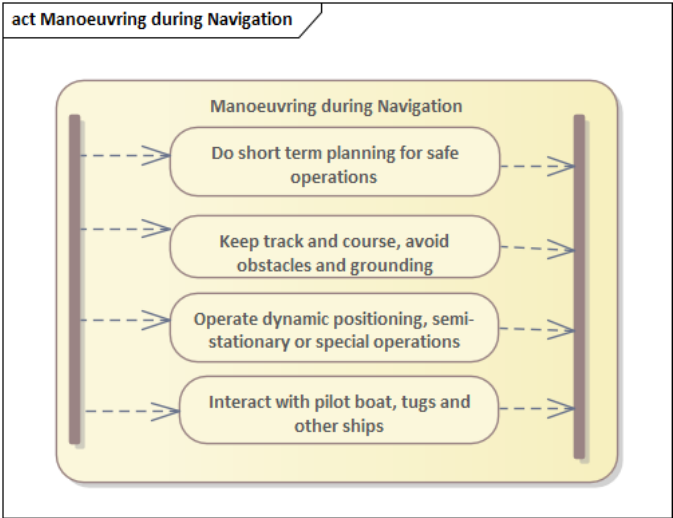


Figure 37: Diagram Component: Activity Diagram for Manoeuvring during Navigation

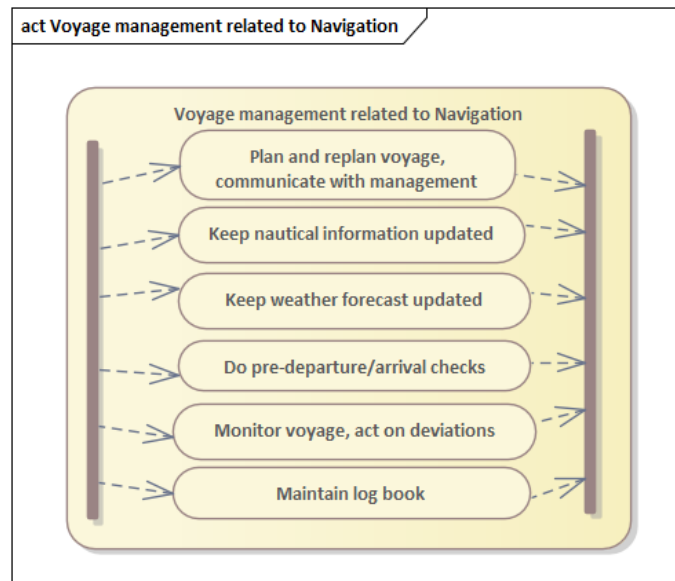


Figure 38: Diagram Component: Activity Diagram for Voyage Management related to Navigation

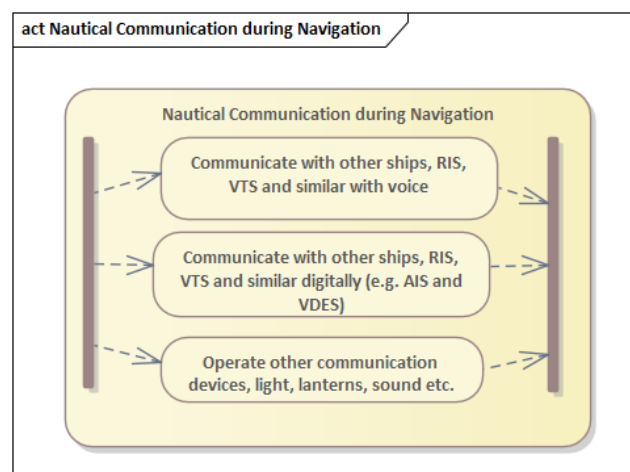


Figure 39: Diagram Component: Activity Diagram for Nautical Communication during Navigation

10.5.2 UML Collaboration Diagram Components

The UML collaboration diagrams in Figure 40, Figure 41, and Figure 42 shows the diagram components that can be used as building blocks when setting up collaboration diagrams for the various System Control Tasks (SCTs).

In Figure 40, the flow starts with the AOC detecting some situation that requires the AOC to request the RCC Operator to take over control and accountability. While the AOC waits for the RCC Operator to reply, the AOC continues to be in control and accountable. Then, three things may happen:

- The situation may be solved by the AOC, and the AOC can continue its operation.
- The RCC Operator takes over control and accountability, and the AOC goes to an idle state, meaning that it only collects information from sensors for possible presentation to the RCC Operator.



- If the RCC Operator fails to respond within the time out, the AOC will ensure that the ship goes to a fallback state.

The current state of the RCC Operator is not known at the time when the AOC requests the RCC Operator to take over control. When this request comes when the RCC operator is idle, he must get situational awareness before confirming the handover. This means that the notification about the handover must be received by the RCC Operator in time for him to react on the notification, get situational awareness, do some actions, and the ship to react accordingly.

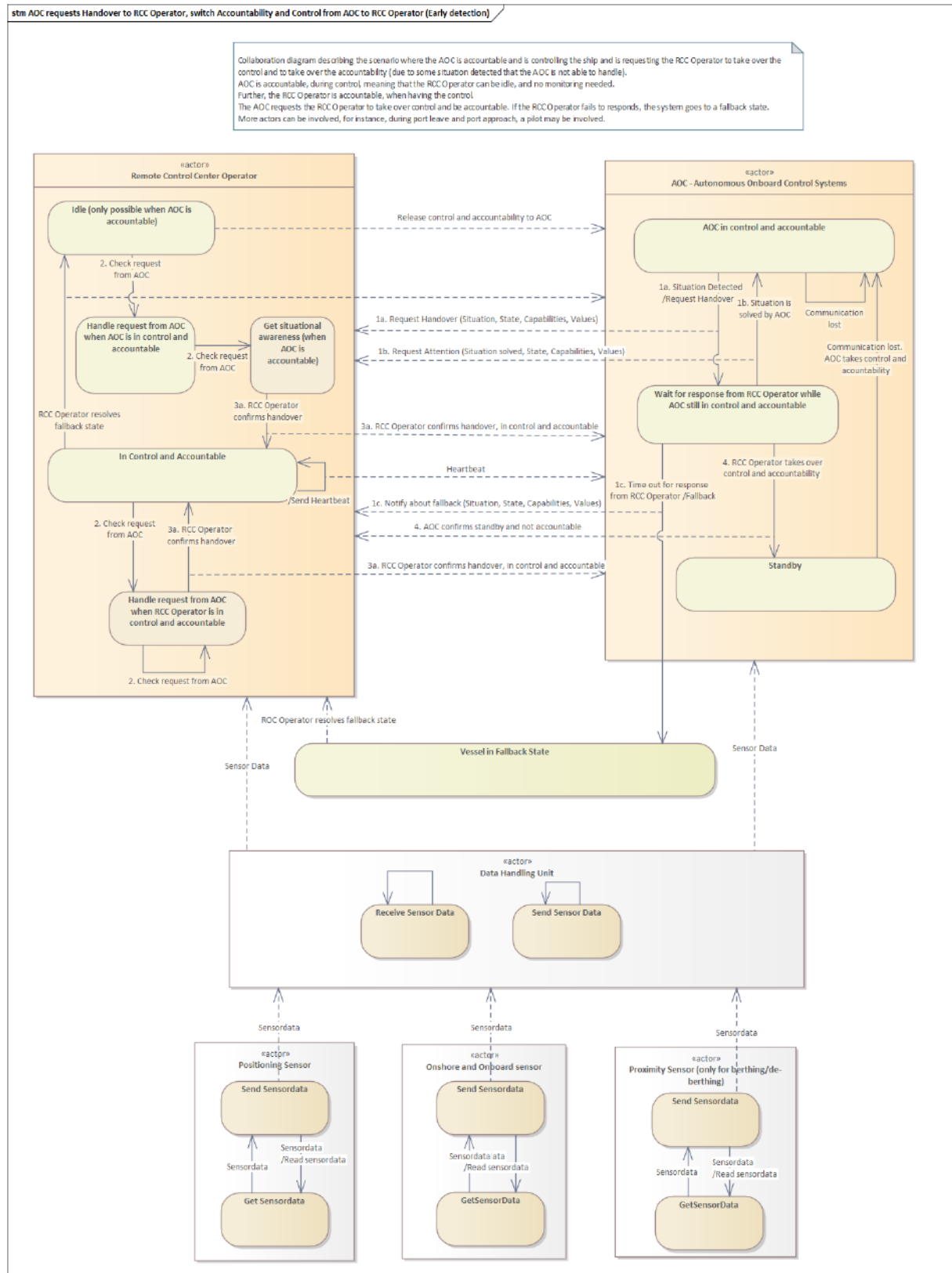


Figure 40: Diagram Component: Collaboration diagram for AOC requests Handover to RCC Operator, switch Accountability and Control from AOC to RCC Operator (Early detection)

Figure 41 shows the collaboration diagram when the AOC sends some information to the RCC Operator. The RCC Operator sends back a notification saying that the information has been received.

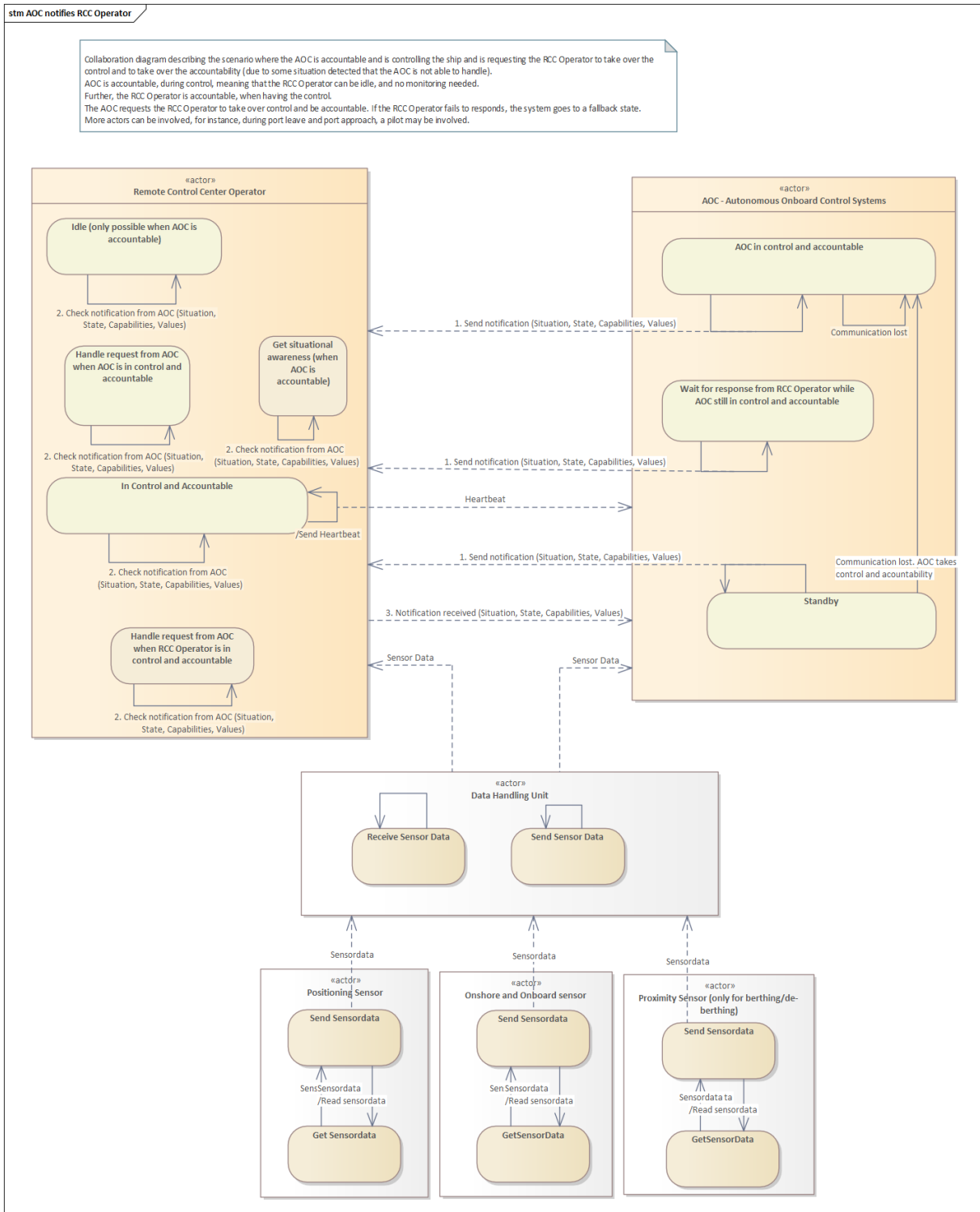


Figure 41: Diagram Component: Collaboration diagram for AOC notifies RCC Operator

Figure 42 shows the collaboration diagram when the RCC Operator takes control from the AOC, and AOC at the same time releases the control to the RCC Operator. Also, this diagram shows that the RCC Operator releases the control and accountability to the AOC.

