European Maritime Safety Agency

TESTING OF RBAT ON SPECIFIC CASES OF MASS CONCEPTS

REPORT 4

Version: 2022-0481, Rev. 0

Date: 26/09/2022

EMSA

Table of contents

EXECUTIVE SUMMARY

Introduction

EMSA has contracted DNV to perform a functional study for developing a Risk-Based Assessment Tool (RBAT) for maritime autonomous surface ships (MASS). As outlined in DNV's proposal (DNV, 2020a) and EMSA's Tender Specifications (EMSA, 2020), the RBAT study consist of three parts:

- Part 1: Develop a framework for a generic MASS risk assessment tool
- Part 2: Test the risk assessment tool on specific cases and develop software tool prototype
- Part 3: Re-iterate testing on more complex cases and finalize the software tool

Objective

The objective of this report is to document the input to the testing of RBAT, the results and experiences from the testing, and an updated framework and method description.

Scope of work

The study is currently at the end of Part 2 which includes the following scope of work:

a) Identify and select specific MASS concepts and sub-functions for testing RBAT

b) Develop a risk evaluation technique appropriate to be applied to MASS concepts

c) Perform a gap analysis of RBAT and further develop the framework

d) Develop test cases for the identified MASS concepts and sub-functions, and test RBAT

e) Based on the results from the test cases, update RBAT and develop a first version of a functional software prototype

Activities a) to c) is documented in the first report of Part 2 and the Third Report of the RBAT study.

Activity d) and part of activity e) are documented in this report, namely the second (interim) report of Part 2 and the Fourth Report of the RBAT study. A separate report is issued for describing the software development. In addition, a link giving access to the RBAT software prototype will be provided.

Activity d) Develop test cases for the identified MASS concepts and sub-functions, and test RBAT

The Third Report suggested that the following MASS concepts should be developed for testing:

- Concept A – a fleet of three identical unmanned and uncrewed, autonomous, and remotely supervised short-sea cargo vessels.
- Concept B – a fleet of ten identical uncrewed, autonomous, and remotely supervised small passenger ferry.
- Concept C – a fleet of three identical Ro-Pax ferries, with a manned bridge, remotely control machinery, and navigational decision support system.

Each concept was described using a Concept of Operation (ConOps) format:

- A description of the vessel and fleet mission, including
    - Operational tasks
    - Operational area and conditions

- Weather and sea-state limitations

- A description of concepts main physical characteristics, including
  - Vessel dimensions and layout
  - Remote control centre
  - Communication link
- A description of autonomous systems
  - Functionality
  - System hierarchy
  - Redundancy philosophy
  - RCC capabilities
- Operational roles involved

RBAT was tested by populating the tool with relevant input from the ConOps. This included:

- a breakdown of missions into mission phases, operations, control functions and control actions
- systems or operational roles identified as agents responsible for either performing or supervising execution of control actions

In addition, descriptions related to the operational context (weather, locations etc.) were used as basis for evaluating the potential severity of accidents and whether mitigations implemented for preventing losses from unsafe conditions would be expected to be effective in given settings.

The testing was done inhouse DNV through workshop discussions involving internal subject matter experts.

Experiences made during the testing was systematically recorded. Some were made because of specific test activities suggested in the Third Report, and some emerged spontaneously through the testing.

The main impression is that RBAT successfully can identify and addressing key challenges associated with MASS, but that adjustments to the methodology were needed to more accurately capture and differentiate between risk levels for different scenarios.

Activity e) Based on the results from the test cases, update RBAT

How to improve and update RBAT was decided in a series of follow-up meetings after the workshops. Significant efforts were invested in how to assess independence between the systems performing the failed autonomous or automated control actions, and the systems required for mitigation of such failures.

The method description from the Third Report has been updated to incorporate improvements based on experiences from the testing.

TABLE OF FIGURES

LIST OF TABLES

DEFINITIONS

Terms	Definitions
abnormal situation	A disturbance in the normal operation which can potentially result in an accident.
accident	An unintended event involving fatality, injury, ship loss or damage, other property loss or damage, or environmental damage (IMO, 2018).
accident category	A designation of accidents reported in statistical tables according to their nature, e.g., fire, collision, grounding, etc. (IMO, 2018).
accident scenario	A sequence of events from the initiating event to one of the final stages (IMO, 2018).
agent	Human or software (computer) responsible for performing or supervising control actions.
annunciated failure	An annunciated failure is one which fails 'actively', i.e., in such a manner as to inform crew of the failure by virtue of system generated cues such as visual and/or audible notifications, warnings, and alarms.
anticipated event	Events which do not force the system outside the safe operating envelope (SOE), and which can be handled while also maintaining normal operations.
automation	The execution by a 'software' *agent* (usually a computer) of a function that was previously carried out by a human" (Parasuraman & Riley, 1997).
autonomy	"Technology operates alone". See sub-chapter 3.3.1 in Report 1oo2 for Part 1 of RBAT (DNV GL, 2020a).
causal factors	The minimum combination of causes required to initiate the unsafe condition/mode. May comprise of a single initiating cause, a combination of multiple causes, or initiating causes in the presence of other enabling events.
common cause failures	Failures of multiple items, which would otherwise be considered independent of one another resulting from a single cause (IEC, 2018).
ConOps	Document describing the characteristics of a proposed system from the viewpoint of an individual who will use that system (ISO/IEC/IEEE 15288:2015).
context	External and internal environment in which the organization seeks to achieve its objectives (ISO, 2009).
control	Purposeful action on or in a process to meet specified objectives (IEC, 2013).
control function	Control actions performed by humans or software for the accomplishment of a functional goal (adapted from IEC, 2000).
control action	Acquisition of information, analysis of information, decision-making, or implementation of physical actions performed as part of a control function.

Terms	Definitions
direct cause	Events which singly, or in few numbers, can cause an accident (and severe losses) if they occur in the presence of a hazard.
enabling event	Occurrence of a failure or presence of a hazard which contributes to escalating an unsafe condition/mode into an accident.
essential continuous function	A function which is required to continuously perform according to its specifications to maintain the safety of the vessel during one or more of its normal type of operations.
failure	Loss of the ability of an item to perform the required (specified) function within the limits set for its intended use. This occurs when the margin (to failure) is negative (DNV, 2021b).
failure cause	Set of circumstances that leads to failure (IEC, 2018).
failure effect	A description of the operation of a system or an item as the result of a failure; i.e., the consequence(s) a failure mode has on the operation, function or status of a system or an item (SAE, 1996).
failure frequency	The number of failures expressed in failures per unit of time (calendar or operational).
failure mechanism	Process that leads to failure (IEC, 2018). The process may be physical, chemical, logical, psychological or a combination thereof.
failure mode	The observed way in which the failure (of an item) occurs (adapted from SAE, 1996 and DNV, 2021b).
function	Specific purpose or objective to be accomplished, that can be specified or described without reference to the physical means of achieving it (IEC, 2020). In RBAT functions refer to how systems perform to successfully accomplish operations. Sub-functions are offspring (sub-goals) of higher-level, parent function.
functional allocation/ assignment	Distribution of functions between human and software (ISO, 2000). Functional allocation can also be referred to functional assignment (IEC, 2000).
functional analysis	The examination of the functional goals of a system with respect to available manpower, technology, and other resources, to provide the basis for determining how the function may be assigned and executed (IEC, 2009).
functional goal	The performance objectives that shall be satisfied to achieve a higher-level corresponding function (adapted from IEC, 2009).
function tree	Hierarchical breakdown of high-level key functions into a set of sub-functions.

Terms	Definitions
hazard	A potential to threaten human life, health, property or the environment (IMO, 2018). For the purpose of RBAT, this is interpreted as the source of harm which, unless managed, has the potential to cause accidents involving harm or losses. In terms of *safety*, a hazard therefore often refers to conditions, situations, or states in which various sources of energy, biological or chemical agents are present.
hierarchical goal structure	Relationship between a goal and sub-goals structured in a hierarchical order (adapted from IEC, 2009).
human-automation interaction	The way a human is affected by, controls, and receives information from automation while performing a task (Sheridan & Parasuraman, 2006).
human error	Discrepancy between the human action taken or omitted, and that intended or required to achieve a task goal (adapted from IEC, 2018).
incident	Occurrence of any event, other than an accident, that is associated with a ship or its required infrastructure and affects or could affect its safety.
initiating event	The first of a sequence of events leading to a hazardous situation or accident (IMO, 2018).
fault detection, isolation, and recovery (FDIR)	A control function's internal capacity to withstand or self-recover from a failure so that normal operations are not disrupted to the extent where they cannot be continued safely. In case system self-monitoring identifies a fault, what type, and its location, examples of recoveries include: Switch-off of a faulty equipment Switch-over from a faulty equipment to a redundant equipment Change of state of the complete system into a Safe Mode with limited functionalities In RBAT, FDIR represents a type of *mitigation*.
item	Subject being considered (IEC, 2018).
key function	High level functional goal shared by a set of control functions. Navigation, manoeuvring, and communication are examples of key functions. In RBAT, key functions are located at the highest level in the Function Tree.
loss	A loss involves something of value to stakeholders. Losses may include a loss of human life or human injury, property damage, environmental pollution, loss of mission, loss of reputation, loss or leak of sensitive information, or any other loss that is unacceptable to the stakeholders (Leveson & Thomas, 2018).

Terms	Definitions
minimum risk condition	A temporary as-safe-as-possible state that the vessel enters when it experiences situations which, if continued, involves operating outside the safe operating envelope.
mission	The commercial, political (e.g., defence) or public intentions which have contributed to and justifies the vessel concept development and operation.
mission model	Hierarchical breakdown of a vessel mission into a set of mission phases and operations.
mission phase	Subdivisions of the mission typically characterized by a recognizable shift in where the vessel is located in terms of geographical surroundings, or the start and end of one or more operations.
mitigation	A measure implemented to prevent unsafe conditions or modes from resulting in losses (see “accident”).
mitigation layer	A mitigation capable of preventing a scenario from proceeding to an accident without being adversely affected by the initiating event or the action of any other mitigation layer associated with the scenario.
node	In RBAT a node is one operation for a mission phase under which a set of control functions and actions a grouped together for analysis.
operations	Activities performed as part of a mission phase in order to achieve the mission goal. Sub-operations are offspring (sub-goals) of higher level, parent operations.
operational goals	The ultimate purposes of a vessel (adapted from IEC, 2009). In RBAT operational goals are explained in terms of the mission, mission phases and operations.
performance	The performance of a technology is its ability to provide its specified functions (DNV, 2021b). These functions contribute to safety/reliability as well as the output or value generated by the system, equipment, or component when in operation.
performance margin	The difference between the achieved performance and the specified performance requirement (DNV, 2021b).
performance shaping factors	Human, workplace, or other contextual factors which have a significant effect on an operator’s or crew of operator’s performance.
process	Set of interrelated or interacting activities that transforms inputs into outputs (IEC, 2018)
reliability	The ability of an item to perform a required function under given conditions for a given time interval or at a specified condition (DNV, 2021b). In quantitative terms, it is one (1) minus the failure probability.

Terms	Definitions
recovery actions	Actions taken to recover the system from a degraded, failed, or unsafe state and back to a state which allow normal and safe operations to be continued.
redundancy (of a system)	Having multiple capabilities for performing the same function, typically in parallel (DNV, 2021b).
risk control measure	A means of controlling a single element of risk (IMO, 2018). This may refer to […] measures taken to reduce the risks to the operation of the system, and to the health and safety of personnel associated with it or in its vicinity by (DNV, 2021b): — reduction in the probability of failure — mitigation of the consequences of failure *Guidance note:* The usual order of preference of risk control measures is: a) inherent safety b) prevention c) detection and d) control e) mitigation f) emergency response.
risk control options	A combination of risk control measures (IMO, 2018).
safe operating envelope (SOE)	Conditions, both internal and external, in which a system can safely execute its normal and planned operations.
scenario	Possible sequence of specified conditions under which the system, item or process functions are performed (IEC, 2018). See also “accident scenario”.
severity	Relative ranking of potential or actual consequences of a failure or a fault (IEC, 2018).
situational awareness	Situational awareness or situation awareness (SA) is the perception of environmental elements and events with respect to time or space, the comprehension of their meaning, and the projection of their future status (Endsley 1995).
supervision	A role with an explicit responsibility to monitor system performance and detect abnormalities so that the desired outcome can be achieved through implementation of corrective responses.
system	Combination of interacting elements organized to achieve one or more stated purposes, i.e., goals (IEC, 2018).

Terms	Definitions
task	A set of [control] actions taken by humans to enable functions and perform operations. A task may involve interactions with several different functions, but also with humans. Task goals is the same as *operations*.
unannunciated failures	An unannunciated failure is one which is latent or fails 'passively', i.e., in such a manner as to not inform the crew of the failure by virtue of system generated cues, or the provided information is misleading, incomplete, or not presented in due time.
unsafe condition/ mode	Incident where a system is operating outside its normal (and safe) operating envelope due to degraded performance (e.g., failures) or exceeded capabilities which, if left unmitigated, has the potential to directly cause an accident.
uptime	Measure of system reliability, expressed as the percentage of time a machine, typically a computer, has been working and available. Uptime is the opposite of downtime (source: https://en.wikipedia.org/wiki/Uptime)
worst-case outcomes	The most severe foreseeable outcome of an unsafe condition/mode when assuming there is no mitigation. In RBAT, worst-case outcomes assume the contextual presence of a *hazard*. For example, loss of steering (an unsafe condition) close to shore (a hazard) results in a grounding (a worst-case outcome).

1 INTRODUCTION

1.1 Background

EMSA has contracted DNV to perform a functional study for developing a Risk-Based Assessment Tool (RBAT) for maritime autonomous surface ships (MASS). As outlined in DNV's proposal (DNV, 2020a) and EMSA's Tender Specifications (EMSA, 2020), the RBAT study consist of three parts:

- Part 1: Develop a framework for a generic MASS risk assessment tool
- Part 2: Test the risk assessment tool on specific cases and develop software tool prototype
- Part 3: Re-iterate testing on more complex cases and finalize the software tool

1.2 Objective

The objective of this report is to document the input to the testing of RBAT, the results and experiences from the testing, and an updated framework and method description.

1.3 Scope of work

The study is currently at the end of Part 2 which includes the following scope of work:

f) Identify and select specific MASS concepts and sub-functions for testing RBAT

g) Develop a risk evaluation technique appropriate to be applied to MASS concepts

h) Perform a gap analysis of RBAT and further develop the framework

i) Develop test cases for the identified MASS concepts and sub-functions, and test RBAT

j) Based on the results from the test cases, update RBAT and develop a first version of a functional software prototype

Activities d) and e) are documented in this report, namely the second (interim) report of Part 2 and the Fourth Report of the RBAT study. Activities a) to c) is documented in the first report of Part 2 and the Third Report of the RBAT study.