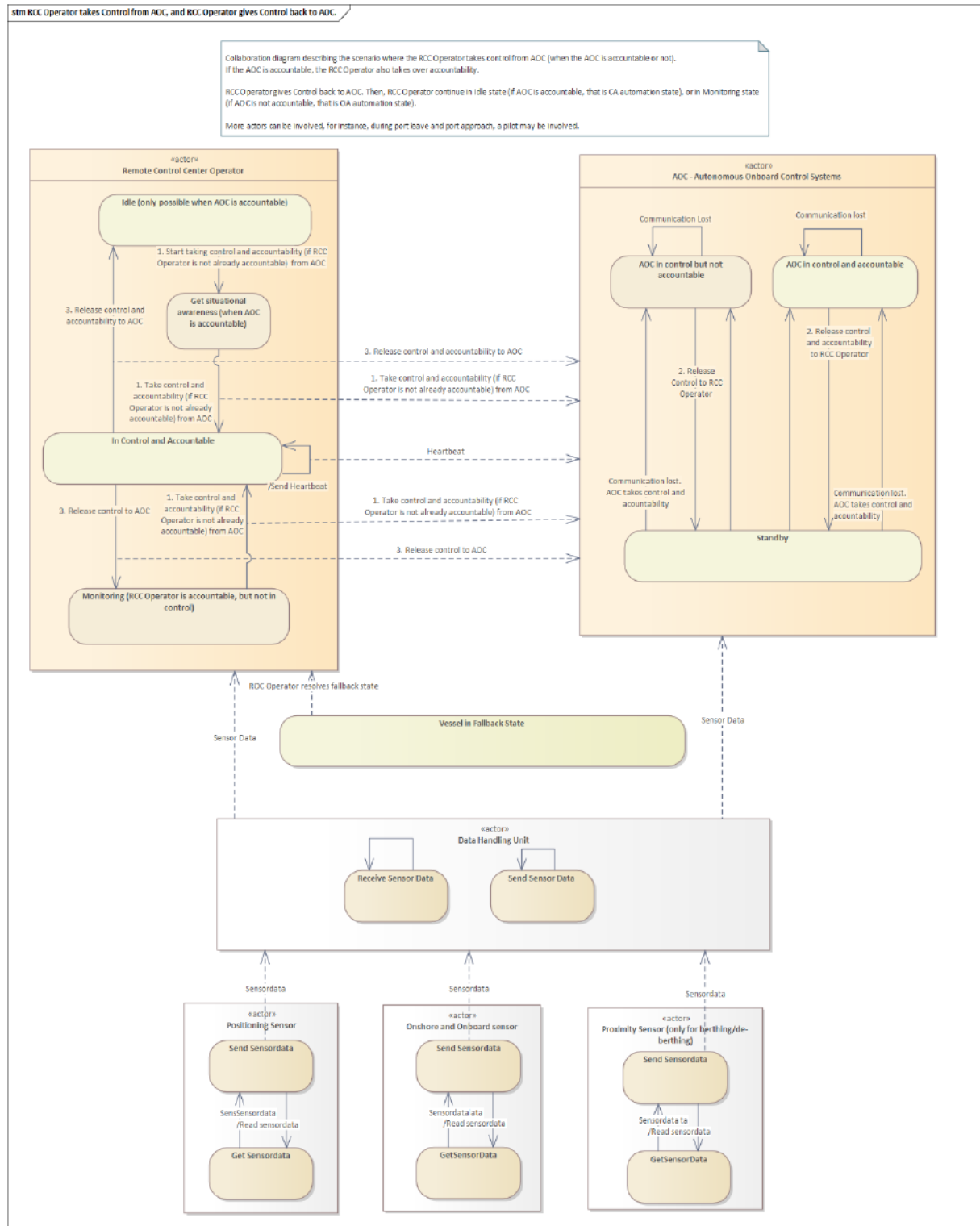


Figure 42: Diagram Component: Collaboration diagram for RCC Operator takes Control from AOC, and RCC Operator gives Control back to AOC

10.5.3 UML Sequence Diagram Components

The UML sequence diagrams in Figure 43, Figure 44, Figure 45, and Figure 46 shows the diagram components that can be used as building blocks when setting up sequence diagrams for the various System Control Tasks (SCTs).

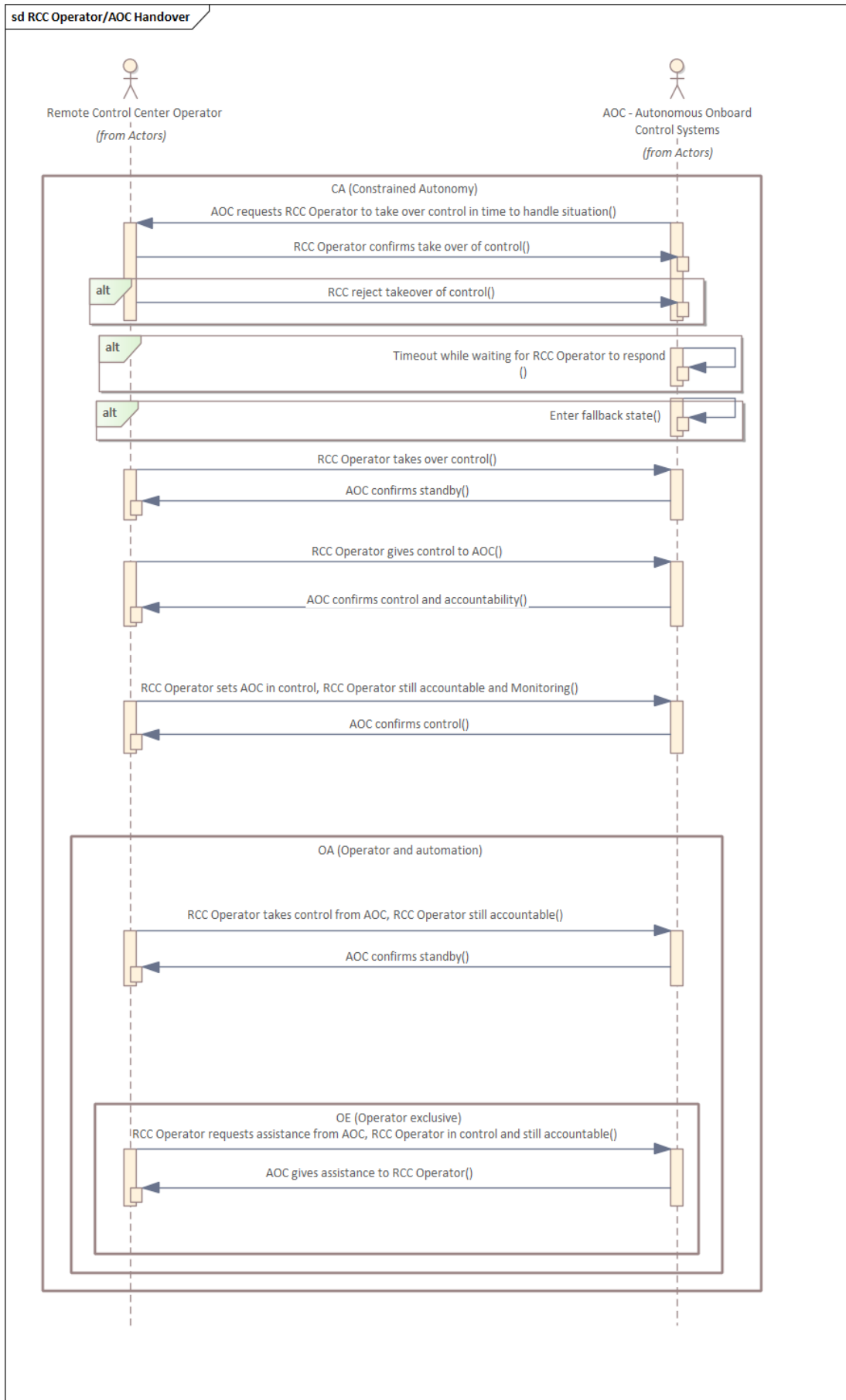


Figure 43: Diagram Component: Sequence diagram for RCC Operator/AOC Handover

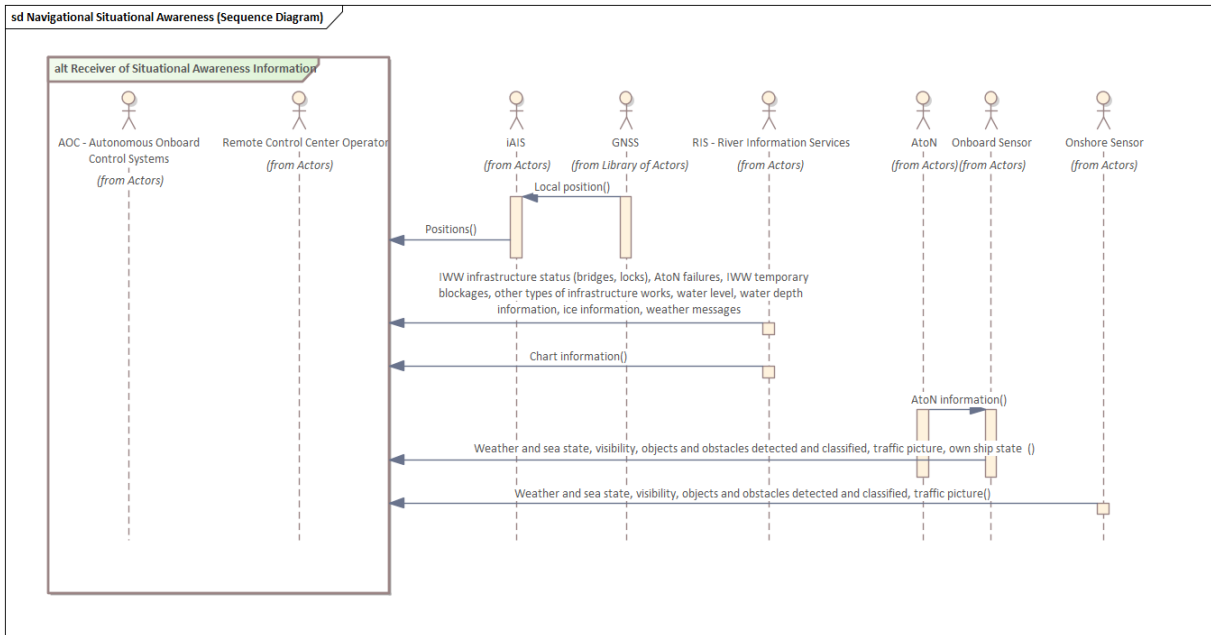


Figure 44: Diagram Component: Sequence Diagram for Navigational Situational Awareness

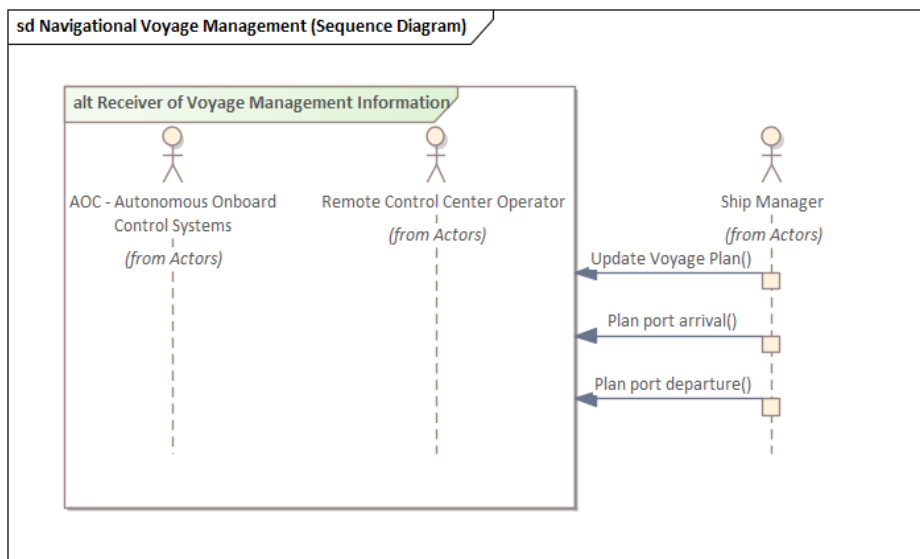


Figure 45: Diagram Component: Sequence diagram for Navigational Voyage Management

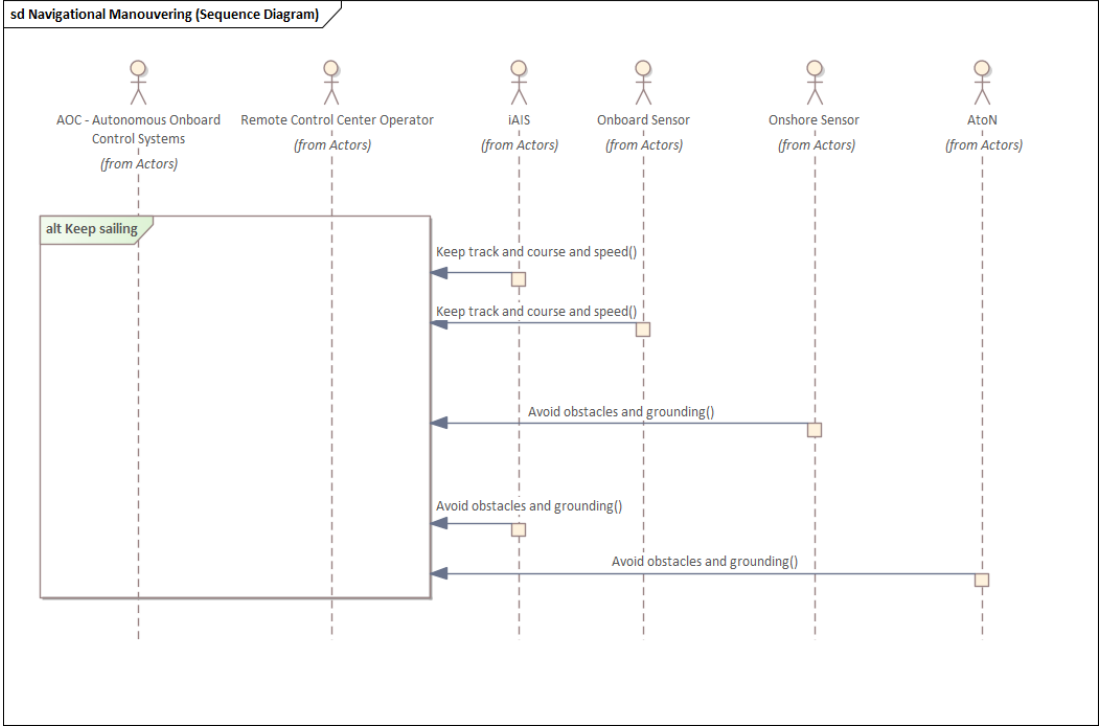


Figure 46: Diagram Component: Sequence diagram for Navigational Manoeuvring



11 Safety and Security Analysis

In our analysis we want to identify risks caused by both safety and security incidents. Overall risk is usually done by combining the likelihood and consequence of threats. In practice this can be done in several ways as already explained in Section 2.4, and we do not dictate what way is the "best", but show how established practices can be applied. We initially apply hazard analysis to explore the range of causes and consequences when losing control of the operational envelope. We then perform a more detailed analysis, focusing on intentional threats. This approach to threat analysis has already been explained in *D5.3 Safety and Security Analysis and Remedial Measures*. It is a structured approach that is tied with the design of the autonomous operations. We identify top level threats through misuse cases, and then use sequence diagrams to exemplify attack scenarios. This information is used to make informed estimations on likelihood for the threats. Finally, we make an overall assessment of the safety and security risks based on the analysis.

11.1 Exploring potential hazards

As shown in Section 2.4.1, we can use bow-tie diagrams to identify causes and consequences when one loses control over a hazard. In our case, this would be situations that are outside of the operational envelope and would trigger a fallback function to prevent the potential consequences.

Figure 47 shows such a diagram for SCT related to locks, such as SCT1 and SCT4. We have modelled both unintended causes (yellow) and intentional threats (blue). The consequences (red) can take place independently if the type of intent that could trigger the top event (orange). To simplify the analysis, we have not added preventive and reactive controls at this point.

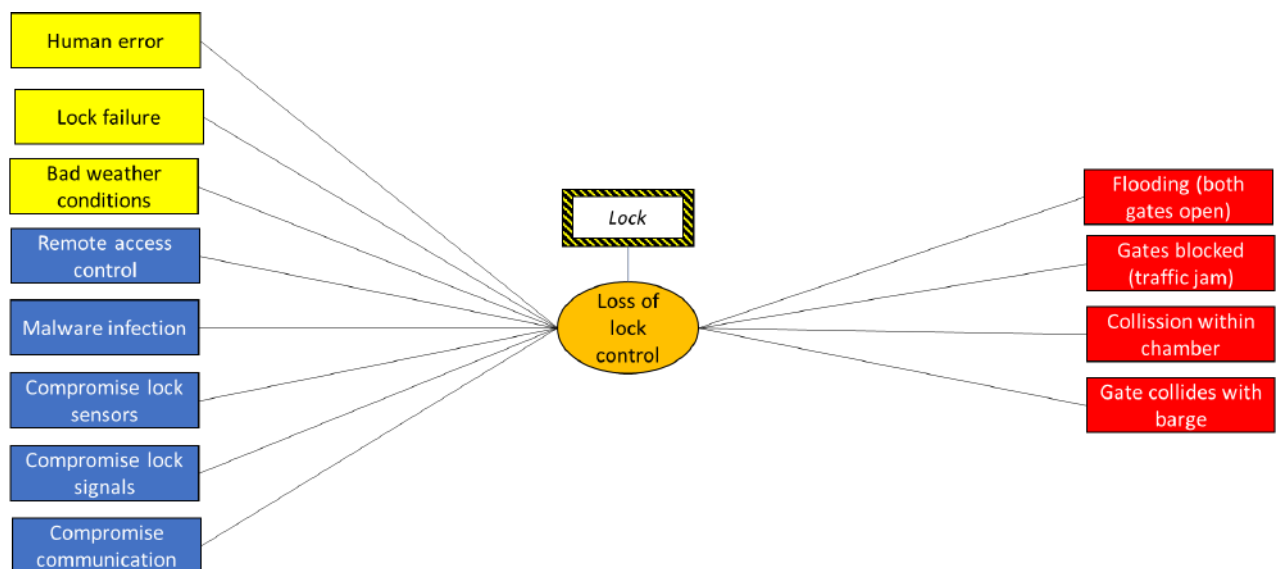


Figure 47: Causes and consequences of losing control during lock operations.

Figure 48 is about bridge operations relevant to SCT2, SCT3, and is very much similar to Figure 47 when looking at the left side of the bow-tie diagrams. However, the consequences are different as other types of traffic can be more directly affected.

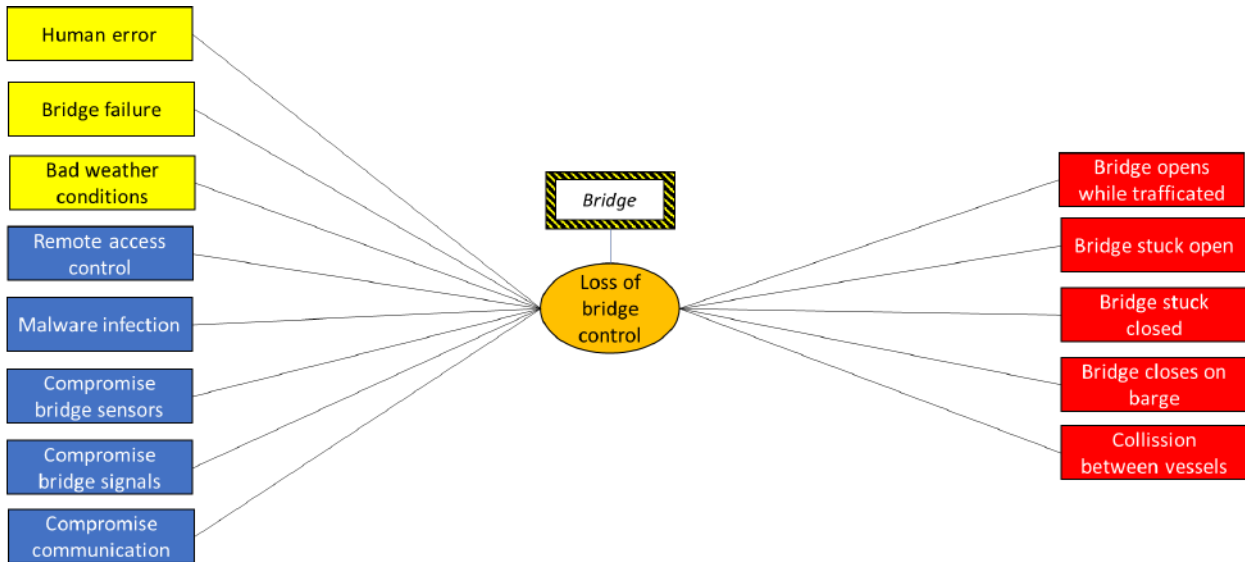


Figure 48: Causes and consequences of losing control during bridge operations.

With Figure 49, we have a generalized bow-tie diagram for navigation that can be related to most SCTs when the ship is sailing (SCT1-SCT8). Note that the consequences can have different levels of severity, e.g. blocking could have more impact in high traffic areas (close to port, bridge and lock) than under simple sailing conditions.

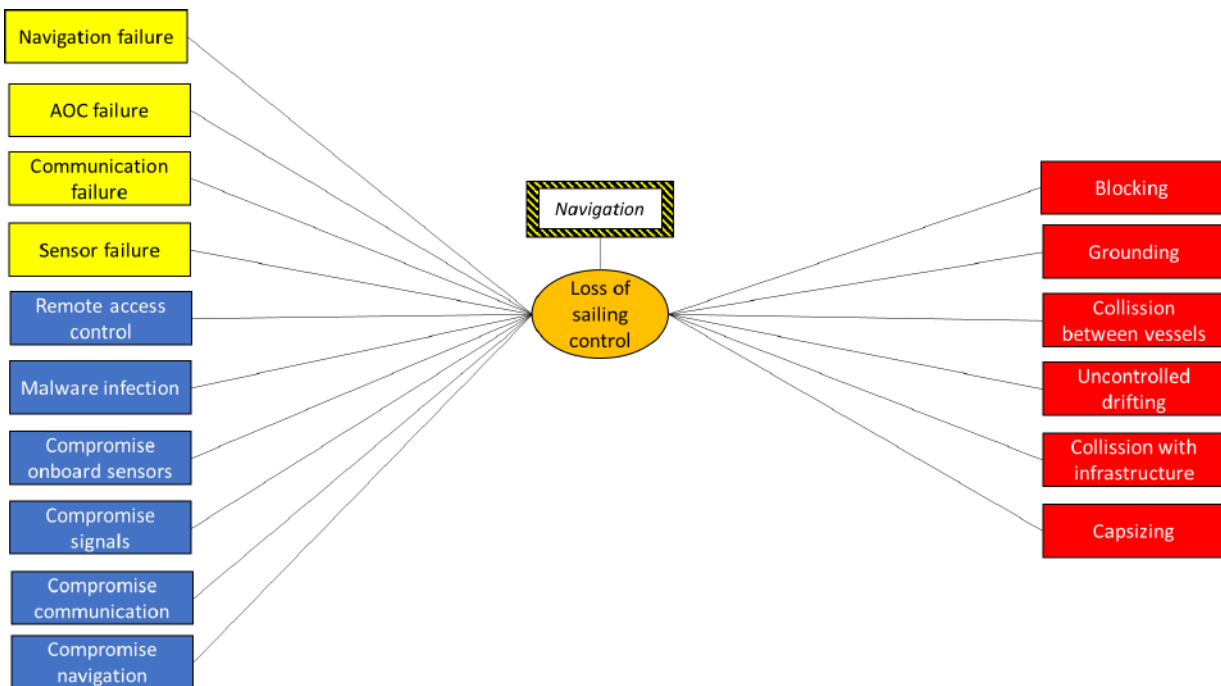


Figure 49: Causes and consequences of losing control during navigation (both simple and complex).

With our example mission, deck operations will take place either at a terminal or along the route. Figure 50 shows a bow-tie related to SCT9 and SCT10, where the barge is fixed, but still need to maintain some situational awareness while goods are being handled. Here, there may be humans more involved in the lashing and use of vehicles, and therefore there could be consequences related to injuries (or death) if there is loss of RoRo control.

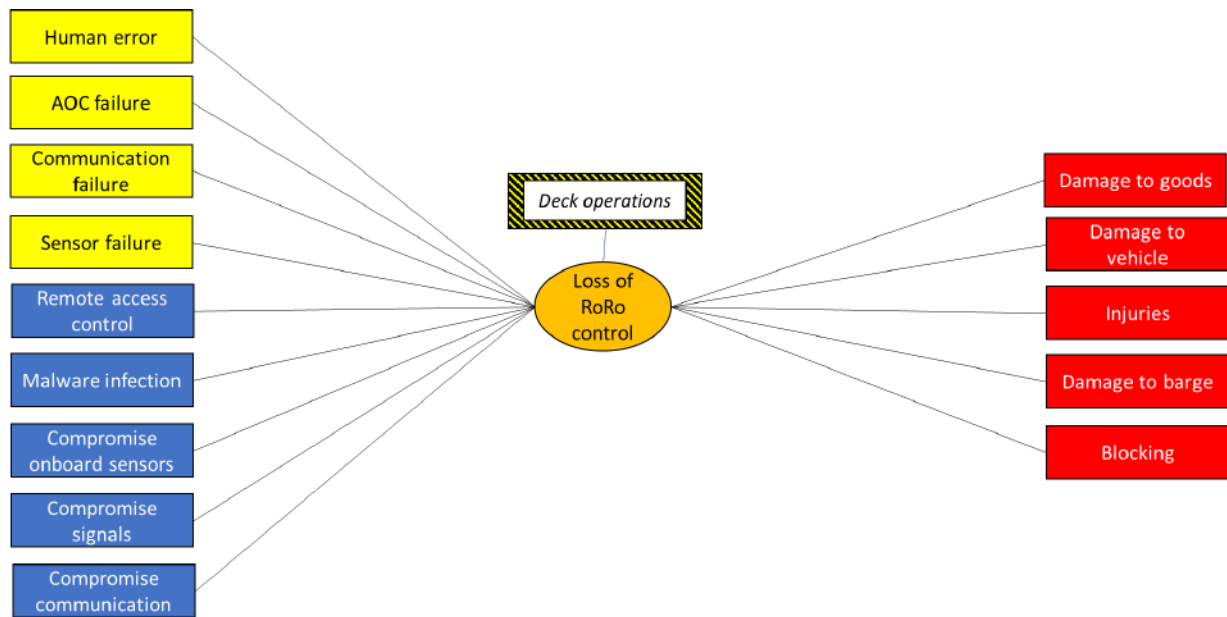


Figure 50: Causes and consequences of losing control during RoRo operations.