1.4 Limitations

Chapters 2 to 4 present the detailed descriptions, as concept of operation (ConOps), of the three MASS concepts proposed as test cases in the Third Report (DNV, 2022). In some areas the ConOps' include more details than what has been tested. This is a result of the concepts being developed in an exhaustive manner, while only a selected set of functions and sub-functions were initially identified for the testing of the tool. The additional functions do however provide some completeness to the concept descriptions and can be used and updated for further testing in Part 3.

Note that the ConOps' of the three selected MASS concepts, namely the short-sea cargo vessels (Chapter 2), the small passenger ferries (Chapter 3), and the Ro-Pax ferry (Chapter 4), have all been written as standalone ConOps'. This means that some parts are repeated for each ConOps.

1.5 Updates to the framework described in the Third Report

Updates to the RBAT framework and method description described in the Third Report are documented in sub-chapter 5.4 and chapter 6.

1.6 How to read this report

The report structure follows the sequence of activities listed as scope of work for the second half of Part 2.

- Chapters 2 to 4 present the MASS concepts and sub-functions developed for the purpose of testing RBAT (Activity d).
- Chapter 5 summarizes the test approach, who was involved, examples from the analyses, and how the method has been updated based on experiences from applying RBAT to the cases (Activity e).
- Chapter 6 includes an updated RBAT method description based on the experiences reported in chapter 5 (Activity e).
- Contents considered too lengthy or dominating to be included in the main body of the report have been included as Appendices.

To avoid an excessively lengthy report due to duplications of contents in previous report, it is assumed that reader is familiar with the previous deliverables of the RBAT project, namely the First (DNV, 2020b), Second (DNV, 2021a), and Third Report (DNV, 2022a).

A separate report (DNV, 2022b) will be issued for describing the software deliverables.

2 CONOPS CONCEPT A – SHORT-SEA CARGO VESSEL

2.1 Overall description

The short-sea cargo vessel is planned to be operated as an autonomous, unmanned vessel, with active supervision from a remote-control centre (RCC). This document contains a conceptual description of how the vessel is equipped for an unmanned operation, and how tasks and duties will be shared and solved in cooperation between humans and control systems. The document gives an introduction to the vessel, and the context and environment in which the vessel will operate.

The vessel is a small sized container feeder designed for daily transport of containers between Horten and Moss. It will be powered by batteries and be part of an integrated logistical container-solution involving autonomous cargo handling and crane operations.

For better utilizing the capacity of the RCC and making the concept commercially viable, the personnel will monitor several vessels at the time. The short-sea cargo vessel fleet will consist of three identical ships, sailing in different areas. They will perform the same task, namely, to transfer cargo from one port to another. For the scope of this ConOps, only the route between Horten and Moss in Ytre Oslofjord will be analysed.

2.2 Mission description

The overall purpose of the short-sea cargo vessel is daily transport of up to 100 TEU[1] containerized cargo from Horten to Moss. This ConOps, which is limited to the four concept-function combinations presented in the Third RBAT report (DNV, 2020), the missions and operations considered are given in Table 1.

[1] TEU is an acronym used in logistics, which means 'Twenty Equipment Unit' or in other terms a '20-foot container.

Table 1: Mission specification selected for the short-sea cargo concept

	Concept-function combination #1	Concept-function combination #2	Concept-function combination #3	Concept-function combination #4
Mission phase	Arrival in port	Transit to location	Activities in port	Transit to location
Traffic density	Medium	Medium	NA	Medium
Operation	Perform harbour manoeuvring	Navigate through enclosed waters	Perform loading/unloading	Handle loss of communication link
Functions	*Perform navigation:* - Observe surroundings -Avoid collision and grounding *Perform manoeuvring:* - Provide steering - Provide acceleration/ deceleration *Perform mooring:* -Prepare mooring line -Deploy mooring line -Fix/secure mooring line to quay	*Perform collision and grounding avoidance:* - Detect vessels/ objects - Classify vessels/ objects - Observe vessels/ objects movements (heading and speed) - Determine vessels/ objects relative position, distance, and movement (bearing) - Determine CPA/TCPA for vessels/objects - Implement collision and grounding avoidance strategy	*Handle and monitor cargo:* - Plan & prepare cargo handling -Un-secure cargo -Unload cargo *Perform ballasting & trim:* -Calculate and verify trim & stability -Operate ballast pumps *Maintain communication:* - Communication between vessel and dock operator	*Maintain communication (data, voice/sound, visual signalling):* - Use AIS and light signals to notify other ships - Notify VTS *Perform manoeuvring:* - Maintain position until communication is established (MRC)
Supervision	Active supervision	Active supervision	Active supervision	No supervision

2.2.1 Operational tasks

The vessel will transport cargo as part of a bigger supply chain from Horten to Moss which is located in the outer Oslofjord. The port in Horten will be used for loading cargo, while the port in Moss is designated for unloading. The vessel will transport empty containers when returning to Horten from Moss. Both ports will be equipped with automated cranes designed for servicing the vessel. In addition to this automatic charging capabilities will be established in both ports. As presented, the mission phases *arrival in port, transit to location* and *activities in port* are in focus.

2.2.2 Operational area and conditions

The crossing between Horten and Moss is approximately 5.7 nm (10.5 km) and will take approximately 35 minutes at normal service speed (10 kn). The depth at the port in Horten is approximately 6 m, and 8 m at the port in Moss. The maximum depth on the route is approximately 200 m.

The area has medium traffic density. This is illustrated in Figure 1 which shows AIS tracks for all vessels in the area from 2019. Besides traffic crossing the actual route, a highly trafficked car ferry also sails on the same route as the short-sea cargo vessel.

Sailing in the area is governed by the law “Havne og farvannsloven” (Lovdata, 2019), and is under surveillance by Horten VTS. Figure 2 shows the Horten VTS control area in dark green shade.

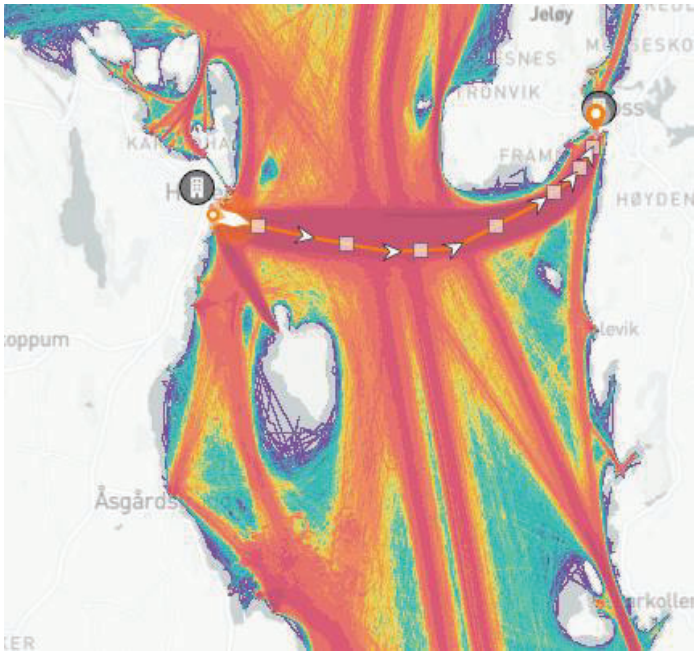


Figure 1: Concept A route (Marine Traffic, 2022)

Figure 2: Horten VTS control area in green (Kystverket, 2022)

In the area in question, the Norwegian Coastal Administration (NCA) has pointed out the locations shown in Figure 3 as safe harbours for vessels in distress to avoid contamination/spills, to secure access from rescue services, and to ensure that the vessel does not become a hazard to other traffic. All the locations are considered relevant for the short-sea cargo vessel except the harbour located in Horten Indre havn, as this harbour is located too far from the route. Table 2 shows the specific properties for each safe harbour.

Figure 3: Safe harbours (Kystverket, 2022)

Table 2: Safe harbours (Kystverket, 2022)

Location	No pollution risk	With pollution risk	With fire/ explosion risk	Water depth at location	Conditions for anchoring
Horten dypvannskai	Good	Suitable	Suitable	8 m	Good
Bastøybukta	Good	Suitable	Suitable	20-40 m	Good
Verlebukta/Moss havn	Good	Suitable	Suitable	8 m	Good

2.2.3 Weather and sea-state limitations

The relevant area is sheltered and is therefore not normally exposed to high waves. Still, the vessels may occasionally be exposed to heavy weather. Figure 4 shows dominant wind speeds and directions. The data is recorded at Gullholmen outside Moss. As can be seen from the figures the maximum wave height has been approximately 3.5 m, while the wind speed is rarely above 8 m/s.

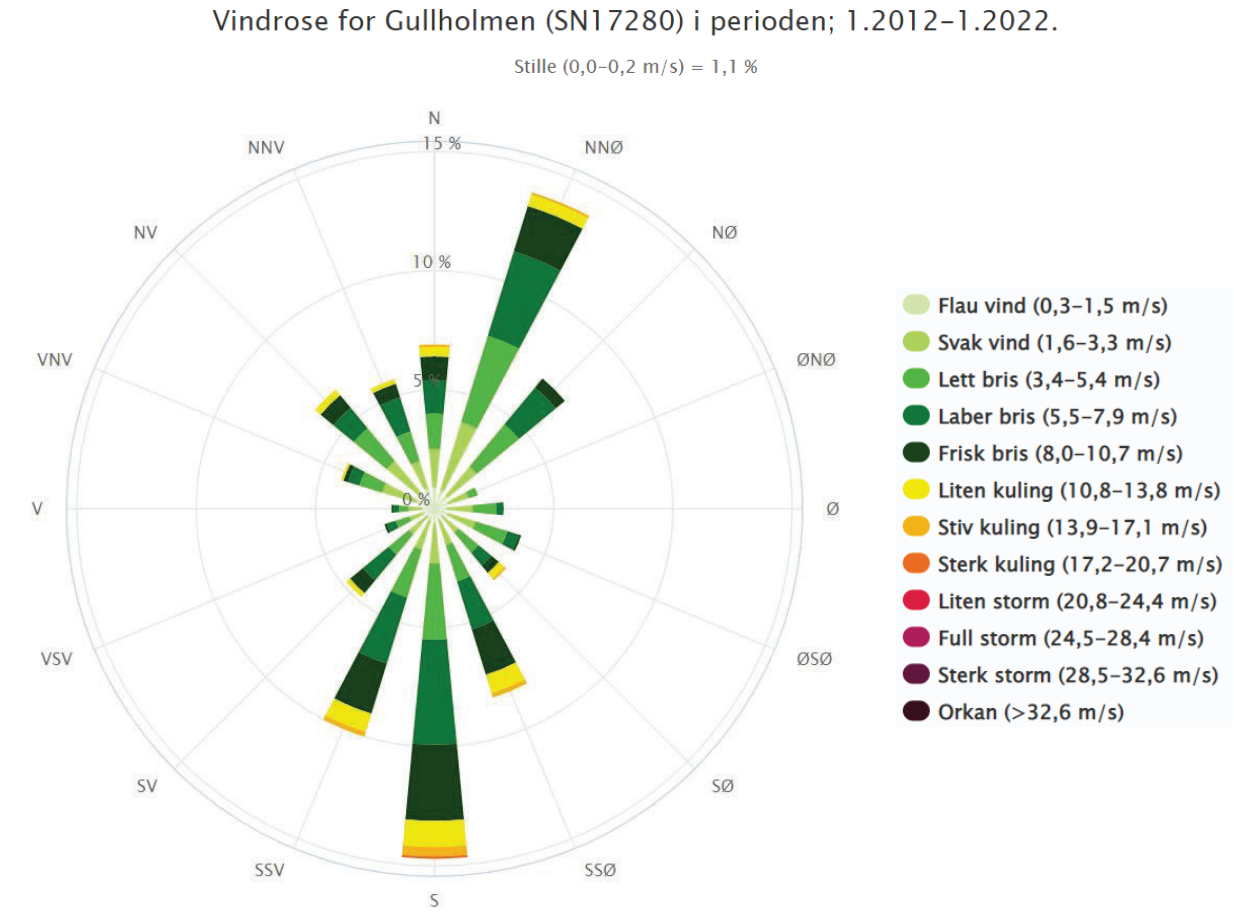


Figure 4: Wind rose, Gullholmen last 10 years (Norsk klimaservicesenter, 2022)

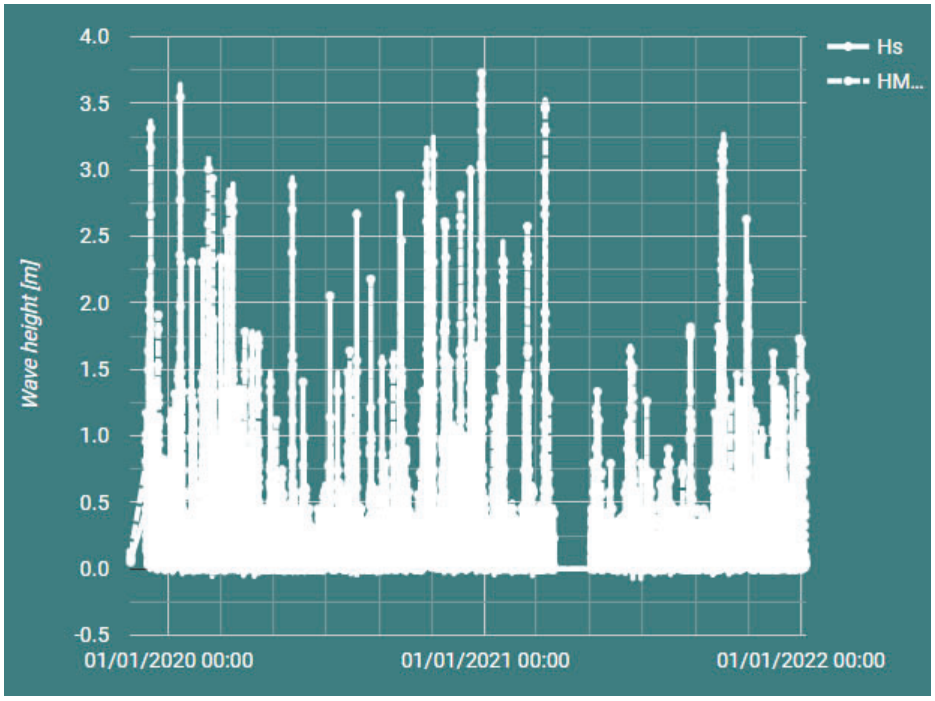


Figure 5: Wave heights from 2020 and 2021 (Norce, 2022)

2.3 Main characteristics

2.3.1 Key vessel characteristics

The ship characteristics for the short-sea cargo vessel is presented in Table 3 below.