Related to SCT11-SCT14, we have the use of mooring (or anchoring) to secure the barge while queuing, inside lock chambers or when berthing. There are different types of mooring systems, but a number of possible causes to loss of control and consequences are shown in Figure 51.

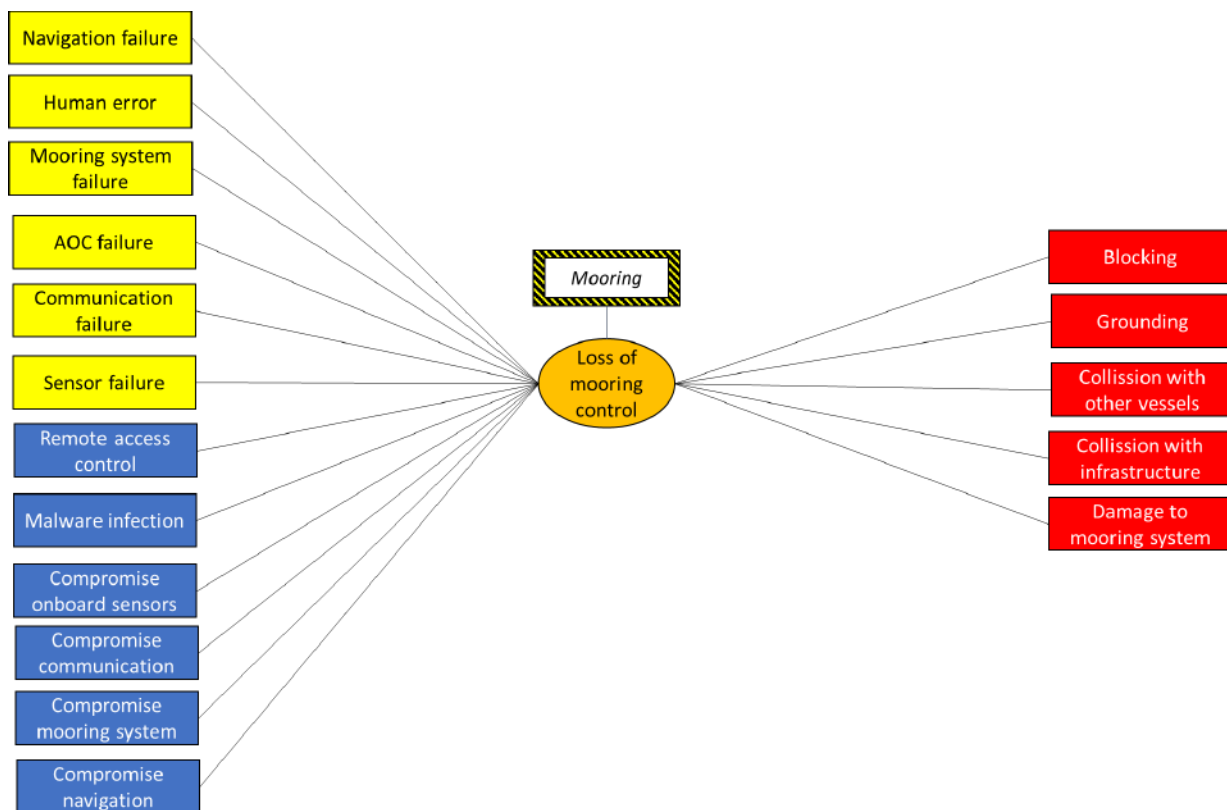


Figure 51: Causes and consequences of losing control during mooring operations.



11.2 Top-level Misuse Case

The top-level misuse case diagram in Figure 52 extends the use case diagram in Figure 15 defined for the mission with potential threats and associated threat actors. The threats are based on malicious intents, and there could be several attack intents towards the different mission phase patterns.

In the misuse case diagram, we have used notes to explain the rationale behind the intents. The associated threat actors are typical for these types of attack but could be performed by others as well. Note that we have not explicitly modelled any insider threat agents, but it should be kept in mind that in general many attacks are done in collaboration with insiders, e.g., information theft. Instead, we focus on threats and threat agents that are more specific to autonomous systems.

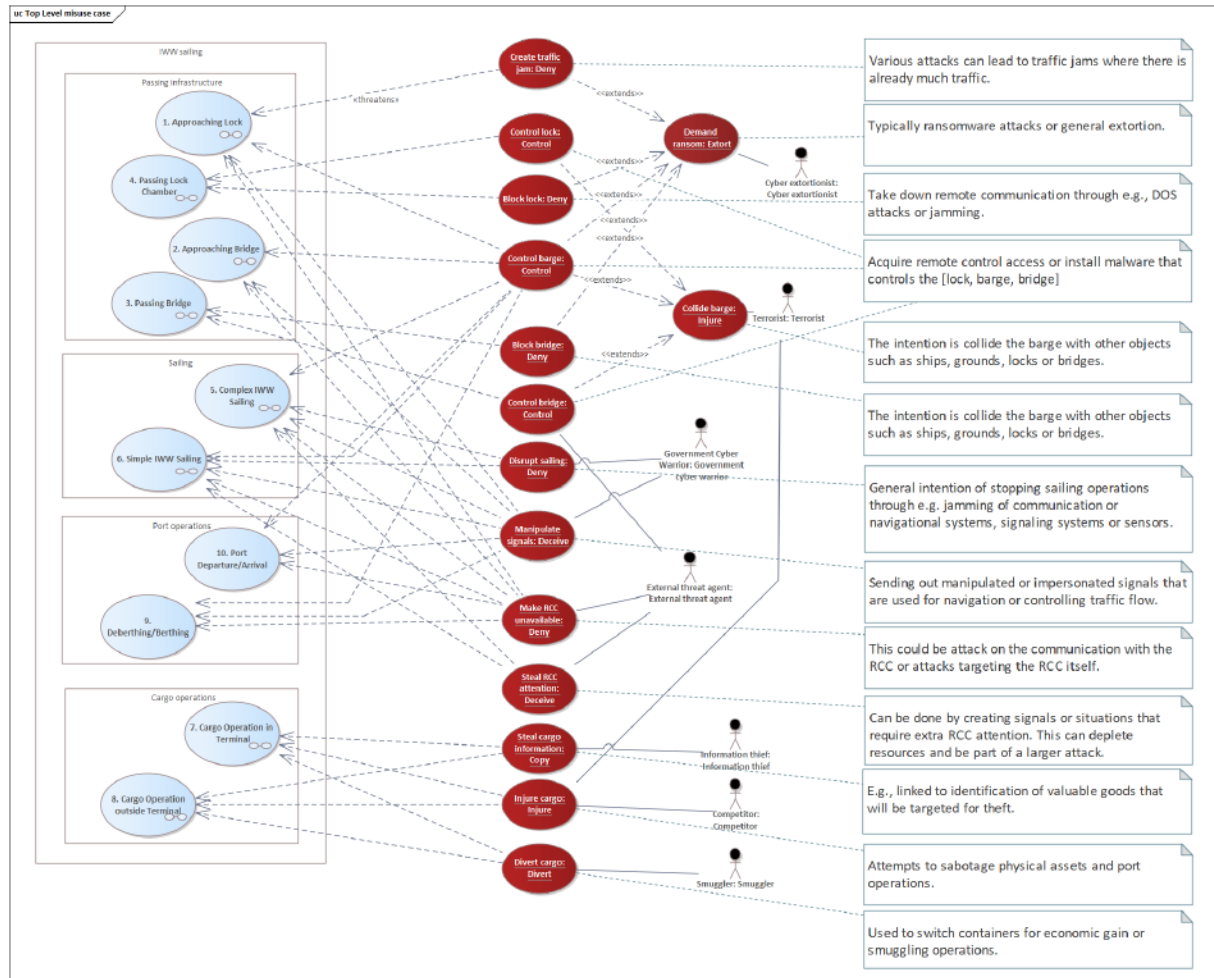


Figure 52: Top-level misuse case diagram

11.3 Mission Phase Pattern Threats

For each mission phase pattern, we have created a set of threat models based on UML-diagrams describing the normal behaviour of the system and the intents taken from the misuse case diagram. The point with these models is to show the variety of attack possibilities under different conditions and what threat actors would typically be involved. Note that these models are not complete, meaning that there might be other variants that are relevant as well. Each model includes attack scenarios that are feasible for certain intents in the different mission phase patterns. In order to avoid too much repetition, we refer to some of the same attack scenarios in several mission phase patterns.



11.3.1 Approaching Lock

When a barge approaches a lock, it will most likely have OA or OE as operational mode (see Table 7). In Figure 53, we have modelled attack scenarios where the intent is to deny this phase of the mission. This can efficiently be done by sending false lock passing request, sending false lock passing responses, invalid confirmations or through jamming communication between the AOC or RCC. All of these could lead to traffic jams or use of unnecessary resources to sort out fallback situations.

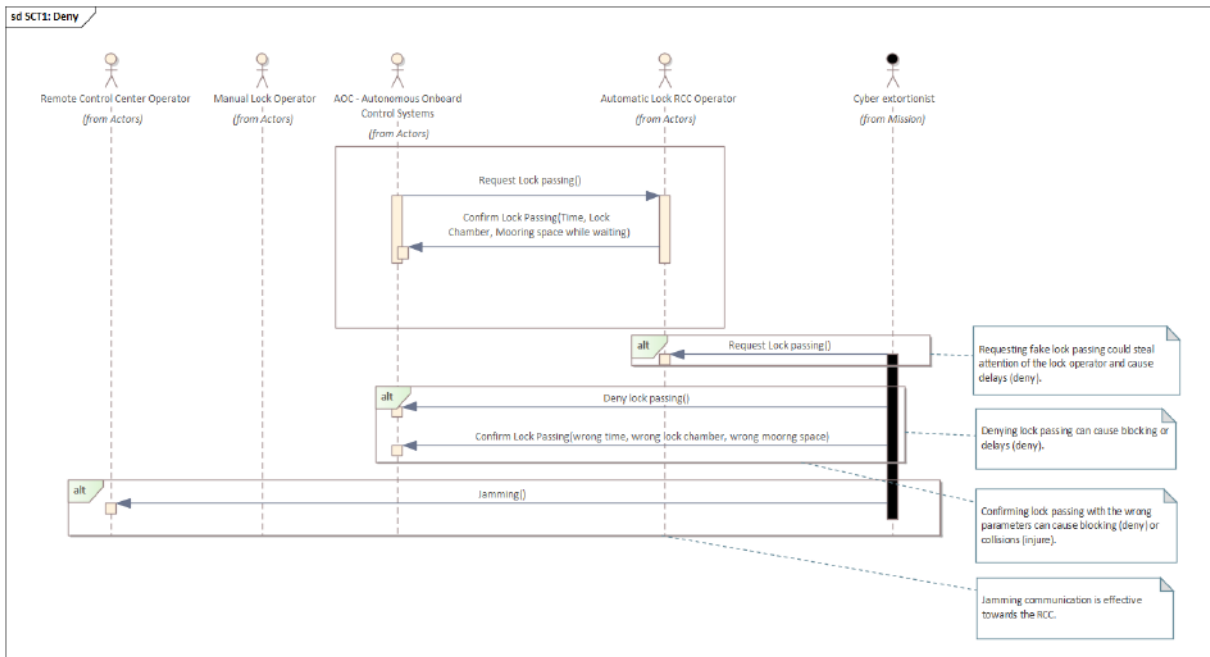


Figure 53: Variants of attack scenarios denying operations when approaching locks.

11.3.2 Approaching Bridge

Approaching a bridge has many similarities to approaching locks. Figure 54 shows attack scenarios where intentional misinformation, e.g., about e.g. the ship height above water, could cause denial of traffic or in the worst case a collision. Ships that need mooring could be denied this by someone impersonating as a RIS or bridge operator. Also, we have highlighted the many possibilities of jamming different actors.

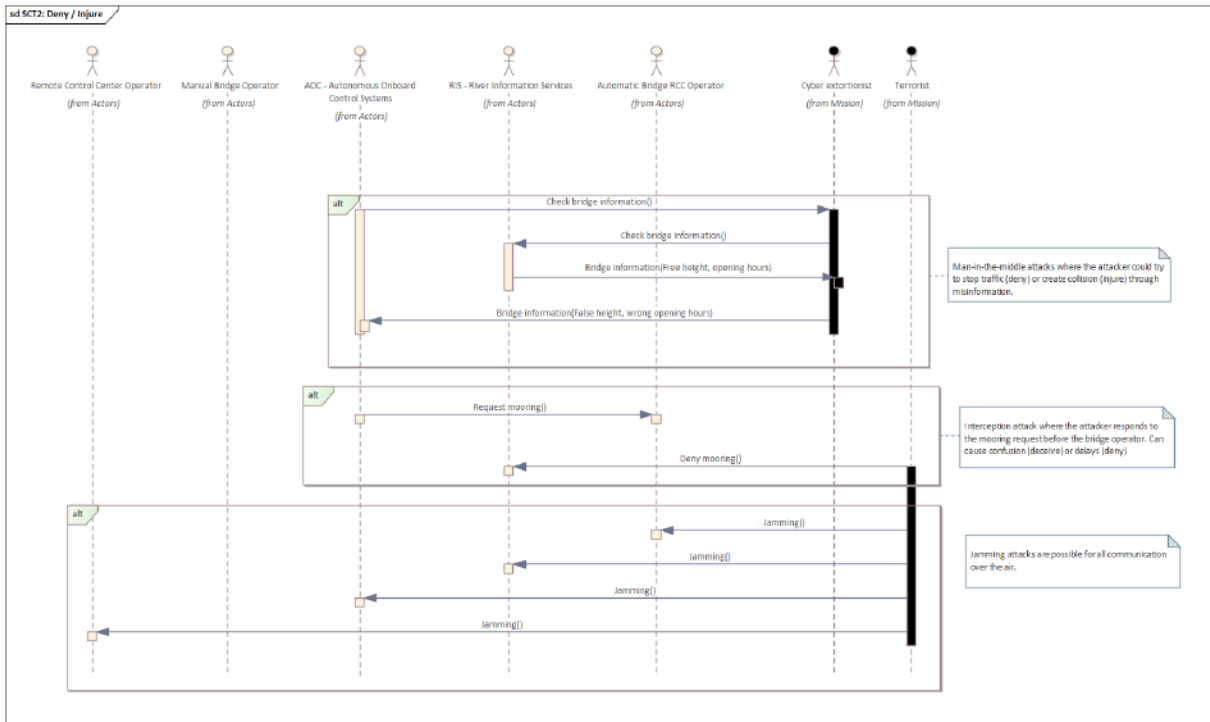


Figure 54: Attacks that could deny or injure operations when approaching a bridge.