Table 3: Ship characteristics for short-sea cargo

Route	Horten – Moss
Type	Short-sea cargo
LOA	80,0 m
Beam	15,0 m
Draught	5,0 m
DWT	3000
Capacity	100 TEU
Design speed	10 kn

2.3.1.1 Power generation and propulsion

The vessel will be powered by rechargeable batteries located in segregated battery rooms. Switchboards are located as shown in Figure 6, and are responsible for distribution of electric power via DC. The capacity will be dimensioned for a return trip using the route presented in this case, plus allowance for contingencies. This requires fully charged batteries at the starting point.

A redundant propulsion system will be installed onboard to ensure that propulsion and maneuvering capabilities will remain operational in case of a single failure in propulsion- or auxiliary systems. As shown in Figure 6 this is obtained with two bow thrusters, each supplied from separate switchboards, and with the same set-up for the two azimuth thrusters aft. Further, a bus-tie between the switchboards can be closed in order to supply consumers on both sides.

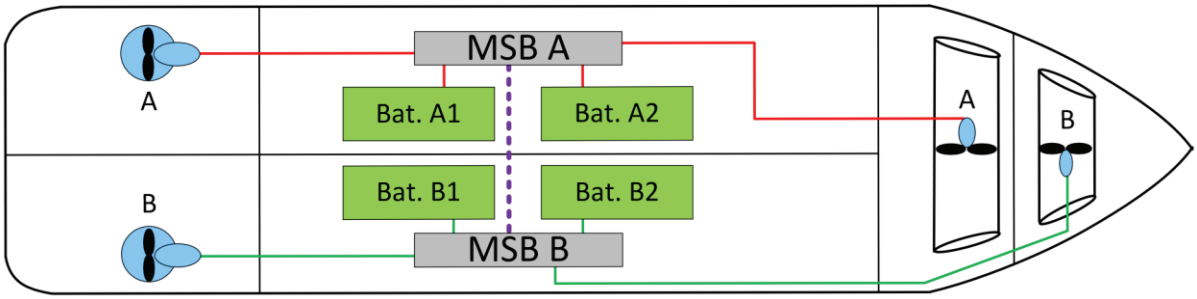


Figure 6: Propulsion redundancy philosophy

2.3.2 Remote control center characteristics

There is one remote control centre (RCC) responsible for supervising the fleet of short-sea cargo vessels, located in the Oslo area. The RCC consists of the control room, equipment room, an emergency preparedness room, and a resting area with facilities such as restroom, small kitchen, etc. All essential equipment is configured with redundancy to prevent system breakdown caused by any single point of failure. In addition, the equipment is connected to UPS, and an emergency generator providing power redundancy in case of power outage.

2.3.3 Communication-link characteristics

The area is covered by public GSM and has very good coverage with 4G+ around the docks and 4G at the rest of the route as illustrated in Figure 7. This is an example from one of the available cellular network providers in the area. The bandwidth required by the vessel and/or the RCC depend on the mission

phase/situation, with estimated higher requirement when entering/leaving port and/or transfer to an MRC takes place.

The vessels verify connection status at start-up/before departure. The status of the communication is continuously and automatically monitored while the vessel is in operation.

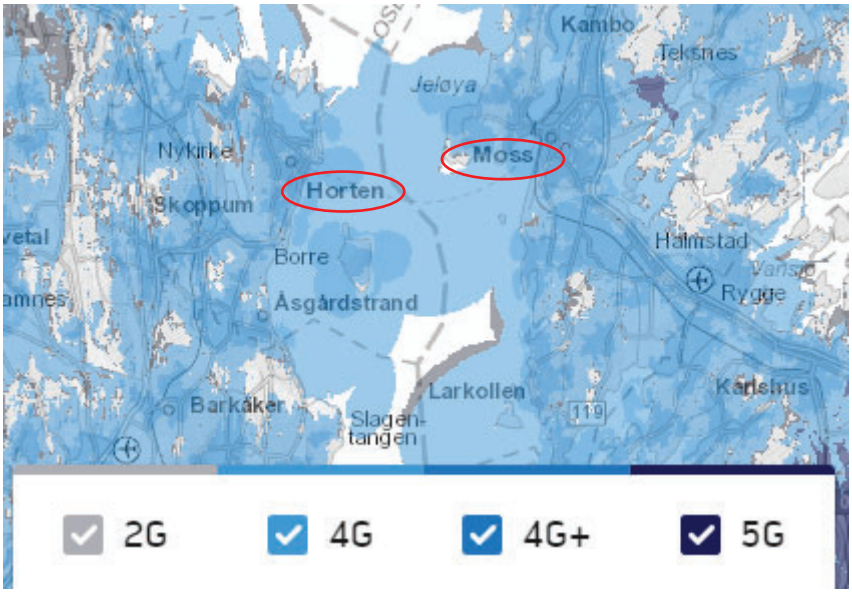


Figure 7: GSM coverage (Telenor, 2022)

2.4 Description of autonomous systems

In this chapter a preliminary description of the onboard systems is given. Note that additional systems and functionalities are necessary for the vessel to be operational, and that this ConOps is focused on the mission and the operations selected in Table 1. I.e., the following lists and overviews are not exhaustive.

2.4.1 Functionality

Basic and essential continuous functionalities:

Some of the systems on the vessel have functionalities which need to be in place and stable to enable normal operation. These are the electric power system and the integrated automation system (IAS).

- Monitoring of state of charge, loads, electric consumers, and management of charging is conducted by the electric power system. This power system status is important for planning of trips according to the timetable, planning for charging, and for information about the vessel's capacity in case of an event.
- An IAS integrates the various control systems onboard the vessel and makes it possible for users that are onboard a vessel to control and monitor all those systems from a single user interface. For this short-sea cargo vessel, the IAS will in addition forwarded monitoring data to the autonomy system and the RCC, and it will distribute commands received from the autonomy system and the RCC to the relevant systems onboard the vessel. Since it facilitates the command flow to the propulsion and motional control system, failures in the IAS may potentially lead to no or reduced capabilities for propulsion and steering.

Navigation and manoeuvring related functionality:

The autonomous navigation system is the overall control system responsible for navigation and consists of the situation awareness system and the collision and grounding avoidance system. Based on the interaction

with these systems the autonomous navigation system controls speed and direction using the propulsion and motion control system. The systems are further described in the following:

- The situation awareness system manages and utilises the information about the vessel surroundings from AIS, ECDIS, GNSS, radar, lidar, IR, cameras, speed log, echo sound, gyro compass, microphone, thermometer, anemometer, and inertial measurement unit (IMU).
- When the vessel is moving or about to move, the collision and grounding avoidance system utilises information from the situation awareness system to determine whether the vessel can continue as planned or adjustments are required to avoid collision or grounding.
- The propulsion and motion control system ensures acceleration, deceleration, and directional change of the vessel, with the azimuth thrusters.
- Cargo handling related functionalities

For safe and efficient loading and unloading of cargo the cargo handling system and the loading computer works together.

- For unloading, the cargo handling system ensures the right container is un-secured at the right time, and that it is unloaded to the designated area/truck at the quay side. Data about the container is retrieved, e.g., weight, centre of gravity, contents. The data and unloading sequence are shared with the loading computer. For loading, the operation is reversed.
- The loading computer calculates the trim and stability of the vessel, based on the information shared by the cargo handling system and on actuals from the IMU. The ballast pumps are engaged as required to obtain the desired trim and stability.

Mooring related functionalities:

The vessel is equipped with an automatic mooring system. Based on information from the situation awareness system the mooring operation is initiated at the right time. The mooring lines are deployed, fixed and tightened as required by the weather and sea conditions. The tension in the lines is continuously monitored and adjusted as needed.

Communication related functionalities:

There are three communication related systems onboard: Internal communication, external communication and the telecommunication system where the latter enables communication and remote control from the RCC.

- Internal communication is available for any personnel on board for e.g., manual intervention, or maintenance. These systems are not further elaborated in the current version of the ConOps.
- The external communication concerns communication with other vessels by the use of VHF radio. Any incoming call is routed to the RCC via the datalink, as there are no personnel onboard. It is the remote operator who is responsible for receiving the call and responding appropriately. Any outgoing VHF call is routed via the datalink from the RCC to the vessel and from there to the receiver using the vessel's VHF radio.
- Communication data/link between Short-sea Cargo vessel and RCC is handled by the telecommunication system and is dependent on antennas and cellular network coverage. A similar system is located in the RCC to receive the data stream from the ferry and transmit commands to the vessel.

Emergency response – handle loss of communication link:

The emergency response in focus for the short-sea cargo vessel is a loss of communication link scenario where the remote operators in the RCC has lost communication with the vessel. This event could lead to a dangerous situation where the RCC is not able to take control or in other ways intervene with the vessel when

required. If the communication link is lost it is essential that the vessel is put in a state that poses least risk to life, environment, and property. This state is called the minimum risk condition (MRC), and several MRCs can be relevant for the emergency. Depending on the emergency, various mitigations and MRCs are relevant and/or available.

This scenario involves using the following functionalities:

- AIS and light signals to notify other ships.
- Enter MRC: Maintain position (using dynamic positioning system (DP), thrusters/propulsion system, batteries/power system)

2.4.2 Hierarchical structure

Figure 8 illustrates the hierarchical control structure of the short-sea cargo vessel. The structure represents the ship systems and their subsystems, as described in Chapter 2.4.1. Each of the functions is performed by a system of the autonomous vessel. Connections between the different systems are represented by arrows. The RCC supervises the operation and can take direct control of the individual systems, via remote connection, outlined in green if necessary. The integrated automation system (IAS) is the integrator and facilitates control and monitoring of the different systems onboard.

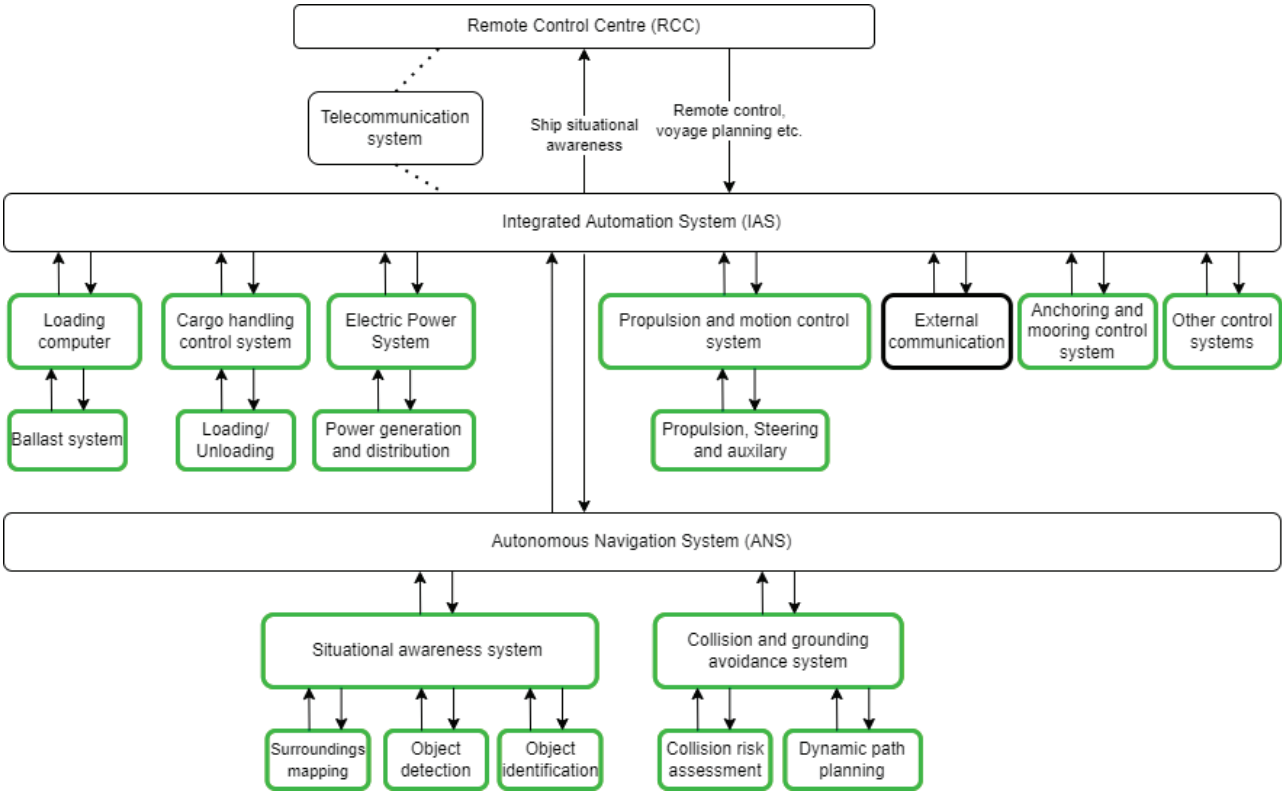


Figure 8: SSC hierarchical control structure

Figure 9 shows the specific equipment and hardware which is part of the autonomous navigation system.

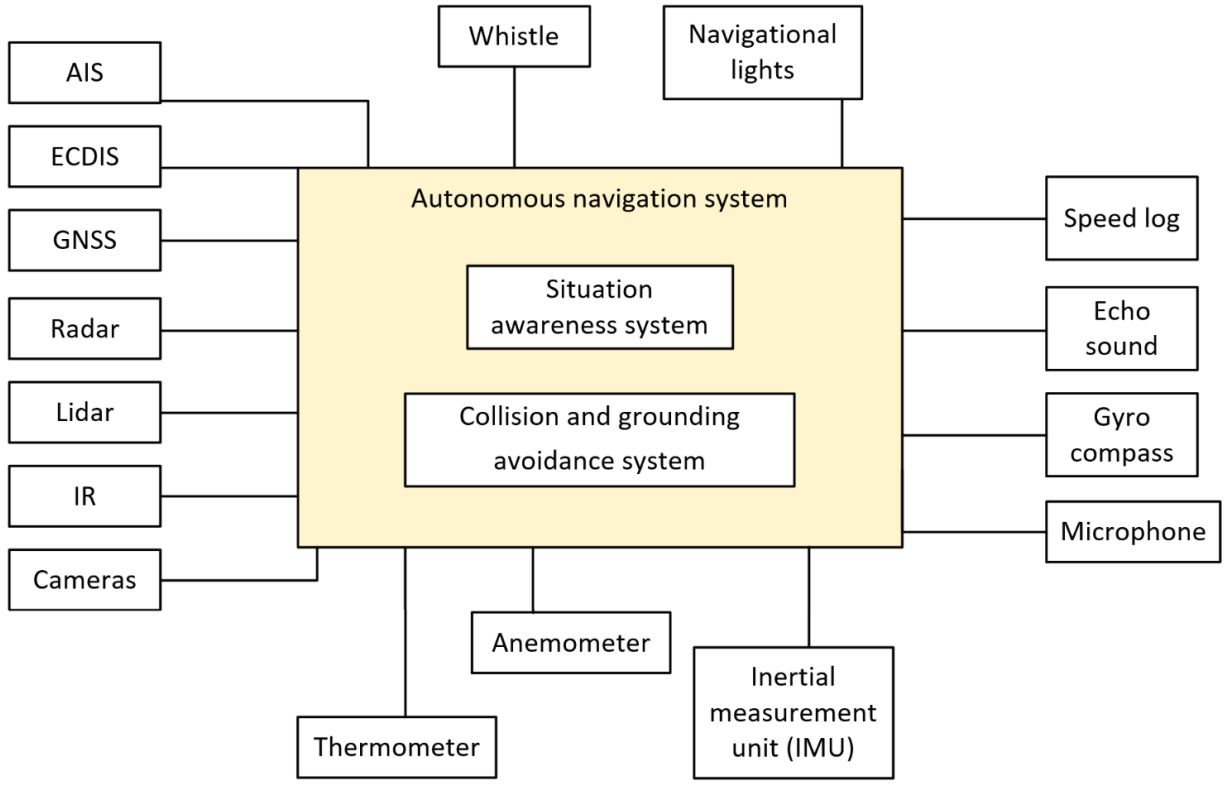


Figure 9: Overview of autonomous navigation system related equipment

2.4.3 Redundancy philosophy

Figure 10 illustrates the redundancy principle of the vessel's systems, meaning that they can handle single failures. This applies to both the propulsion, as was seen in Figure 6, and to the control systems. The control system is segregated into A and B sides where the Autonomous Navigation System (ANS) is physically separated. Only one side will be operational at a time, but both sides will be fully synchronized, meaning the other side should be able to take over immediately if one side should fail. The sensors/units refer to the physical hardware/equipment and propulsion.

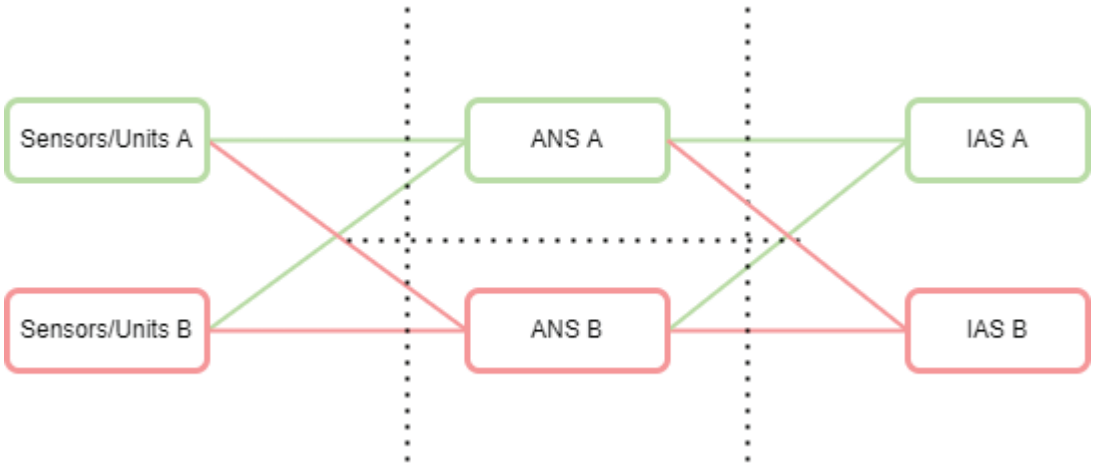


Figure 10: System's redundancy principle

2.4.4 RCC capabilities

In this subchapter, a preliminary description of the systems available in the RCC and required for the operators to be able to intervene the operation are defined.

The RCC have full responsibility of the vessel's operation, and therefore the vessel does not require qualified operators onboard. For tasks requiring human assistance it is assumed that the RCC operator will be alerted in form of a visual and/or audible alarm in a similar manner as would be the case for a conventional bridge system. The capabilities of the RCC and operational roles are further described in Chapter 2.5.

Note that this ConOps is only focused on the mission and operations selected in Table 1. I.e., the following lists and overviews are not exhaustive.

Basic and continuous functionality

The RCC will have a telecommunication system in place in order to ensure stable and normal operation. The connection control system involves the communication data/link between the short-sea cargo vessel and the RCC and is dependent on antennas and cellular network coverage. This system is used to receive and transmit information to and from the vessel.

Navigation related functionality

The RCC consists of a Bridge and ECR workstation designed to provide equivalent function and interface as if the operation was conducted onboard the vessel. Thus, interfacing data from the same instruments as found on the Bridge and ECR, such as: ECDIS, AIS, radar, lidar, echo sounder, loading computer, IAS, PMS etc. High quality cameras provide live view from the bridge for visual monitoring of traffic and navigational hazards. Likewise, CCTV are covering the entire vessel and interface to displays in the RCC. The instruments for each vessel are displayed on multi-function displays (MFD), enabling each screen to show vessel data for all three vessels (the fleet). A larger screen display is provided to give a visual overview of the more critical issues that may occur (e.g., navigational data and status and performance of main ship functions).

The vessel is equipped with additional sensors and equipment related to situational awareness and collision and grounding avoidance which is not a part of the vessel's own situational awareness system. This system is for the RCC operators in case the situational awareness system of the ship should fail. Additionally, the RCC is equipped to monitor the fleet, independently from the information feed from the vessels themselves, through the use of shore-based radar and AIS information.

2.5 Operational roles

Qualified operators will supervise the vessel operation from the RCC and interfere if one or more of the vessel systems are outside defined parameters. The operators require maritime competence to understand the functions and actions executed by the systems. Hence, maritime competence from both bridge/deck and engine department is required. This competence is already defined by the STCW conventions (IMO, 1974) and serves as basic requirement for RCC operators. In addition, more specialized competence regarding the autonomous system is required.

The RCC will be manned by four vessel operators working in shifts of two. The primary responsibility of the personnel is risk management, to supervise the operation ensuring that it progresses according to plan and observe that situations with potential hazards do not escalate. Personnel in the RCC also have the ability to intervene and control certain functions on board as described in Chapter 2.4.2.

Table 4: RCC operator responsibilities

Department	Title	No.	STCW	Responsibility	Duty
Bridge, deck, and engine	RCC operator	2	II/2	- Navigational supervision - Machinery supervision	4 hrs on, 4 hrs off
			II/5	- Supervise all bridge equipment - Supervise all deck equipment - Supervise cargo handling (load/discharging, securing) - Supervise vessel stability, integrity and ballast mgt.	
			III/5, III/6	- Supervise all engine machinery and equipment - Supervise all electrical equipment	
Port	Cargo operator	1		- Supervise loading/unloading	

3 CONOPS CONCEPT B – SMALL PASSENGER FERRIES

3.1 Overall description

The small passenger ferries concept is a relative low-cost and high benefit socio-economical solution to increasing transport efficiency. It gives flexibility and a new tool for city planners, enabling new means of transport and opening new areas. By using the waterway, these ferries can help reduce traffic on the roads, and due to short and fixed routes, be fully electric, making it an environmentally friendly alternative.

The fleet consists of ten unmanned battery driven sister vessels, allowing for on-demand transport and full availability for passengers. This means that the passengers should be able to order a ferry when needed. The fleet perspective and operation profile facilitate for a human supervisor on shore supervising a large number of ferries, only interfering in case of an alarm. This leads to relatively low crew costs. The vessels operate in enclosed/sheltered waters.

Although the fleet of ferries could operate to several ports in the inner Oslofjord, this ConOps only focuses on the route between Aker Brygge and Hovedøya.

3.2 Mission description

The overall purpose of the small passenger ferries is to transport passenger in a safe, frequent, and reliable manner between stops in the Oslo fjord. This ConOps, which is limited to the four concept-function combinations presented in the Third RBAT report (DNV, 2022), the missions and operations considered are given in Table 5.

Table 5: Mission specification selected for the small passenger ferries concept

	Concept-function combination #1	Concept-function combination #2	Concept-function combination #3	Concept-function combination #4
Mission phase	Transit to location	Transit to location	Transit to location	Emergency response in Transit
Traffic density	High	High	High	High
Operation	Navigate through enclosed/sheltered waters	Navigate through enclosed/sheltered waters	Navigate through enclosed/sheltered waters	Perform evacuation (fire)
Functions	*Perform navigation:* - Perform voyage planning - Observe surroundings - Follow planned route *Perform manoeuvring:* - Provide steering - Provide acceleration/ deceleration	*Perform collision and grounding avoidance:* - Detect vessels/ objects - Classify vessels/ objects - Observe vessels/ objects movements (heading and speed) - Determine vessels/ objects relative position, distance and movement (bearing) - Determine CPA/TCPA for vessels/objects - Implement collision and grounding avoidance strategy	*Maintain communication:* - Communication/ data link between RCC and ferry	*Provide means for evacuation:* - Mitigate fire - Guide passengers - Evacuate vessel *Perform navigation:* Observe surroundings *Perform manoeuvring:* - Provide steering and speed adjustments to move away from objects or approach quay/land (MRC) - Call for assistance (MRC) - Drop anchor (MRC)
Supervision	Passive supervision	Passive supervision	Passive supervision	Active supervision

3.2.1 Operational tasks

The small ferries transport passenger between the islands in the inner Oslofjord. As presented, the mission phases *transit to location* and *emergency response* are in focus. The transit is assumed to be between Oslo city centre and the closest island, and the emergency response is assumed to happen during transit. Three of the operations of the concept-function combinations are navigation, while the fourth is evacuation related to a fire scenario. A variation of functions has also been decided for each operation which will be further described in the following chapters.

3.2.2 Operational area and conditions

The vessels operate in the inner Oslofjord transporting passengers between stops along the fjord and on the islands. In the continued study the itinerary is limited to a single crossing; from the Aker brygge in Oslo city centre to Hovedøya, the closest island, as shown in Figure 11. The distance is approximately 1.3 km, or 0.7 nautical miles, and the area is defined as enclosed waters, *Fartsområde 1*. This means that it is an area not normally exposed to high waves. Still, the vessels may occasionally encounter heavy weather.

The depth is approximately 6 m at Aker brygge, increases to 21 m approximately 250 m from the quay, before decreasing again at approximately 90 m from Hovedøya. At the Hovedøya quay the depth is 3 m.

Figure 11: The route of the small passenger ferries, from Aker brygge to Hovedøya

The area has high traffic density as shown in Figure 12 and indicated with the black dotted ellipse. The traffic around the route from Aker Brygge to Hovedøya is mainly characterised by crossing general cargo vessels and passenger vessels. Other types of vessels can also be encountered. The area is popular for pleasure crafts, kayakers, stand-up paddle boarders and swimmers.

Sailing in the area is governed by “Havne og farvannsloven” (Lovdata, 2022), and is under surveillance by Horten VTS as indicated by the green area in Figure 13.

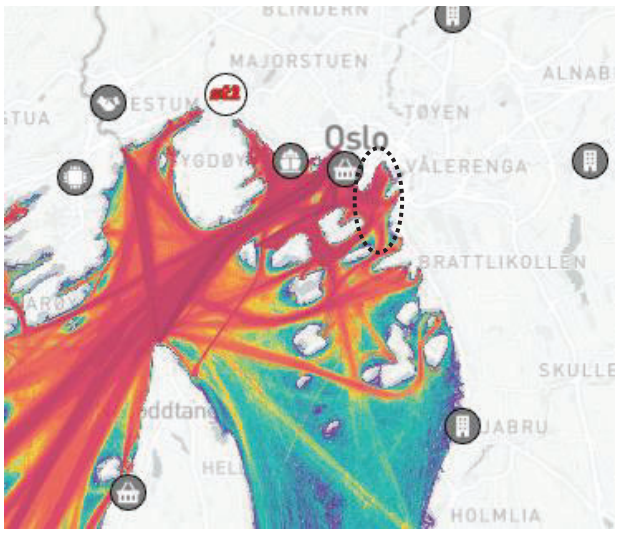


Figure 12: Traffic density in Indre Oslofjord (MarineTraffic, 2022)

Figure 13: Horten VTS control area (Kystverket, 2022)

Both Aker Brygge and Hovedøya quay are equipped with a docking area tailored for the small passenger ferries for safe and efficient embarkation and disembarkation of passengers. Infrastructure for automatic charging is available at the quay by Aker Brygge. The charging is high speed so that the ferry doesn't have to spend long periods at the quay.

3.2.3 Weather and sea-state limitations

The inner Oslofjord area is sheltered and and is therefore not normally exposed to strong wind or high waves. Still, the vessels may occasionally experience heavy weather. Figure 14 shows the wind speed direction, and frequency (in percent) for Bjørvika, which is 1.3 km, or 0.7 nm, East of Aker Brygge. Winds of 0-5 m/s have the highest frequency of approximately 6 %, from Northeast. Winds of 5-10 m/s and 10-15 m/s are mainly from South, with frequencies of approximately 4.5 % and 1 % respectively. Stronger winds are indicated by dots in the middle of the rose, indicating the frequency is very low, and a governing direction can't be concluded.

Figure 15 shows historical wave data from the last two years. The maximum wave height has been approximately 0.7 m, while most of the waves were around 0.1 m.