11.3.3 Passing Bridge

When doing the actual bridge passing, there could be different types of attacks with the intent of causing injuries as shown in Figure 55. One could be to make the bridge operator lower it while there are barges passing. A terrorist could also take control of the iAIS system and send misleading control signals to the AOC. The RCC in control could also be misled by incorrect information about the bridge state.

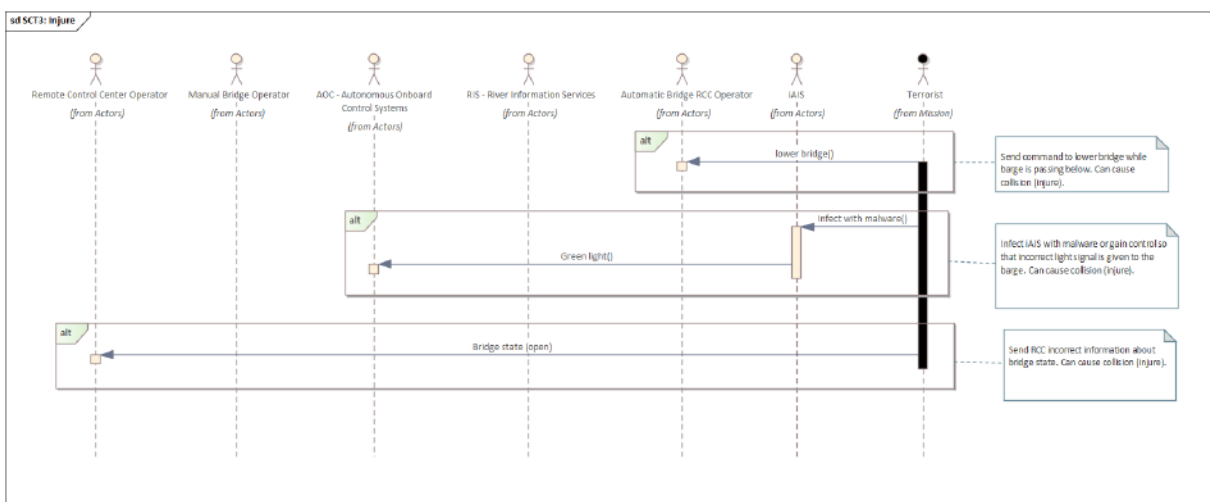


Figure 55: Attempts to cause injury to barges passing a bridge.



11.3.4 Passing Lock Chamber

Within the lock chamber, there could be attacks that target the lock systems as shown in Figure 56. From classical jamming, to taking control of the lock gates, sending wrong signals, misinformation, malware infections and possible combinations of all.

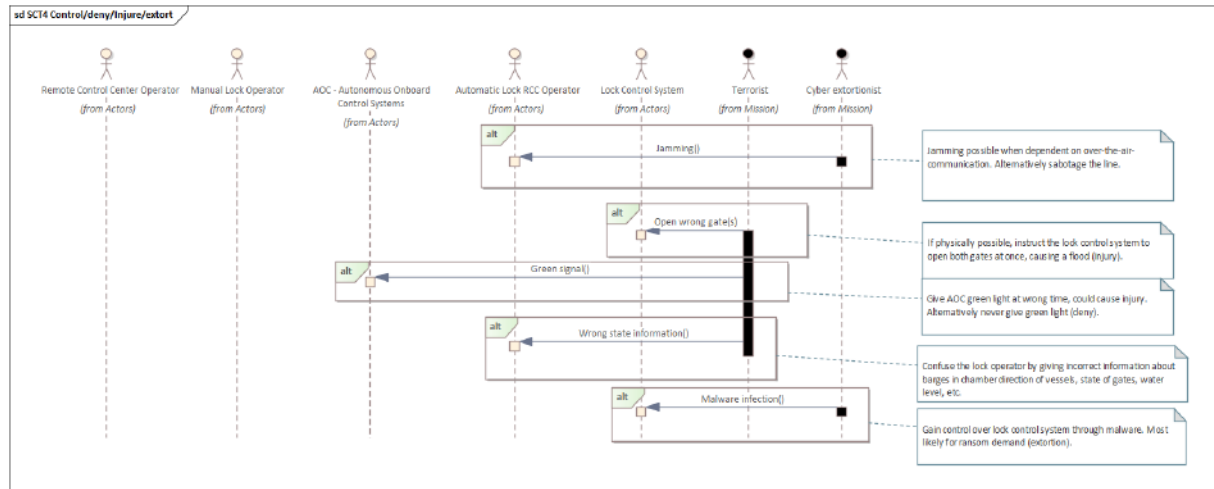


Figure 56: Attacks targeting the lock system.

11.3.5 Complex IWW Sailing

Most of the complex IWW sailing attack scenarios can be applied to all the other mission phase patterns as well. Here, we are looking at OA and OE modes, which are highly dependent on RCC attention, stable communications and interactions with the environment.

In Figure 57, we have simply shown that malware infections could take place both on the AOC and RCC side. Though the RCC side might be more probable based on higher exposure, the AOC will also need to be updated from time to time, leaving a window of opportunity in e.g., supply chain attacks. Also, any remote control operation will need secure authentication and authorisation to withstand attackers trying to exploit the remote control functionality.

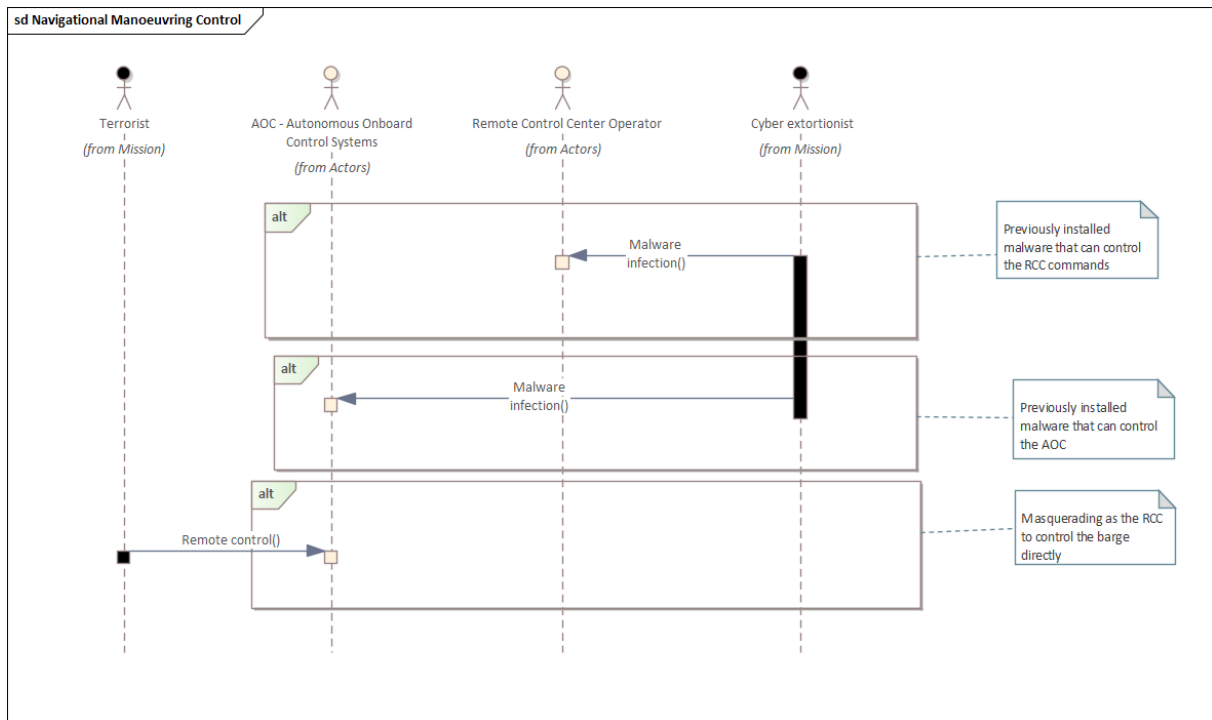


Figure 57: Attacks that could take control of the manoeuvring subprocess.

In Figure 58, we have highlighted scenarios for manipulating the signals and information that the manoeuvring subprocess depends on. This could be done directly or indirectly. For the latter, the attacker could send false ship information to the RIS, that subsequently gives a misleading traffic information picture to the AOC. This could trigger the AOC to request a unnecessary take over from the RCC. Furthermore, the attacker could corrupt beacon signals on mislead the onboard sensors to trigger fallbacks or take overs. Finally, GNSS spoofing is known attack technique that could lead to improper navigation.

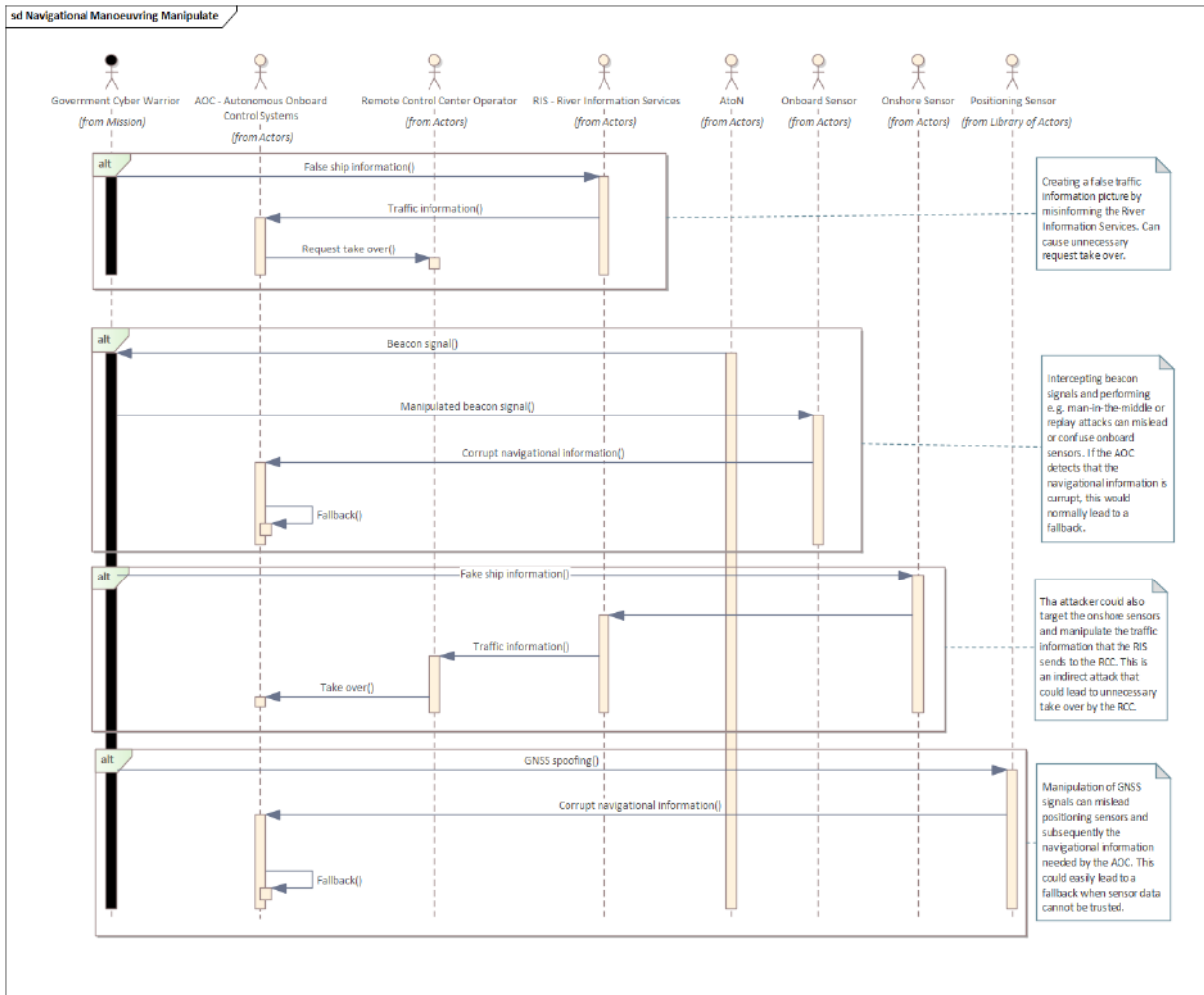


Figure 58: Attacks related to manipulating the manoeuvring subprocess.

The handover between the different modes of operation represents particular vulnerable transitions. In Figure 59, we have modelled variations of attack scenarios could either prevent handover, trigger unnecessary handovers or confuse the process, resulting in fallbacks.

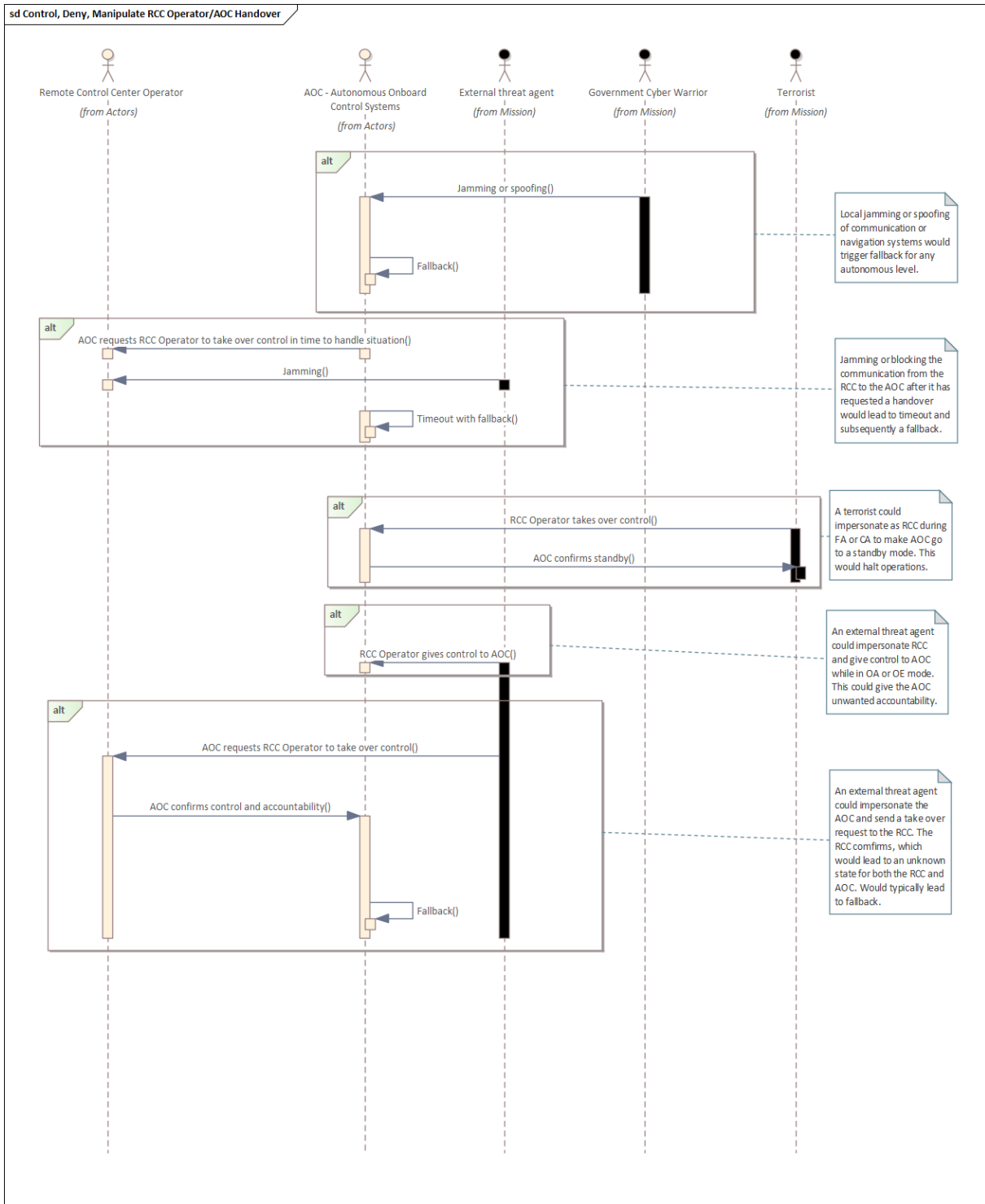


Figure 59: Various attack scenarios for RCC-AOC handover situations.

11.3.6 Simple IWW Sailing

Simple IWW sailing can be seen as a subcase of complex IWW sailing. There could be FA or CA modes of operation in addition to OA and OE, but that does not lead to additional attack scenarios worth highlighting.



11.3.7 Cargo Operation in Terminal

In Figure 60 we have modelled some scenarios where the barge is not moving, but only cargo operation is the main active process. We still see that there are possibilities for causing injury through remote control of AGVs handling the trailers. Also, there could be attacks related to information theft (e.g., cargo manifest). This information could be used as a source of information for physical attacks at a later stage. We have also included an attack scenario where tampered RoRo instructions are used to skip, shuffle or replace trailers. It can be foreseen that smugglers would have this kind of intention.

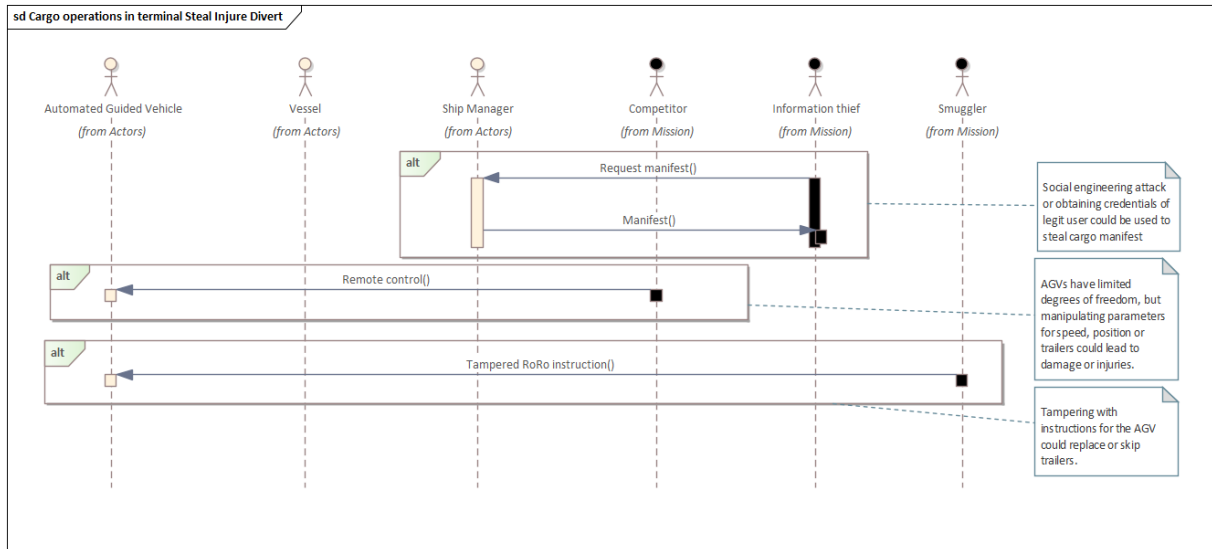


Figure 60: Attack scenarios while the barge is in a terminal.

11.3.8 Cargo Operation outside Main Terminals (foreseen)

For cargo operations outside the main terminal, we do not foresee any particular new attack scenarios, but the physical security of the area and systems might be less extensive, creating a higher exposure to cyber related attacks as well.

11.3.9 Deberthing/Berthing

This mission phase patterns will typically include subprocesses for mooring or anchoring the barge. The diagram in Figure 61 therefore show attack scenarios that could target the proximity sensors used during this operation. Also, classical jamming is relevant as real-time communication would be central for automated mooring systems. If the mooring is to be remotely controlled by someone at the port, this could lead to remote control attacks without proper local authentication and authorisation in place.

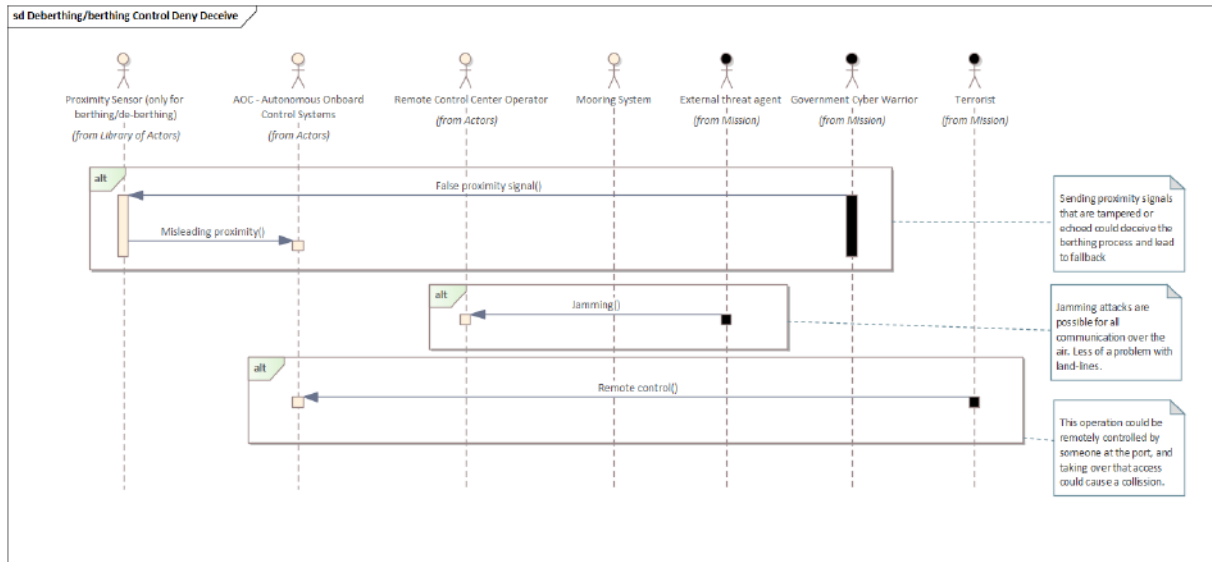


Figure 61: Attacks during deberthing/berthing.

11.3.10 Port Departure/Arrival

For port departure/arrival we foresee many of the same attack scenarios as for complex IWW sailing.

11.4 Likelihood Estimations

To estimate the likelihood of a successful cyberattack, a simple probabilistic approach based on statistics is generally not sufficient. Cyber-crime is a relatively new and rapidly evolving phenomenon, so existing information about past events has limited usability. Furthermore, cyber threats are mainly caused by intelligent actors with malicious intent, and attack likelihoods are therefore expected to be influenced by various factors. The proposed method for likelihood estimation for a given threat is based on the approach described in [33], where attack likelihood is estimated based on the following factors:

- **Threat actors:** The size of the group of potential threat actors influences the likelihood of an attack. In otherwise equivalent circumstances, a large group of actors represents a higher attack likelihood than a small group of actors. The term threat actor is not reserved for those with malicious intent, it includes all relevant actors who may become involved in an attack.
- **Opportunities:** The likelihood of a given attack mission also depends on how favourable the circumstances are for an attack. A weighted average is determined based on the threat actor's spatial opportunity (is the location of relevant equipment and/or actors to the attacker's advantage?), temporal opportunity (does the timing increase the likelihood of a successful attack?) and vulnerability exploiting opportunity (what vulnerabilities does the victim or target have that the attacker can exploit?).
- **Means:** This likelihood factor describes the degree to which an attacker has the necessary means to perform an attack, and this is mainly influenced by competence as well as technological and financial resources.
- **Motivation:** A weighted average is assigned based on the threat actor's motivation and intent. Motivation depends greatly on the expected reward (from the attacker's perspective) in case of a successful attack.



This method is in accordance with the axiom by Ross Anderson [21] that “One of the first things the security engineer needs to do when tackling a new problem is to identify the likely opponents” and “...what sort of capabilities will the adversaries have, and what motivation?”. For each identified threat, the first step is to identify relevant threat actors which might be involved in an attack. This is known as an attacker centric approach [34] to threat modelling.

When the possible threat actors have been identified, the next step is to assign a weight (relative number between 0 and 10) to each likelihood factor, for each threat actor. The likelihood value for a given threat actor is the average of the likelihood factors for that threat actor, and the overall likelihood value for a threat is defined as the highest (worst-case) likelihood value among the potential threat actors. The likelihood factors are typically estimated based on input from security experts, domain specialists and available documentation, in this case the operational envelope.

Based on the threat models for our use case, estimated values for threat actors, opportunity (mapped to mission phase pattern), means and motivation (intent) have been summarised in Table 8. The elements of this table are based on the top-level misuse case (presented in Section 11.2).

Table 8: Threat summary table.