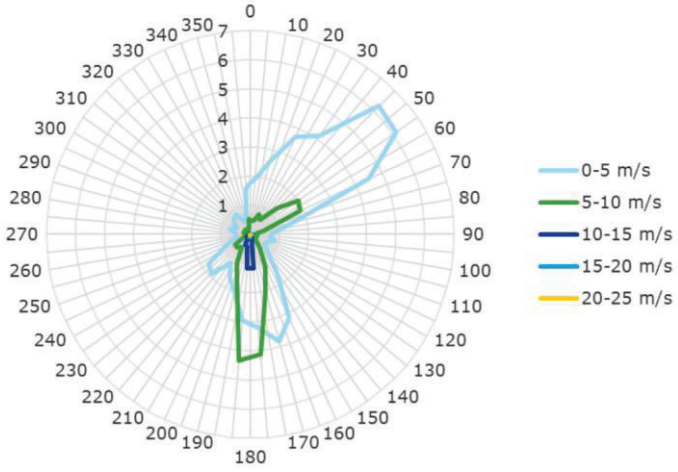


Figure 14: Wind rose for Bjørvika (DNV, 2017)

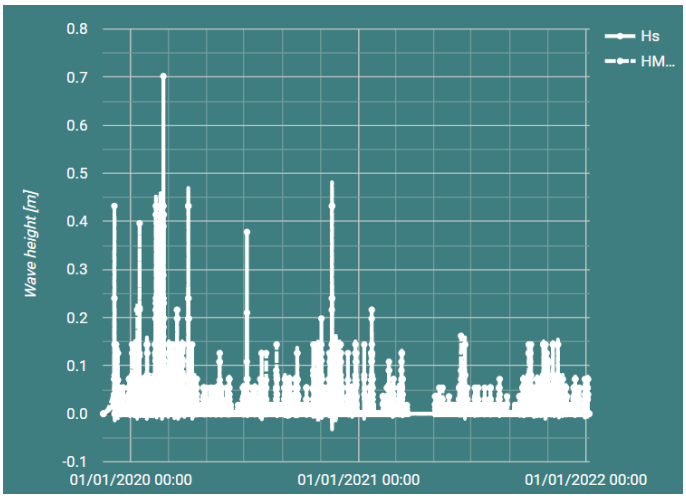


Figure 15: Historical wave heights (Norce, 2022)

3.3 Main characteristics

3.3.1 Key vessel characteristics

The general characteristics, including ship dimensions for the small passenger ferries, is described in Table 6. The ferries are electrically powered and will be charged by power from shore while docked. Propulsion and manoeuvrability are provided by four azimuth thrusters.

Table 6: Ship characteristics for small passenger ferries

Route	Aker Brygge – Hovedøya
Type	Passenger ferry
LOA	8 m
Beam	3 m
Draught	1.5 m
Capacity	12 passengers
Design speed	5 kn

3.3.1.1 Power generation and propulsion

The propulsion arrangement ensures redundancy and reliability by using segregated systems, as shown in Figure 16. There are two separated main battery rooms with respective switchboards. The capacity will be dimensioned for a return trip for the route presented in this case, plus allowance for contingencies. This requires starting with fully charged batteries at the starting point.

Propulsion and maneuvering capabilities will remain operational in case of a single failure in propulsion- or auxiliary systems. As shown in Figure 16 this is obtained with four azimuth thrusters, each pair supplied from separate switchboards. Further, a bus-tie between the switchboards can be closed in order to supply consumers on both sides.

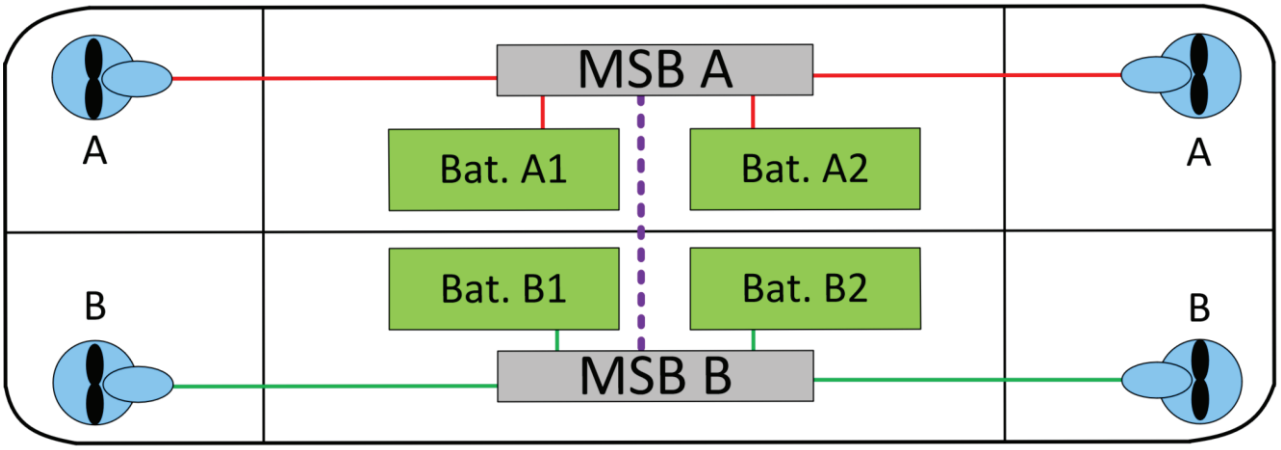


Figure 16: Propulsion redundancy philosophy

3.3.2 Remote control centre characteristics

There is one remote control centre (RCC) responsible for supervising the fleet of small passenger ferries, located in the Oslo area. The RCC consists of the control room, equipment room, an emergency preparedness room, and a resting area with facilities such as restroom, small kitchen, etc. All essential equipment is configured with redundancy to prevent system breakdown caused by any single point of failure. In addition, the equipment is connected to UPS and an emergency generator providing power redundancy in case of power outage.

3.3.3 Communication link characteristics

The communication link is based on the cellular network coverage in the area. Figure 17 shows that the whole route from Aker brygge to Hovedøya has 5G coverage, with 4G+ areas nearby. This is an example from one of the available cellular network providers in the Oslo area. The bandwidth required by the vessel and/or the RCC depend on the mission phase/situation, with estimated higher requirement when entering/leaving port and/or transfer to an MRC takes place.

The vessels verify connection status at start-up/before departure. The status of the communication is continuously and automatically monitored while the vessel is in operation. For redundant 5G coverage two cellular network providers can be considered.

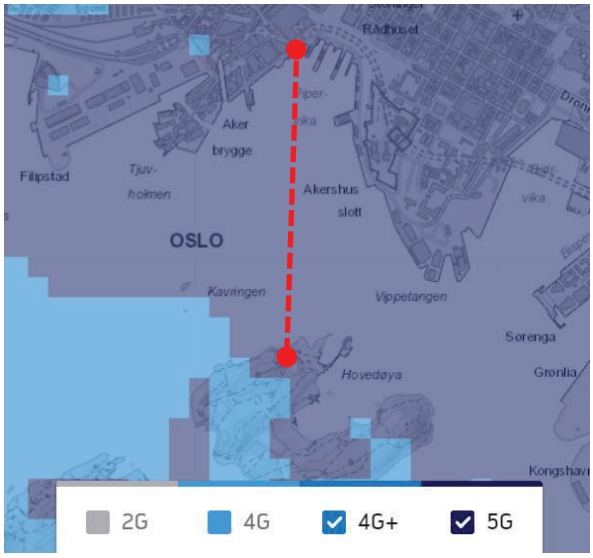


Figure 17: Cellular network coverage around Aker brygge and Hovedøya (Telenor, 2022)

3.4 Description of autonomous systems

In this chapter a preliminary description of the onboard systems is given. Note that additional systems and functionalities are necessary for the vessel to be operational, and that this ConOps is focused on the mission and operations selected in Table 5. I.e., the following lists and overviews are not exhaustive.

3.4.1 Functionality

Basic and essential continuous functionalities:

Some of the systems on the vessel have functionalities which need to be in place and stable to enable normal operation. These are the electric power system and the integrated automation system (IAS).

- Monitoring the state of charge, loads, electric consumers, and management of charging are conducted by the electric power system. This power system status is important for planning of trips according to the timetable, planning for charging, and for information about the vessel's capacity in case of an event.
- An IAS integrates the various control systems onboard the vessel and makes it possible for users that are onboard a vessel to control and monitor all those systems from a single user interface. For this small passenger ferry, the IAS will in addition forwarded monitoring data to the autonomy system and the RCC, and it will distribute commands received from the autonomy system and the RCC to the relevant systems onboard the vessel. Since it facilitates the command flow to the propulsion and motional control system, failures in the IAS may potentially lead to no or reduced capabilities for propulsion and steering.

Navigation and manoeuvring related functionalities:

The autonomous navigation system is the overall control system responsible for navigation and consists of the situation awareness system, the voyage planning system, and the collision and grounding avoidance system. Based on interaction with these systems the autonomous navigation system controls speed and direction with the propulsion and motion control system. The systems are further described in the following.

- The situation awareness system manages and utilises the information about the vessel surroundings from AIS, ECDIS, GNSS, radar, lidar, IR, cameras, speed log, echo sound, gyro compass, microphone, thermometer, anemometer, and inertial measurement unit (IMU).

- The voyage planning system generates the optimal route for the vessel, based on external conditions (such as weather and traffic), internal conditions (e.g., state of charge of batteries), and the timetable.
- When the vessel prepares to leave the dock, the collision and grounding avoidance system utilises information from the situation awareness system to determine whether the vessel can continue as planned or adjustments are required to avoid collision or grounding.
- The propulsion and motion control system ensures acceleration, deceleration, and directional change of the vessel, with the azimuth thrusters.

Communication related functionalities:

There are three communication related systems onboard: internal communication, external communication, and the telecommunication system where the latter enables contact and communication and remote control from the RCC.

- The external communication concerns communication with other vessels by the use of VHF radio. Any incoming call is routed to the RCC via the datalink, as there are no personnel onboard. It is the remote operator who is responsible for receiving the call and responding appropriately. Any outgoing VHF call is routed via the datalink from the RCC to the vessel and from there to the receiver using the vessel's VHF radio.
- Internally onboard the vessel a public address (PA) system is used for communication with the passengers. It is most frequent used to play pre-recorded information messages related to the standard operational phases, but the system also has messages to guide the passengers in an emergency. Further, the system has the functionality of two-way communication with the RCC. The remote operator can override pre-recorded messages and give information or instructions directly if needed.
- Communication data/link between ferry and RCC is handled by the telecommunication system and is dependent on antennas and cellular network coverage. A similar system is located in the RCC to receive the data stream from the ferry and transmit commands to the ferry.

Emergency response – evacuation due to fire:

The emergency response in focus for the small passenger ferries is a fire scenario where the passengers are to be evacuated. In addition to relevant systems mentioned above, e.g., communication systems, navigational systems, an evacuation due to fire requires a lifesaving appliance (LSA) system and a fire mitigation and control system.

- The LSA system consists of the life rafts, their deployment arrangement, and a control system. The life rafts are released either automatically by the control system, remotely by the remote operator, or locally by any of the passengers.
- The fire mitigation control system has two sub systems, the fire and smoke detection system, and fire extinguishing system. The fire and smoke detection system will quickly detect any smoke or fire and will sound alarms onboard and in the RCC. The alarm can also be started locally by passengers. The fire extinguishing system isolates the affected area, e.g., a battery compartment, releases the fire suppression medium.

3.4.2 Hierarchical structure

Figure 18 illustrates the hierarchical control structure of the Small Passenger Ferry. The structure represents the ship systems and their subsystems, as described in Chapter 3.4.1. Each of the functions is performed by a system of the autonomous vessel. Connections between the different systems are represented by arrows. The RCC supervises the operation and can take direct control of the different systems outlined in green if

necessary. The integrated automation system (IAS) is the integrator and facilitates control and monitoring of the different systems onboard.

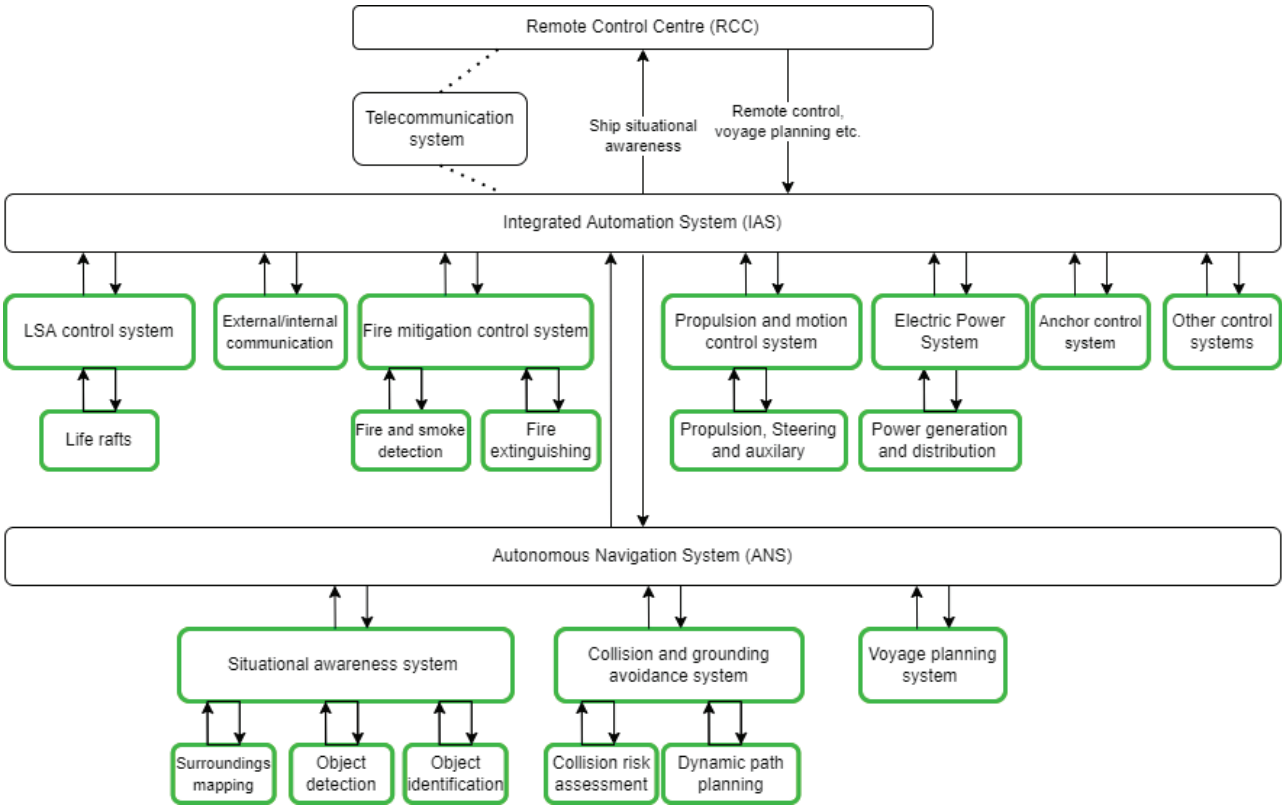


Figure 18: Small Passenger Ferry hierarchical control structure

Figure 19 shows the specific equipment and hardware which is part of the autonomous navigation system.