Threat actor			Opportunity			Means		Motivation			Average weight
Who	Relative size weight	Justification	Opportunity	Opportunity weight	Justification	Means assessment	Means weight	Motivation (Intent)	Motivation weight	Justification	
Cyber extortionist	8	There are many known and unknown groups financing their illegal activities through ransomware and other means of extortion.	Approaching lock	3	Limited time window, 4 locks during voyage	Various attacks can be performed cheaply.	7	Create traffic jam (deny)	4	Potential reward, but small scale.	5,5
Cyber extortionist	8	There are many known and unknown groups financing their illegal activities through ransomware and other means of extortion.	Passing lock chamber	3	Limited time window, 4 locks during voyage	Various attacks can be performed cheaply.	7	Block lock (deny)	4	Potential reward, but small scale.	5,5
Cyber extortionist	8	There are many known and unknown groups financing their illegal activities through ransomware and other means of extortion.	Approaching lock	3	Limited time window, 4 locks during voyage	Should be expensive to take control.	4	Control barge (control)	3	Little reward for single barge. More for multiple.	4,5
Cyber extortionist	8	There are many known and unknown groups financing their illegal activities through ransomware and other means of extortion.	Approaching bridge	2	Limited time window, 2 bridges, but only one needs to be raised.	Should be expensive to take control.	4	Control barge (control)	3	Little reward for single barge. More for multiple.	4,25
Cyber extortionist	8	There are many known and unknown groups financing their illegal activities through	Complex IWW sailing	7	Majority of voyage	Should be expensive to take control.	4	Control barge (control)	3	Little reward for single barge.	5,5



Threat actor			Opportunity			Means		Motivation			Average weight
Who	Relative size weight	Justification	Opportunity	Opportunity weight	Justification	Means assessment	Means weight	Motivation (Intent)	Motivation weight	Justification	
		ransomware and other means of extortion.								More for multiple.	
Cyber extortionist	8	There are many known and unknown groups financing their illegal activities through ransomware and other means of extortion.	Simple IWW sailing	3	During special safe conditions, minor part of voyage.	Should be expensive to take control.	4	Control barge (control)	3	Little reward for single barge. More for multiple.	4,5
Cyber extortionist	8	There are many known and unknown groups financing their illegal activities through ransomware and other means of extortion.	Port departure/arrival	4	Two main areas, many systems to exploit	Should be expensive to take control.	4	Control barge (control)	3	Little reward for single barge. More for multiple.	4,75
Cyber extortionist	8	There are many known and unknown groups financing their illegal activities through ransomware and other means of extortion.	Deberthing/berting	4	Two main areas, low speed, several systems	Should be expensive to take control.	4	Control barge (control)	3	Little reward for single barge. More for multiple.	4,75
Cyber extortionist	8	There are many known and unknown groups financing their illegal activities through ransomware and other means of extortion.	Passing bridge	2	Limited time window, 2 bridges, but only one needs to be raised.	Various attacks can be performed cheaply.	7	Block bridge (deny)	5	Potential reward, medium scale.	5,5
Cyber extortionist	8	There are many known and unknown groups financing their illegal activities through ransomware and other means of extortion.	Traffic jam, block lock, control barge, block bridge	7	Highest value from given situations	More expensive to write OT malware.	3	Demand ransom (extort)	5	Highest value for given actor.	5,75
Terrorist	2	There are not so many active terrorist organisations targeting shipping operations.	Passing lock chamber	3	Limited time window, 4 locks during voyage	Should be expensive to take control.	4	Control lock (control)	7	High damage potential.	4
Terrorist	2	There are not so many active terrorist organisations targeting shipping operations.	Approaching lock	3	Limited time window, 4 locks during voyage	Should be expensive to take control.	4	Control barge (control)	5	Medium damage potential.	3,5
Terrorist	2	There are not so many active terrorist organisations targeting shipping operations.	Approaching bridge	2	Limited time window, 2 bridges, but only one needs to be raised.	Should be expensive to take control.	4	Control barge (control)	5	Medium damage potential.	3,25



Threat actor			Opportunity			Means		Motivation			
Who	Relative size weight	Justification	Opportunity	Opportunity weight	Justification	Means assessment	Means weight	Motivation (Intent)	Motivation weight	Justification	Average weight
Terrorist	2	There are not so many active terrorist organisations targeting shipping operations.	Complex IWW sailing	7	Majority of voyage	Should be expensive to take control.	4	Control barge (control)	5	Medium damage potential.	4,5
Terrorist	2	There are not so many active terrorist organisations targeting shipping operations.	Simple IWW sailing	3	During special safe conditions, minor part of voyage.	Should be expensive to take control.	4	Control barge (control)	5	Medium damage potential.	3,5
Terrorist	2	There are not so many active terrorist organisations targeting shipping operations.	Port departure/arrival	4	Two main areas, many systems to exploit	Should be expensive to take control.	4	Control barge (control)	5	Medium damage potential.	3,75
Terrorist	2	There are not so many active terrorist organisations targeting shipping operations.	Deberthing/berting	4	Two main areas, low speed, several systems	Should be expensive to take control.	4	Control barge (control)	5	Medium damage potential.	3,75
Terrorist	2	There are not so many active terrorist organisations targeting shipping operations.	Passing bridge	2	Limited time window, 2 bridges, but only one needs to be raised.	Should be expensive to take control.	4	Control bridge (control)	7	High damage potential.	3,75
Terrorist	2	There are not so many active terrorist organisations targeting shipping operations.	Control lock, control barge, control bridge	7	Highest value from given situations	Should be expensive to override safety mechanisms.	3	Collide barge (injure)	6	High damage potential, but depends on size of barge.	4,5
Terrorist	2	There are not so many active terrorist organisations targeting shipping operations.	Cargo operations in terminal	8	Can be done at any time	Should be expensive to override safety mechanisms.	3	Injure cargo (injure)	5	Minor damage, increases with human injury.	4,5
Terrorist	2	There are not so many active terrorist organisations targeting shipping operations.	Cargo operations outside terminal	3	Can only be done when barge is docked	Should be expensive to override safety mechanisms.	3	Injure cargo (injure)	5	Minor damage, increases with human injury.	3,25
Government cyber warrior	6	There are state sponsored groups in operation in Europe, especially with the current Russian aggression.	Complex IWW sailing	7	Majority of voyage	Fairly cheap to disrupt communication or navigation.	7	Disrupt sailing (deny)	4	Temporary retribution.	6
Government cyber warrior	6	There are state sponsored groups in operation in Europe, especially with the current Russian aggression.	Simple IWW sailing	3	During special safe conditions, minor part of voyage.	Fairly cheap to disrupt communication or navigation.	7	Disrupt sailing (deny)	4	Temporary retribution.	5
Government cyber warrior	6	There are state sponsored groups in operation in Europe, especially with the	Approaching lock	3	Limited time window, 4 locks during voyage	fairly cheap to hack signalling systems	6	Manipulate signals (deceive)	4	Steal attention, gain publicity	4,75



Threat actor			Opportunity			Means		Motivation			Average weight
Who	Relative size weight	Justification	Opportunity	Opportunity weight	Justification	Means assessment	Means weight	Motivation (Intent)	Motivation weight	Justification	
		current Russian aggression.									
Government cyber warrior	6	There are state sponsored groups in operation in Europe, especially with the current Russian aggression.	Approaching bridge	2	Limited time window, 2 bridges, but only one needs to be raised.	fairly cheap to hack signalling systems	6	Manipulate signals (deceive)	4	Steal attention, gain publicity	4,5
Government cyber warrior	6	There are state sponsored groups in operation in Europe, especially with the current Russian aggression.	Complex IWW sailing	7	Majority of voyage	fairly cheap to hack signalling systems	6	Manipulate signals (deceive)	4	Steal attention, gain publicity	5,75
Government cyber warrior	6	There are state sponsored groups in operation in Europe, especially with the current Russian aggression.	Simple IWW sailing	3	During special safe conditions, minor part of voyage.	fairly cheap to hack signalling systems	6	Manipulate signals (deceive)	4	Steal attention, gain publicity	4,75
Government cyber warrior	6	There are state sponsored groups in operation in Europe, especially with the current Russian aggression.	Port departure/arrival	4	Two main areas, many systems to exploit	fairly cheap to hack signalling systems	6	Manipulate signals (deceive)	4	Steal attention, gain publicity	5
Government cyber warrior	6	There are state sponsored groups in operation in Europe, especially with the current Russian aggression.	Deberthing/berthing	4	Two main areas, low speed, several systems	fairly cheap to hack signalling systems	6	Manipulate signals (deceive)	2	Steal attention, gain publicity	4,5
External threat agent	5	Uncertain number of wildcard agents, given an average score.	Passing bridge	2	Limited time window, 2 bridges, but only one needs to be raised.	Should be expensive to take control.	4	Control bridge (control)	2	No real motivation	3,25
External threat agent	5	Uncertain number of wildcard agents, given an average score.	Approaching lock	3	Limited time window, 4 locks during voyage	Cheap to block communication	7	Make RCC unavailable (deny)	2	No real motivation	4,25
External threat agent	5	Uncertain number of wildcard agents, given an average score.	Approaching bridge	2	Limited time window, 2 bridges, but only one needs to be raised.	Cheap to block communication	7	Make RCC unavailable (deny)	2	No real motivation	4
External threat agent	5	Uncertain number of wildcard agents, given an average score.	Complex IWW sailing	7	Majority of voyage	Cheap to block communication	7	Make RCC unavailable (deny)	2	No real motivation	5,25
External threat agent	5	Uncertain number of wildcard agents, given an average score.	Simple IWW sailing	3	During special safe conditions, minor part of voyage.	Cheap to block communication	7	Make RCC unavailable (deny)	2	No real motivation	4,25



Threat actor			Opportunity			Means		Motivation			Average weight
Who	Relative size weight	Justification	Opportunity	Opportunity weight	Justification	Means assessment	Means weight	Motivation (Intent)	Motivation weight	Justification	
External threat agent	5	Uncertain number of wildcard agents, given an average score.	Port departure/arrival	4	Two main areas, many systems to exploit	Cheap to block communication	7	Make RCC unavailable (deny)	2	No real motivation	4,5
External threat agent	5	Uncertain number of wildcard agents, given an average score.	Deberthing/berthing	4	Two main areas, low speed, several systems	Cheap to block communication	7	Make RCC unavailable (deny)	2	No real motivation	4,5
External threat agent	5	Uncertain number of wildcard agents, given an average score.	Complex IWW sailing	7	Majority of voyage	Somewhat expensive to breach message integrity	5	Steal RCC attention (deceive)	2	No real motivation	4,75
External threat agent	5	Uncertain number of wildcard agents, given an average score.	Simple IWW sailing	3	During special safe conditions, minor part of voyage.	Somewhat expensive to breach message integrity	5	Steal RCC attention (deceive)	2	No real motivation	3,75
Information thief	4	Most likely insiders, a few on the outside of organisations.	Cargo operations in terminal	8	Can be done at any time	Somewhat expensive to breach message confidentiality or steal identity	5	Steal cargo information (copy)	2	Limited reward	4,75
Information thief	4	Most likely insiders, a few on the outside of organisations.	Cargo operations outside terminal	3	Can only be done when barge is docked	Somewhat expensive to breach message confidentiality or steal identity	5	Steal cargo information (copy)	2	Limited reward	3,5
Competitor	2	There is a limited number of competitors.	Cargo operations in terminal	8	Can be done at any time	Sophisticated and expensive attack	3	Injure cargo (injure)	3	Potentially damage reputation to gain market share.	4
Competitor	2	There is a limited number of competitors.	Cargo operations outside terminal	3	Can only be done when barge is docked	Sophisticated and expensive attack	3	Injure cargo (injure)	3	Potentially damage reputation to gain market share.	2,75
Smuggler	3	There are several smugglers related to shipping, but not that active for IWW.	Cargo operations in terminal	8	Can be done at any time	Sophisticated and expensive attack	4	Divert cargo (divert)	2	Less reward for doing this for IWW.	4,25



Threat actor			Opportunity			Means		Motivation			Average weight
Who	Relative size weight	Justification	Opportunity	Opportunity weight	Justification	Means assessment	Means weight	Motivation (Intent)	Motivation weight	Justification	
Smuggler	3	There are several smugglers related to shipping, but not that active for IWW.	Cargo operations outside terminal	3	Can only be done when barge is docked	Sophisticated and expensive attack, but less protected outside of terminal	5	Divert cargo (divert)	2	Less reward for doing this for IWW.	3,25

Note that the numerical values in the threat summary table are relative numbers, and not absolute values. Instead, they give an indication on the ranking of the threats. If we consider the top 9 threats based on the average weight values, we get the results shown in Table 9. We see that government warriors disrupting sailing (deny) during complex IWW is the highest ranked with an average weight of 6. In fact, government cyber warrior is identified as the typical threat actors in 4 out of the top 9 threats. Complex IWW sailing is also among 4 out of 9 opportunities. The deny intention appears in 6 out of 9 motivations.

Table 9: Top 9 threats.

Who	Opportunity	Means assessment	Motivation (Intent)	Average weight
Government cyber warrior	Complex IWW sailing	Fairly cheap to disrupt communication or navigation.	Disrupt sailing (deny)	6
Government cyber warrior	Complex IWW sailing	Fairly cheap to hack signalling systems	Manipulate signals (deceive)	5,75
Cyber extortionist	Approaching lock	Various attacks can be performed cheaply.	Create traffic jam (deny)	5,5
Cyber extortionist	Passing lock chamber	Various attacks can be performed cheaply.	Block lock (deny)	5,5
Cyber extortionist	Complex IWW sailing	Should be expensive to take control.	Control barge (control)	5,5
Cyber extortionist	Passing bridge	Various attacks can be performed cheaply.	Block bridge (deny)	5,5
External threat agent	Complex IWW sailing	Cheap to block communication	Make RCC unavailable (deny)	5,25
Government cyber warrior	Simple IWW sailing	Fairly cheap to disrupt communication or navigation.	Disrupt sailing (deny)	5
Government cyber warrior	Port departure/arrival	Fairly cheap to hack signalling systems	Manipulate signals (deceive)	5

11.5 Overall Result of the Analysis

For the overall results of the analysis, we reconsider the bow-tie diagrams by mapping the top-ranked threats to lookup consequences. In cases where we do not find corresponding consequences, we simply make additions. For the analysis of this mission example, we have not ranked or quantified unintentional threats or causes to loss of control. This can be done based on historical (frequency) data (when and where available) as suggested by the FSA guidelines or expert opinion as well. The result of the analysis yields the following:

- During **Complex IWW sailing**, there is a high probability of threat agents such as **government cyber warriors** will try to **disrupt** (1) sailing by denying/blocking communication and



navigation systems. A typical consequence of this could be **blocking** of the waterways. In this phase, there is also a high probability that the same type of threat actors could try to **manipulate** signalling systems (AtoN) to **deceive** navigation (2). Here, worst case consequences could be **collisions** between vessels or **grounding**. Also, there is a medium probability for **cyber extortionists** using malware infections to take **control** of the barge in order to demand **ransom** (3), possibly letting the barge drift without control. Another medium probability is that unknown **external threat agents** could make communication with the RCC unavailable by **denying** communication (4), leading to **blocking** of the waterways.