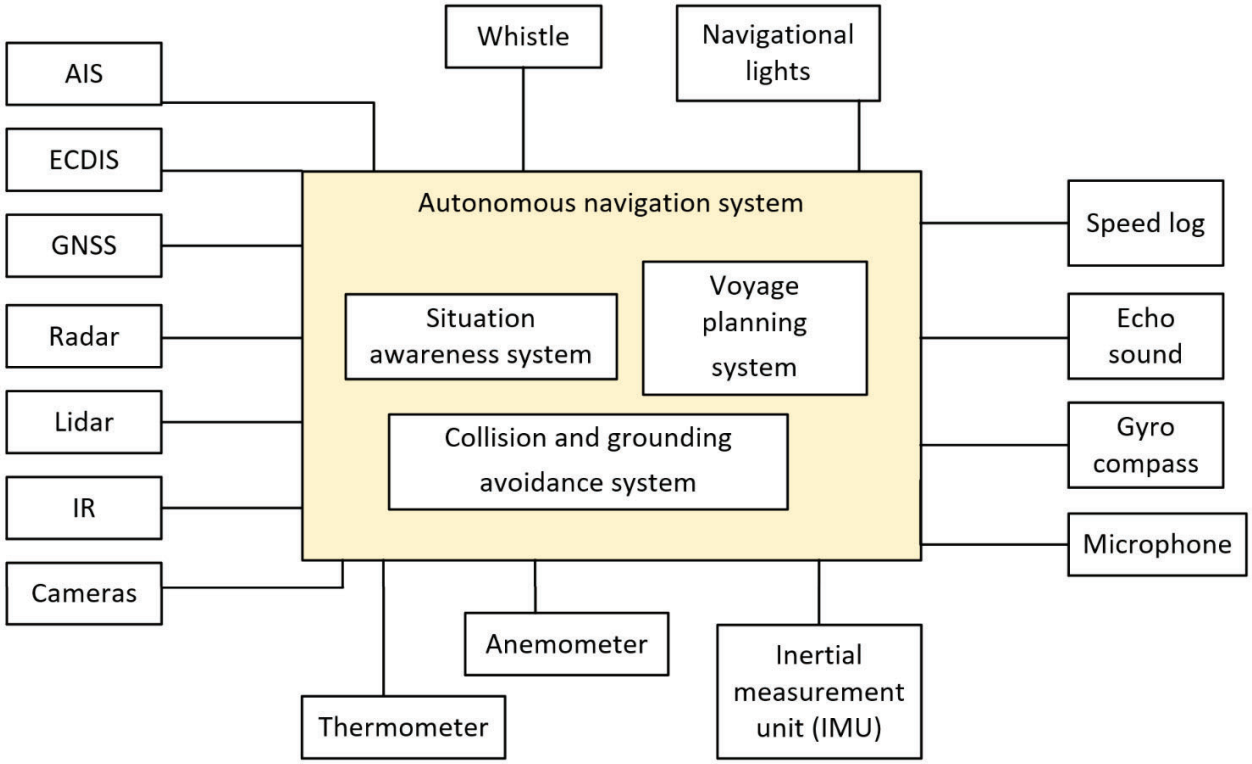


Figure 19: Overview of autonomous navigation system related equipment

3.4.3 Redundancy philosophy

Figure 20 illustrates the redundancy principle of the vessel's systems, meaning that it can handle single failures. This applies to both the propulsion (as seen in Figure 16) and the control systems. The control system is segregated into A and B sides where the Autonomous Navigation System (ANS) is physically separated. Only one side will be operational at a time, but both sides will be fully synchronized, meaning the other side shall be able to take over immediately if one side should fail. The sensors/units refer to the physical hardware/equipment and propulsion.

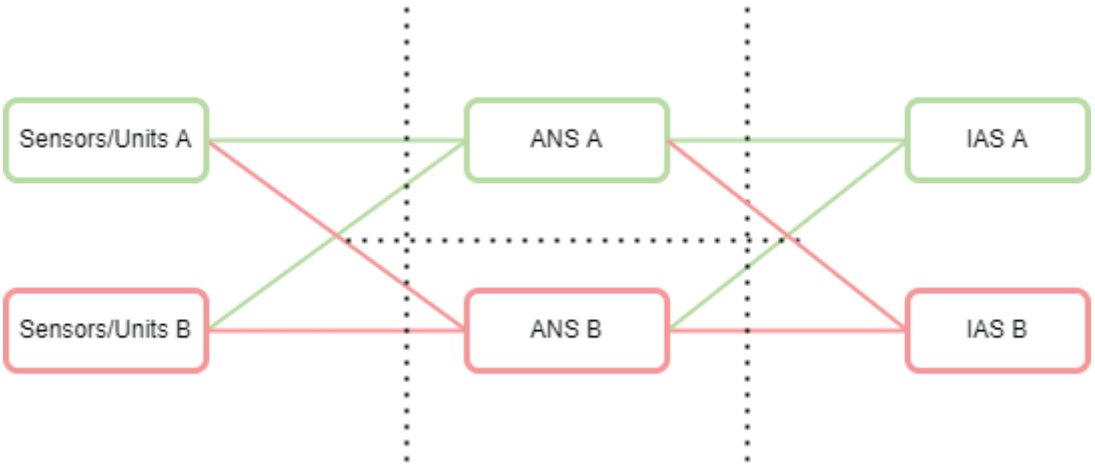


Figure 20: System's redundancy principle

3.4.4 RCC capabilities

In this subchapter, a preliminary description of the systems available in the RCC and required for the operators to be able to intervene the operation will be defined.

The RCC have full responsibility of the vessel's operation and the vessel does not require qualified operators onboard. For tasks requiring human assistance it is assumed that the RCC operator will be alerted in form of a visual and/or audible alarm in a similar manner as would be the case for a conventional bridge system. The capabilities of the RCC and operational roles are further described in Chapter 3.5.

Note that this ConOps is only focused on the mission and operations selected in Table 5. I.e., the following lists and overviews are not exhaustive.

Basic and continuous functionality

The RCC will have a telecommunication system in place in order to ensure a stable and normal operation. The telecommunication system involves the communication data/link between the small passenger ferry and the RCC and is dependent on antennas and cellular network coverage. This system is used to receive information from the ferry as well as transmitting commands the other way.

Navigation related functionality

The RCC consists of a Bridge and ECR workstation designed to provide equivalent function and interface as if the operation was conducted onboard the vessel. Thus, interfacing data from the same instruments as found on the Bridge and ECR such as: ECDIS, AIS, radar, lidar, echo sounder, loading computer, IAS, PMS etc. High quality cameras provide live view from the bridge for visual monitoring of traffic and navigational hazards. Likewise, CCTV are covering the entire vessel and interface to displays in the RCC.

The instruments for each vessel are displayed on multi-function displays (MFD), enabling each screen to show vessel data for all three vessels (the fleet). A larger screen display is provided to give a visual overview of the more critical issues that may occur (e.g., navigational data and status and performance of main ship functions).

The vessel is equipped with additional sensors and equipment related to situational awareness and collision and grounding avoidance which are not a part of the vessel's own situational awareness system. Additionally, the RCC is equipped to monitor the fleet, independently from the information feed from the vessels themselves, through the use of shore-based radar and AIS information.

3.5 Operational roles

Qualified operators will supervise the vessel operation from the RCC and interfere if the vessel system is outside defined parameters. The operators require maritime competence to understand the functions and actions executed by the system. Hence, maritime competence from both bridge/deck and engine department is required. This competence is already defined by the STCW conventions (IMO, 1974), and serves as basic requirement for RCC operators. In addition, more specialized competence regarding autonomous system is required.

The RCC will be manned by four vessel operators working in two shifts. The primary responsibility of the personnel is risk management, and to supervise the operation ensuring that it progresses according to plan and observe that situations with potential hazards do not escalate. Personnel in the RCC also can intervene and control functions on as described in Chapter 3.4.2.

Table 7: RCC operator responsibilities

Department	Title	No.	STCW	Responsibility	Duty
Bridge, deck, and engine	RCC operator	2	II/3	- Navigational supervision - Machinery supervision	4 hrs on, 4 hrs off
			II/5	- Supervise all bridge equipment - Supervise all deck equipment - Supervise vessels stability, integrity and ballast mgt.	
			III/5, III/6	- Supervise all engine machinery and equipment - Supervise all electrical equipment	
			V/2	- Passenger handling	

4 CONOPS CONCEPT C – RO-PAX FERRY WITH ASSISTANT SOLUTIONS

4.1 Overall description

'Assistant solutions' can potentially help reduce fuel costs, crew costs and improve overall operation, making the vessels more reliable, flexible, and safer. By introducing these solutions through increased automation of specific functions, like auto-crossing and auto-docking or certain engineering functions, the technology can be gradually introduced and tested without having to challenge the current regulations. The expected benefits are better operator support, more efficient use of resources (fuel, battery power, winds/currents/waves), and reduced workload for the crew and operators.

The fleet of Ro-Pax ferries will consist of three hybrid sister vessels, sailing in different locations in Norway. The vessels will have reduced manning, meaning there will only be bridge- and deck crew on board. Due to 'assistant solutions', there will be fewer people in the teams than usual. The bridge- and deck crew will be responsible for supervising the normal operation and autonomous functions, while the chief engineer will be supervising the vessels from a remote-control centre (RCC). The ferries should be able to handle the same number of passengers and vehicles as before. For the scope of this ConOps, only the route between Mortavika and Arsvågen in Boknafjorden will be analysed.

4.2 Mission description

This ConOps is limited to the four concept-function combinations presented in the third RBAT report (DNV, 2022), as shown in Table 8. Functions related to the propulsion system are in focus, where the chief engineer, located in a remote-control centre, is expected to play a part in case of failures.

Table 8: Mission specification selected for the Ro-Pax ferry concept

	Concept-function combination #1	Concept-function combination #2	Concept-function combination #3	Concept-function combination #4
Mission phase	Arrival in port	Activities in port	Depart from port	Transit to location
Traffic density	Low	NA	Medium	Medium
Operation	Perform docking	Re-plenish consumables	Perform harbour manoeuvring	Handle blackout (back-up power available)
Functions	*Perform navigation:* -Determine vessel position & relative distance *Perform manoeuvring:* - Provide steering - Provide acceleration/ deceleration -Maintain position *Embark/disembark crew & passengers:* -Operate ramp	*Perform manoeuvring:* - Maintain position *Provide electrical power:* -Charge/receive electrical power from shore	*Embark/disembark crew & passengers:* -Operate ramp *Provide electrical power:* -Generate power -Distribute electrical power	*Maintain communication (data, voice/sound, visual signalling):* - Use AIS and light signals to notify other ships - Notify authorities -Notify other ships -Call for tug assistance *Integrated monitoring and control:* -Restart system *Perform anchoring:* -Emergency release of anchor (MRC)
Supervision	Active supervision	Passive supervision	Passive supervision	Active supervision

4.2.1 Operational tasks

The Ro-Pax ferry is transporting passengers and vehicles between Mortavika and Arsvågen in Boknafjorden. As presented, the operations in focus are *perform docking*, *re-plenish consumables*, *perform harbour manoeuvring*, and *handle blackout*, with the utilisation of the partly automated assistant solutions.

4.2.2 Operational area and conditions

The ferries will sail in enclosed waters in different locations in Norway. This ConOps is limited to the single crossing between Mortavika and Arsvågen. The route is located in the Boknafjord which has medium traffic density. This is illustrated in Figure 21 which shows AIS tracks for all the vessels in the area from 2019. The traffic in the area is both for utility and recreational purposes.

The distance between the quays is 4.2 nautical miles and will take the ferry approximately 25 minutes to cross with a service speed of 12 kn. The depth at the port in Mortavika is 5.5 m, and 10 m at the quay in Arsvågen. The maximum depth of the route is approximately 600 m.

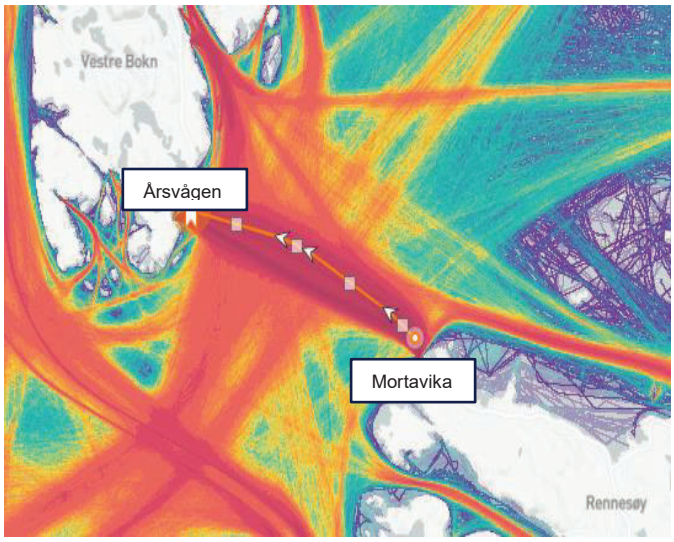


Figure 21: Route between Mortavika and Arsvågen (MarineTraffic, 2022)

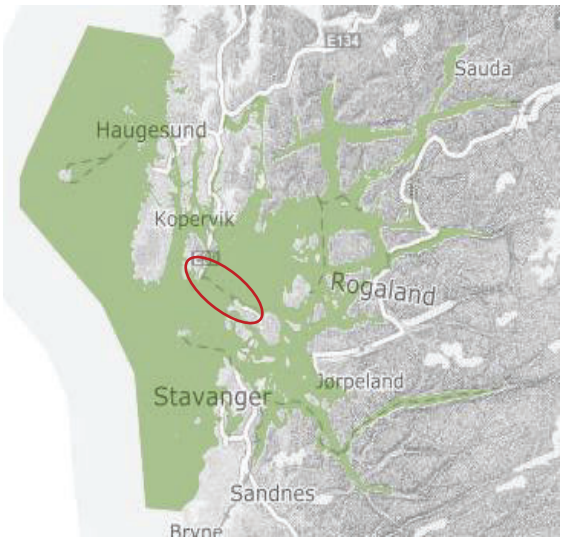


Figure 22: Kvitsøy VTS area (Kystverket, 2022)

Sailing in the area is governed by “Havne og farvannsloven”, and under surveillance by Kvitsøy VTS as shown in Figure 22. In the specific area, there are no safe harbours in proximity to the route. The harbours in Mortavika and Arsvågen will therefore be considered as *Safe harbours* in relation to MRC’s.

4.2.3 Weather and sea state limitations

The Boknafjord is a relatively open area and can be exposed to heavy weather. Figure 23 and Figure 24 shows the distribution and speed of wind and the wave profile respectively in the actual area. Wind speeds up to 20 m/s and wave heights up 11 m can occur.

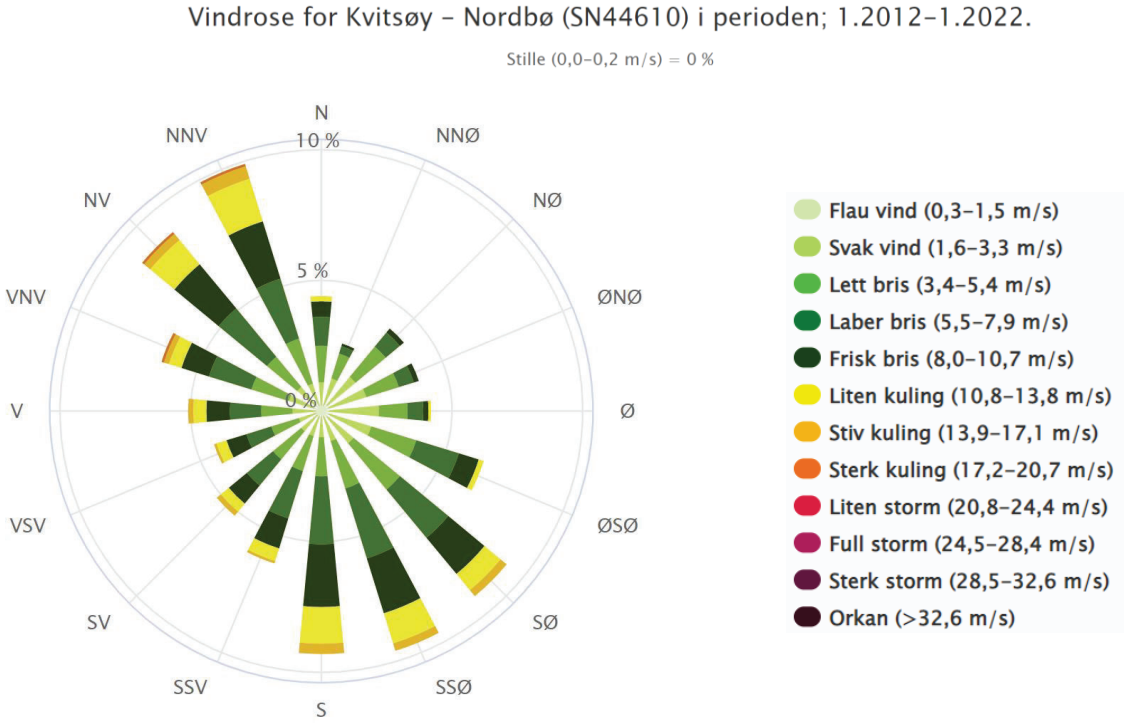


Figure 23: Wind rose, Kvitsøy last 10 years (Norsk Klimaservicesenter, 2022)

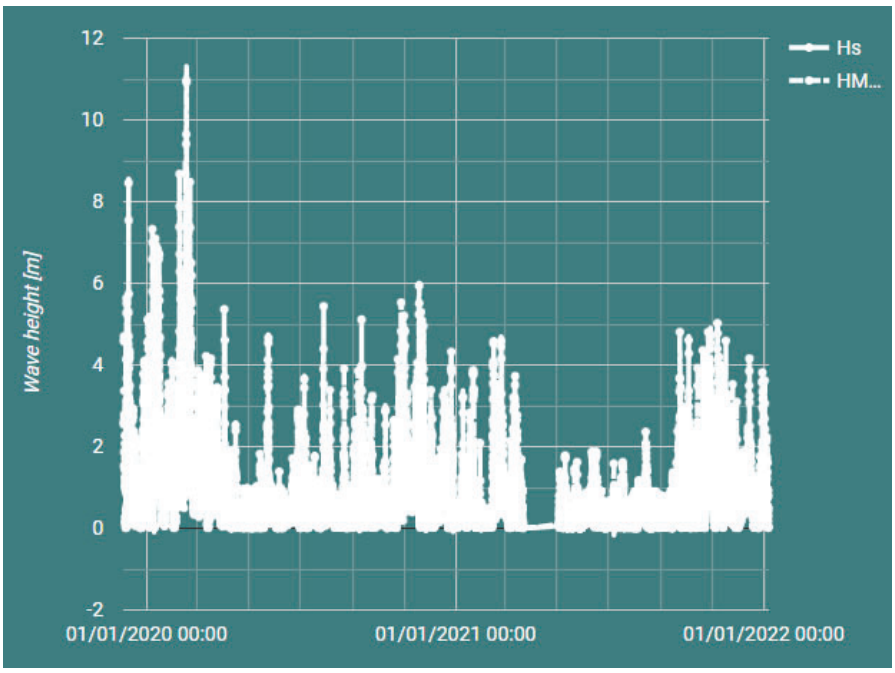


Figure 24: Wave profile Mortavika-Arsvågen, last 2 years (NORCE, 2022)

4.3 Main characteristics

4.3.1 Key vessel characteristics

The ship characteristics for the Ro-Pax ferry is given in Table 9 below. The ferry has diesel electric propulsion. Both quays are equipped with automatic charging capabilities able to charge the batteries with up to 7 200 kW.

Table 9: Ship characteristics for Ro-Pax

Route	Mortavika – Arsvågen
Type	Ro-Pax
LOA	144 m
Beam	20 m
Draught	5 m
DTW	1350
Capacity	600 passengers / 200 cars
Design speed	12 kn

4.3.1.1 Power generation and propulsion

The vessel will be powered by rechargeable batteries located in segregated battery rooms. Switchboards are located as shown in Figure 25, and is responsible for distribution of electric power via DC. The capacity will be dimensioned for a return trip for the route presented in this case, plus allowance for contingencies. This requires starting with fully charged batteries at the starting point.

A redundant propulsion system will be installed onboard to ensure that propulsion and maneuvering capabilities will remain operational in case of a single failure in propulsion- or auxiliary systems. As shown in Figure 25 this is obtained with two bow thrusters, and two aft thrusters. Each supplied from separate

switchboards. Further, a bus-tie between the switchboards can be closed in order to supply consumers on both sides.

The ferry will be flexible and robust capable of running fully electric, and in hybrid mode using diesel generators.

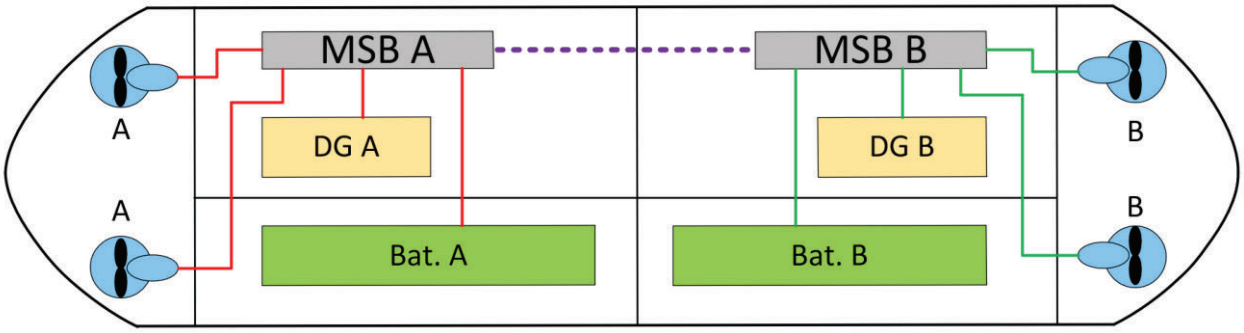


Figure 25: Propulsion redundancy philosophy

4.3.2 Remote control center characteristics

There will be one remote control center located at the west coast of Norway responsible for supervising parts of the operation of the entire fleet of Ro-Pax ferries. The RCC consists of the control room, equipment room, an emergency preparedness room, and a resting area with facilities such as restroom, small kitchen etc. All essential equipment is configured with redundancy to prevent system breakdown caused by any single point failure. In addition, the equipment is connected to UPS and an emergency generator providing power redundancy in case of power outage.

As the ferries will be manned to an extent with both crew on the bridge and on deck, the primary role of the RCC will be to monitor the machinery systems. Therefore, a chief engineer will be responsible for remotely supervising, and if necessary, take control over the machinery. Tasks include:

- Respond to alerts from vessel systems
- Observe system performance/health status of machinery
- Condition monitoring of rotating machinery

During normal operation, intervention from the RCC should not be necessary to maintain a safe operation. However, in cases where the RCC operator has to intervene, it is assumed that the RCC operator will be alerted in form of a visual and/or audial alarm in a similar manner as would be the case for a conventional bridge system.

4.3.3 Communication-link characteristics

The communication link is based on the cellular network in the area. Figure 26 shows that the whole route from Mortavika to Arsvågen has good coverage with 4G+ around the docks and 4G at the rest of the route. This is an example from one of the available network providers in the area.

The vessels verity connection status at start-up/before departure. The status of the communication is continuously and automatically monitored while the vessel is in operation.

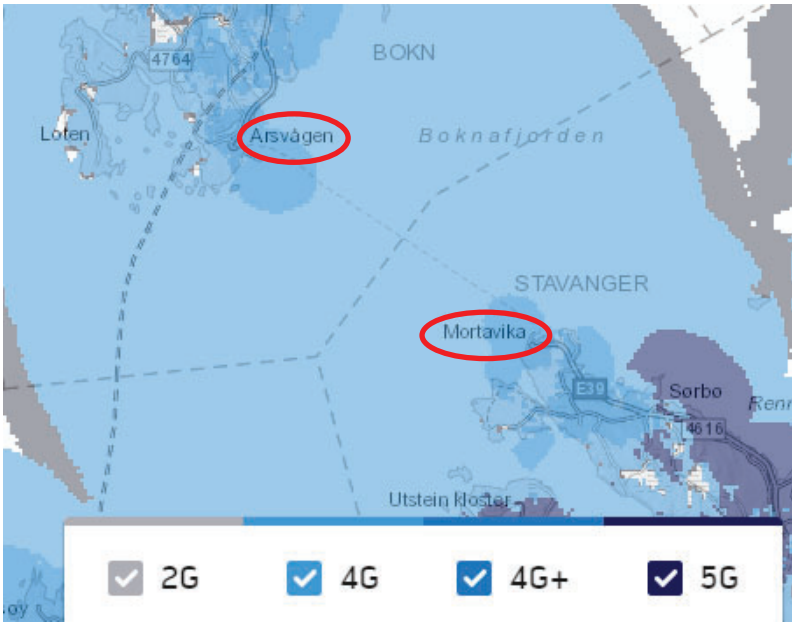


Figure 26: Cellular network coverage Mortavika-Arsvågen (Telenor, 2022)

4.4 Description of autonomous system

In this chapter a preliminary description of the onboard systems is given. Note that additional systems and functionalities are necessary for the vessel to be operational, and that this ConOps is focused on the mission and operations selected in Table 8. I.e., the following lists and overviews are not exhaustive.

4.4.1 Functionality

Basic and essential continuous functionalities:

Some of the systems on the vessel have functionalities which need to be in place and stable to enable normal operation. These are the electric power system and the integrated automation system (IAS)

- Monitoring of state of charge, loads, electric consumers, and management of charging are conducted by the electric power system. This power system status is important for planning of trips according to the timetable, planning for charging, and for information about the vessel's capacity in case of an event.
- An IAS integrates the various control systems onboard the vessel and makes it possible for users that are onboard a vessel to control and monitor all those systems from a single user interface. For this autonomous ferry, the IAS will in addition forwarded monitoring data to the autonomy system and the RCC, and it will distribute commands received from the autonomy system and the RCC to the relevant systems onboard the vessel. Since it facilitates the command flow to the propulsion and motional control system, failures in the IAS may potentially lead to no or reduced capabilities for propulsion and steering.

Navigation and manoeuvring related functionalities:

The autonomous navigation system is the overall control system of the navigation and consists of the situation awareness system, the voyage planning system, and the collision and grounding avoidance system. Based on interaction with these systems the autonomous navigation system controls speed and direction with the propulsion and motion control system. The systems are further described in the following.

- The situation awareness system manages and utilises the information about the vessel surroundings from AIS, ECDIS, GNSS, radar, lidar, IR, cameras, speed log, echo sound, gyro compass, microphone, thermometer, anemometer, and inertial measurement unit (IMU).
- When the vessel prepares to leave the dock, the collision and grounding avoidance system utilises information from the situation awareness system to determine whether the vessel can continue as planned or adjustments are required to avoid collision or grounding.
- The propulsion and motion control system ensures acceleration, deceleration, and directional change of the vessel, with the azimuth thrusters.

Communication related functionalities:

There is one communication related system onboard: The telecommunication system. This enables contact and communication with the RCC.

Communication data/link between Ro-Pax and RCC is handled by the telecommunication system and is dependent on antennas and cellular network coverage. A similar system is located in the RCC to receive the data stream from the Ro-Pax and transmit commands to the ferry.

Automatic docking and charging functionalities:

The vessel is equipped with an automatic docking system. Based on information from the situation awareness system the docking operation is initiated at the right time. The system ensures that the Ro-Pax approaches the quay with appropriate speed and heading, as well as lowering the ramp at the right moment. A charging cable is inserted when the vessel is stable and in the right position.

Emergency response – handle blackout:

The emergency response in focus for the short-sea cargo vessel is a loss of communication link scenario where the remote operators in the RCC has lost contact with the vessel. The scenario involves using the following functionalities:

- Use AIS and light signals to notify other ships (AIS, navigation lights)
- The IAS should initiate a power blackout restart sequence.
- Depending on the surroundings and situation, the vessel should drop anchor

4.4.2 Hierarchical structure

Figure 27 illustrates the hierarchical control structure of the Ro-Pax ferry. The structure represents the ship systems with assistant solutions and their subsystems, as described in Chapter 4.4.1 Each of the functions is performed by a system of the vessel. Connections between the different systems are represented by arrows. The RCC supervises the operation and can take direct control of the individual systems outlined in green if necessary. The integrated automation system (IAS) is the integrator and facilitates control and monitoring of the different systems onboard.