- When **approaching a lock**, there is a medium probability that **cyber extortionists** can use attacks involving fake requests to the lock operator, fake denials of lock passing or jamming. The consequences will typically be **denial** of service (5) causing **traffic jams** in these congested zones.
- When **passing the lock chamber**, there is a medium probability that **cyber extortionists** will jam communication with the lock operator or try to infect the lock control system with malware, effectively leading to **denial** of service (6).
- When **passing bridges**, there is a medium probability that **cyber extortionists** will jam communication or send misleading messages to stop traffic (**deny**) from going through (7).
- During **simple IWW sailing**, there is a medium probability that **government cyber warriors** will try to **disrupt** sailing by denying/blocking communication and navigation systems (8).
- During **port departure/arrival**, there is a medium probability that **government cyber warriors** will try to **deceive** sailing (9) by manipulating the signalling systems. Worst case consequences could be **collisions** between vessels or **collision** with infrastructure.

Table 10 shows a risk diagram where we have combined the probability of the threats with the severity of the consequences. Though there could be many different consequences of a single event, it is considered best to err on the safe side and pick the most severe. This table only considers the risks derived from the top 9 threats, but there could be additional significant risks when considering low probability threats with severe or catastrophic consequence.



Table 10: Risk diagram from the analysis

		<i>Consequence</i>			
		Minor	Significant	Severe	Catastrophic
<i>Probability</i>	Extreme				
	High		1. Disrupted complex IWW sailing, blocked waterways.		2. Deceived navigation during complex IWW sailing, possible collision.
	Medium	7. Denial of service at bridge, partly blocked bridge.	4. RCC made unavailable, blocked waterways. 5. Denial of service in front of lock, blocked waterways. 6. Denial of service within lock, blocked waterways. 8. Disrupted complex IWW sailing, blocked waterways.	3. Malware infection during complex IWW sailing, uncontrolled drifting.	9. Deceived sailing at port, possible collision.
	Low				



12 Discussion and Conclusions

This deliverable presents an approach for doing safety and security analysis of autonomous ship systems based on their CONOPS descriptions in UML. This is particularly useful at an early concept stage where implementation details are still undecided. At this stage, there is seldom any historical data to make quantitative estimates for safety and security risks, but having a systematic approach, based on the context, involved actors, ship particulars/processes and mission phases for the individual missions, provides traceability and justifications for qualitative assessments. Our methodology focuses on finding critical situations where cyber-attacks threaten the different modes of autonomous operations, especially related to the interplay between the automation and human operators. The results of our methodology can help designing operational envelopes that tackle situations out of the ordinary. It will reduce the frequency of resource demanding fallbacks and safety incidents. The risk assessment should be continuously maintained along with the progress of the design, the technological development and decisions, and the changing threats in the operating environment.

We have used autonomous barges for inland waterways transport between Rotterdam and Ghent as an example in this deliverable. This is based on use case B in AEGIS. The example analysis yields that congested areas where complex sailing is required, and also close to bridges and locks, subjects to risks that could cause blocking or in the worst-case collisions. This analysis has also raised some interesting discussions on how we should consider risks for autonomous shipping operations, such as:

- Are risks more acceptable when there are no people onboard?
- What new risks are introduced by the new technologies, e.g., remote control and AI?
- Which situations should be within the operational envelope?
- What are the default fallback functions?
- How much workload/stress can RCC operators handle and how much time is needed for handover?
- Should the AOC at some points disregard the direct commands of the RCC in order to prevent accidents?

Many of these questions are more of a philosophical nature, and need to be revisited by the different stakeholders for the specific shipping operations. It is also worth following and contributing to similar developments within the automotive and aviation sectors.



References

- [1] ISO, 'ISO/TS 23860:2022 Ships and marine technology — Vocabulary related to autonomous ship systems', 2022. Accessed: Feb. 20, 2023. [Online]. Available: <https://www.iso.org/standard/77186.html>
- [2] Ø. J. Rødseth *et al.*, 'Autonomous ship design standards', Autoship, AUTOSHIP deliverable D3.1 Ares(2021)1655844-05/03/2021, 2021. [Online]. Available: <https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5da3b7aa6&appld=PPGMS>
- [3] ISO, 'ISO/IEC 19501:2005 Information technology — Open Distributed Processing — Unified Modeling Language (UML) Version 1.4.2', 2005. Accessed: Feb. 20, 2023. [Online]. Available: <https://www.iso.org/standard/32620.html>
- [4] Ø. J. Rødseth, M. Hagaseth, D. A. Nesheim, P. H. Meland, and E. Wille, 'Safety and Security Analysis and Remedial Measures', AEGIS, Confidential, 2022.
- [5] L. A. L. Wennersberg *et al.*, 'Autonomous ship design methods and test principles', Autoship, AUTOSHIP deliverable D3.2 Ares(2021)1656035-05/03/2021, 2021. [Online]. Available: <https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5da3bc60b&appld=PPGMS>
- [6] Sveinung Johan Ohrem and Eleni Kelasidi, Nina Bloecher, Herman Biørn Amundsen, 'Seatomy applied in operational analysis of an autonomous net cleaning robot: NetClean 24/7 report for work package H1.1: Operational analysis and overall system design'. Sep. 23, 2022.
- [7] E. Kelasidi, 'Seatomy applied in an operational analysis and overall system design for an autonomous underwater vehicle operating in fish cages', SINTEF Ocean, OC2020 A-035, 20200-03-16. [Online]. Available: https://sintef.brage.unit.no/sintef-xmlui/bitstream/handle/11250/2647657/3.1_CageReporterReportReport.pdf?sequence=2&isAllowed=y
- [8] H.-C. Burmeister, W. Bruhn, Ø. J. Rødseth, and T. Porathe, 'Autonomous unmanned merchant vessel and its contribution towards the e-Navigation implementation: The MUNIN perspective', *International Journal of e-Navigation and Maritime Economy*, vol. 1, pp. 1–13, 2014.
- [9] IMO, 'Maritime Safety Committee (MSC 106), 2-11 November 2022', 2022. <https://www.imo.org/en/MediaCentre/MeetingSummaries/Pages/MSC-106.aspx> (accessed Jan. 25, 2023).
- [10] Ø. J. Rødseth, H. Nordahl, L. A. L. Wennersberg, B. Myhre, and P. Petersen, 'Operational Design Domain for Cars versus Operational Envelope for Ships: Handling Human Capabilities and Fallbacks', in *Proceedings of the 31st European Safety and Reliability Conference*, 2021.
- [11] Ø. J. Rødseth, L. A. L. Wennersberg, and H. Nordahl, 'Improving safety of interactions between conventional and autonomous ships', in *1st International Conference on the Stability and Safety of Ships and Ocean Vehicles*, 2021, pp. 7–11.
- [12] Ø. J. Rødseth and M. Vagia, 'A taxonomy for autonomy in industrial autonomous mobile robots including autonomous merchant ships', in *IOP conference series: materials science and engineering*, IOP Publishing, 2020, p. 012003.
- [13] Ø. J. Rødseth, L. A. L. Wennersberg, and H. Nordahl, 'Levels of autonomy for ships', *J. Phys.: Conf. Ser.*, vol. 2311, no. 1, p. 012018, Jul. 2022, doi: 10.1088/1742-6596/2311/1/012018.
- [14] B. Myhre, Ø. J. Rødseth, and S. Petersen, 'Integrating accountability in the systems design of autonomous and remote-controlled operations', *IOP Conf. Ser.: Mater. Sci. Eng.*, vol. 929, no. 1, p. 012020, Nov. 2020, doi: 10.1088/1757-899X/929/1/012020.
- [15] Ø. J. Rødseth, L. A. Lien Wennersberg, and H. Nordahl, 'Towards approval of autonomous ship systems by their operational envelope', *Journal of Marine Science and Technology*, vol. 27, no. 1, pp. 67–76, 2022.
- [16] SAE J3016, *Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles*, 2021st ed. Society of Automotive Engineers, 2021.



- [17] BSI, 'PAS 1883:2020 Operational Design Domain (ODD) taxonomy for an automated driving system (ADS) – Specification', The British Standards Institution, 2020. [Online]. Available: <https://www.bsigroup.com/globalassets/localfiles/en-gb/cav/pas1883.pdf>
- [18] *Revised Guidelines for Formal Safety Assessment (FSA) for use in the IMO Rule-Making Process*. in IMO Circulars, no. MSC-MEPC.2/Circ.12/Rev.2. International Maritime Organization, 2018.
- [19] J. Aust and D. Pons, 'A Systematic Methodology for Developing Bowtie in Risk Assessment: Application to Borescope Inspection', *Aerospace*, vol. 7, no. 7, Art. no. 7, Jul. 2020, doi: 10.3390/aerospace7070086.
- [20] D. Cimpean, J. Meire, V. Bouckaert, S. Vande Castele, A. Pelle, and L. Hellebooge, 'Analysis of cyber security aspects in the maritime sector', ENISA, 2011. [Online]. Available: https://www.enisa.europa.eu/publications/cyber-security-aspects-in-the-maritime-sector-1/at_download/fullReport
- [21] R. Anderson, *Security engineering: a guide to building dependable distributed systems*. John Wiley & Sons, 2020.
- [22] P. H. Meland, D. A. Nesheim, K. Bernsmed, and G. Sindre, 'Assessing cyber threats for storyless systems', *Journal of Information Security and Applications*, vol. 64, p. 103050, 2022.
- [23] B. Svilicic, J. Kamahara, M. Rooks, and Y. Yano, 'Maritime cyber risk management: An experimental ship assessment', *The Journal of Navigation*, vol. 72, no. 5, pp. 1108–1120, 2019.
- [24] I. Mraković and R. Vojinović, 'Maritime cyber security analysis—how to reduce threats?', *Transactions on maritime science*, vol. 8, no. 01, pp. 132–139, 2019.
- [25] V. Bolbot, G. Theotokatos, E. Boulougouris, and D. Vassalos, 'A novel cyber-risk assessment method for ship systems', *Safety Science*, vol. 131, p. 104908, Nov. 2020, doi: 10.1016/j.ssci.2020.104908.
- [26] H. M. Tusher, Z. H. Munim, T. E. Notteboom, T.-E. Kim, and S. Nazir, 'Cyber security risk assessment in autonomous shipping', *Marit Econ Logist*, vol. 24, no. 2, pp. 208–227, Jun. 2022, doi: 10.1057/s41278-022-00214-0.
- [27] C. Grigoriadis, R. Laborde, A. Verdier, and P. Kotzanikolaou, 'An Adaptive, Situation-Based Risk Assessment and Security Enforcement Framework for the Maritime Sector', *Sensors*, vol. 22, no. 1, Art. no. 1, Jan. 2022, doi: 10.3390/s22010238.
- [28] C. Park, C. Kontovas, Z. Yang, and C.-H. Chang, 'A BN driven FMEA approach to assess maritime cybersecurity risks', *Ocean & Coastal Management*, vol. 235, p. 106480, Mar. 2023, doi: 10.1016/j.ocecoaman.2023.106480.
- [29] K. Tam and K. Jones, 'Cyber-Risk Assessment for Autonomous Ships', in *2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*, Jun. 2018, pp. 1–8. doi: 10.1109/CyberSecPODS.2018.8560690.
- [30] P. H. Meland, 'Storyless cyber security: Modelling threats with economic incentives', NTNU, 2021. [Online]. Available: <https://ntnuopen.ntnu.no/ntnu-xmlui/handle/11250/2825312>
- [31] Scheepvaartwest, 'Polybotes - IMO 9280392', *Car Carriers Ro-Ro*, 2014. <https://www.scheepvaartwest.be/CMS/index.php/car-carriers-ro-ro/4826-polybotes-imo-9280392> (accessed May 30, 2023).
- [32] EurIS, 'Voyageplanner', *Compute your voyage*. <https://www.eurisportal.eu/voyageplanner#calculate=1&stops=NLVLA1080BJ330200009%2CNLDOR00111J214400043%2CNLWED00137J196100010%2CNLHAN00131J055500468%2CBEGNEOG010000000004> (accessed May 30, 2023).
- [33] P. H. Meland, K. Bernsmed, E. Wille, Ø. J. Rødseth, and D. A. Nesheim, 'D2.2 Updated cyber risk assessment for the maritime industry', *SINTEF*. <https://www.sintef.no/en/publications/publication/1947808/> (accessed May 12, 2023).
- [34] A. Shostack, *Threat modeling: Designing for security*. John Wiley & Sons, 2014.