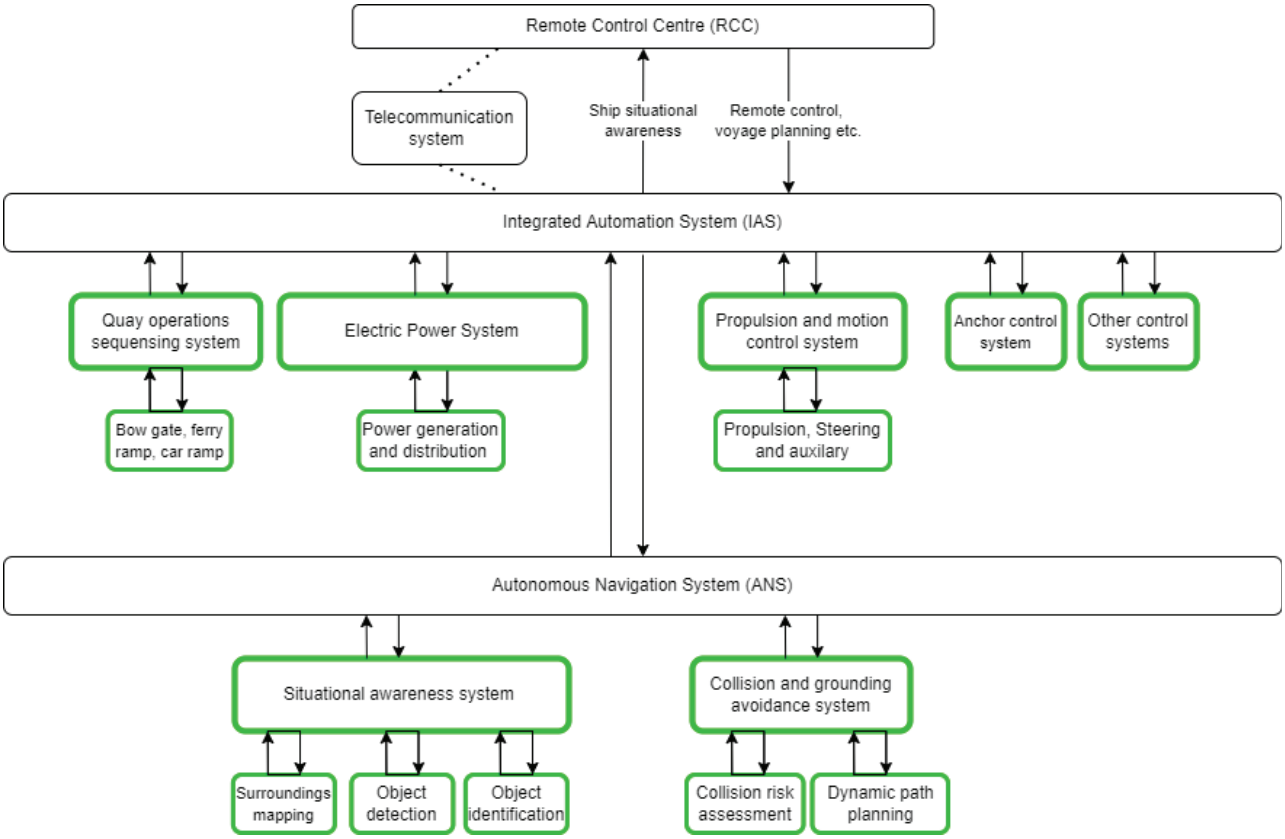


Figure 27: Ro-Pax hierarchical control structure

Figure 28 shows the specific equipment and hardware which is part of the autonomous navigation system.

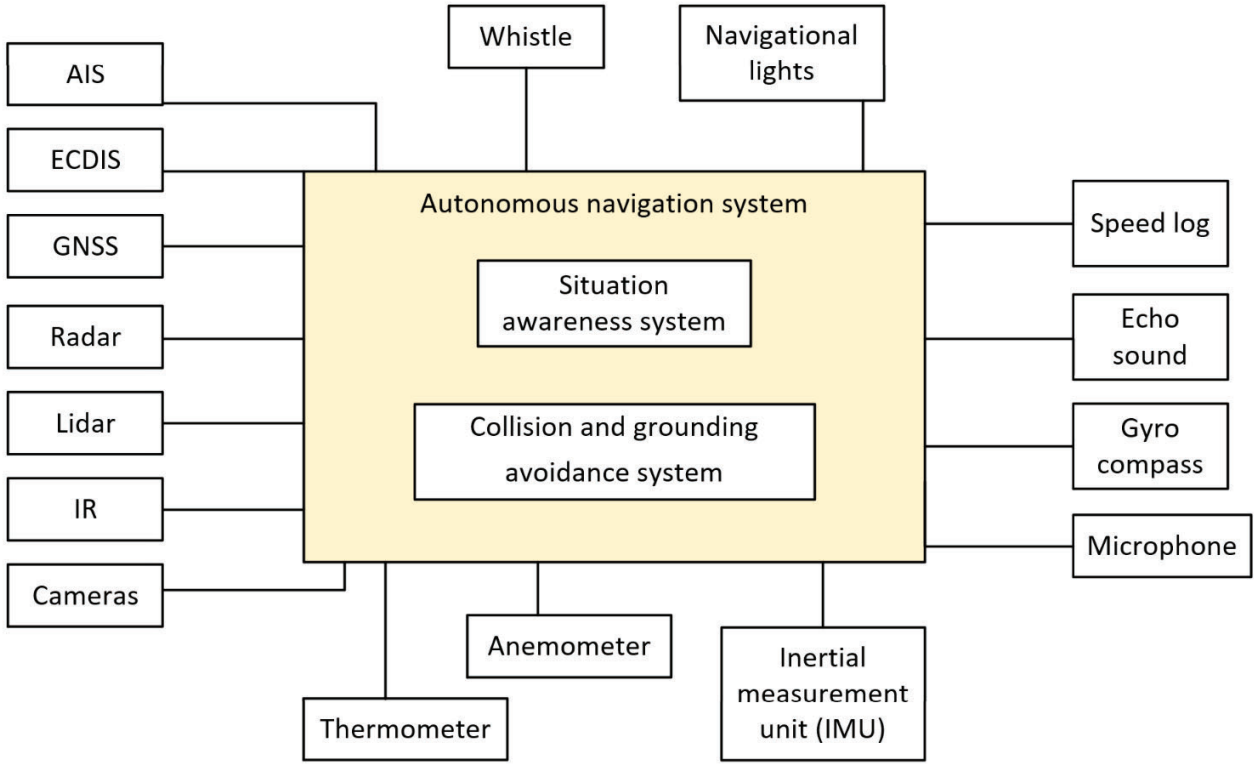


Figure 28: Overview of autonomous navigation system related equipment

4.4.3 Redundancy philosophy

Figure 29 illustrates the redundancy principle of the vessel's system, meaning that they can handle single failures. This applies to both the propulsion, as seen in Figure 25, and the control systems. The control system is segregated into A and B sides where the Autonomous Navigation System (ANS) is physically separated. Only one side will be operational at a time, but both sides will be fully synchronized, meaning the other side should be able to take over immediately if one side should fail. The sensors/units refer to the physical hardware/equipment and propulsion.

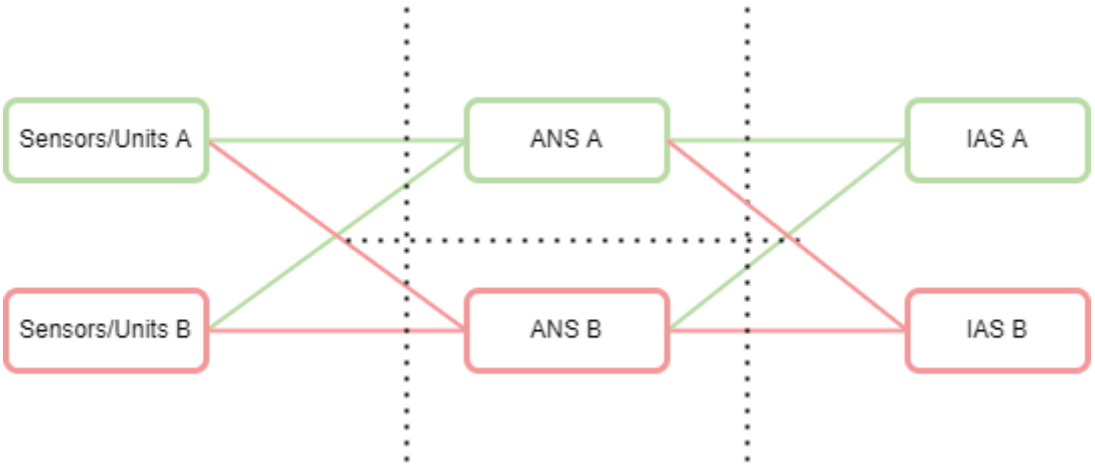


Figure 29: Systems' redundancy principle

4.4.4 RCC capabilities

In this subchapter, a preliminary description of the systems available in the RCC and required for the operators to be able to intervene the operation are defined. Note that this ConOps is only focused on the mission and operations selected in Table 8. I.e., the following lists and overviews are not exhaustive.

Basic and continuous functionality

The RCC will have a telecommunication system in place in order to ensure stable and normal operation. The connection control system involves the communication data/link between the Ro-Pax and the RCC, and is dependent on antennas and cellular network coverage. This system is used to receive information from the ferry as well as transmitting commands the other way.

Navigation related functionality

The vessel is equipped with additional sensors and equipment related to situational awareness and collision and grounding avoidance which is not a part of the vessel's own situational awareness system. In addition to this, the RCC is equipped with AIS and radar to be able to supervise the fleet.

4.5 Operational roles

The 'assistant solutions' onboard the vessel enables operation with a reduced bridge and deck crew. Their competencies are defined by the STCW convention (IMO, 1974), but more specialised expertise regarding autonomous systems is required in addition. The chief engineer works from the RCC and has full responsibility of the vessel's engine room. He/she supervises the operation and interferes if the vessel's engine systems is outside defined parameters. Here as well, the competence is defined by the STCW conventions and serves as basic requirement for the role at the RCC, in addition to competence regarding autonomous systems. Two chief engineers work in shifts at the RCC.

Table 10: Onboard crew responsibilities

Department	Title	No.	STCW	Responsibility	Duty
Bridge and Deck	Bridge Operator	1	II/2 II/5 V/2	- Navigational supervision - Supervise all Bridge equipment - Passenger handling	4 hrs on, 4 hrs off
	As. Bridge Operator	1	II/5 V/2	- Supervise all Deck equipment - Supervise vessels stability, integrity and ballast mgt. - Passenger handling	

Table 11: RCC operator responsibilities

Department	Title	No.	STCW	Responsibility	Duty
Engine	RCC chief engineer	2	II/2 III/5, III/6 V/2	- Machinery supervision - Supervise all Engine machinery and equipment - Supervise all electrical equipment - Passenger handling	4 hrs on, 4 hrs off

5 TESTING OF RBAT

The following sub-chapters presents the testing approach as well as key findings, including a selected set of examples.

5.1 Approach

The analysis was carried out using the method described in the RBAT project's Third Report (DNV, 2022). The three different ConOps' described in the current report was used to prepopulate some of the information in the RBAT, more specifically the "Normal operation" part and the "Hazard Analysis" part. During the workshop these parts were evaluated by the workshop team, before the "Mitigation analysis" was done. The team went through function-by-by function and cooperated in filling the information.

The contextual information (e.g., operating area characteristics) provided by the ConOps was used as a basis for evaluation of which unsafe condition/ modes could occur during the various mission phases and operations, the severity of potential worst-case outcomes, and whether mitigation layers could be qualified for the specific scenarios.

Before the testing was conducted, a set of requirements was identified to see if the tool was able to handle them. These were as follows:

- If the tool is able to separate between active and passive supervision
- If the tool is able to detect critical functions related to safety, and trigger specific discussions about design/solutions
- If the tool is flexible and can handle different missions and operations and abstraction levels
- If the tool is able to differentiate between risks (e.g., not all risks are red/ unacceptable)

In addition, a comprehensive set of test activities had been identified and planned for as part of the Gap Analysis documented in the Third Report. The experiences from these test activities and subsequent updates to the RBAT framework (method description) is reported in sub-chapter 5.4, Table 21.

5.2 Workshop

The testing was performed during three half-day workshops on the 8th, 18th and 21st of February. One workshop was held for each case described by the ConOps. The workshop participants are listed in Table 12, including columns specifying which days they were present. Due to time limitations, not all functions specified in the mission definition for each case were reviewed in plenary (Chapter 2.2, 3.2 and 4.2). However, prioritizations were made to ensure that most function types were addressed. Functions not covered during the workshops were analysed as a desktop exercise by the team members after the all the workshops were completed.

Table 12: Workshop team

Name	Company	Role	Workshop Day 1	Workshop Day 2	Workshop Day 3
Kenneth Kvinnesland	DNV	Senior Principal Consultant	X	X	X
Are Jørgensen	DNV	Senior Principal Engineer	X	X	X
Sondre Øie	DNV	Principal Consultant	X	X	X
Nora Helen Lund Lyngra	DNV	Senior Consultant	X	X	X
Remi Brensdal Pedersen	DNV	Consultant		X	X

5.3 Results

The following sub-chapters presents and discusses the results from the testing. Examples of findings associated with the test requirements listed in sub-chapter 5.1 are provided. The examples are structured according to the first three main parts of RBAT, i.e., use of automation (Part 1), hazard analysis (Part 2), mitigation analysis (Part 3), and risk evaluation (Part 4). Because addressing risk control (Part 5) does not include any novel aspects, and primarily refers to known practices, it was not included as part of the testing.

The entire analysis is documented in Appendix A of this report.

5.3.1 Part 1: Describe use of automation

The first part, called *use of automation*, involves describing the overall mission and operation as well as assigning the responsibility for either performing or supervising functions to software or human agents. This step also indicates at which abstraction level the analysis is performed at. Table 13, Table 14, and Table 15 shows an example from the testing where the analysis has been performed at different abstraction levels. As seen from the testing, RBAT can be performed at different function levels as long as the function can be allocated to a single performing agent. The performing agent is identified using a system hierarchy[2], here illustrated in Figure 8, Figure 18 and Figure 27. The column “Other systems and roles involved” is based on the same information and is intended to include the systems involved further down in the hierarchy. This indicates that if the performing agent identified is high up in the hierarchy, more systems will be involved in the analysis.

[2] The system hierarchy was made after the testing started.

Table 13 shows the use of automation for Small Passenger Ferry. Here, no specific control action was specified, and the high-level control function “Perform navigation” was analysed. The mission phase “Transit to location” and operation “Navigate through sheltered/sheltered waters” defined the context. Due to the analysis being done at high function level, a relatively large set of systems was included in the “Other system and roles involved” column. In this analysis the function is passively supervised.

Table 13: Use of automation for Small Passenger Ferry at a high abstraction level

USE OF AUTOMATION					
Control function	Control action	Performing agent	Supervision category	Supervising agent	Other systems and roles involved (onboard, onshore)
Mission phase: Transit to location					
Operation: Navigate through enclosed/sheltered water					
Perform navigation	N/A	Autonomous Navigation System	Passive supervision	Remote operator	- Situational awareness system - Voyage planning system - Collision and grounding avoidance system

Table 14 shows the use of automation for the Short-sea Cargo Vessel. Here the analysis is done at a lower level than for the Small Passenger Ferry. The control function is to “Perform collision and grounding avoidance” which is already at a lower level than “Perform navigation”. Here the control action “Detect vessels/objects” performed by the Situational awareness system was included as the item subject to analysis. When analysing at a lower level, less systems will be part of the analysis, as you move further down in the hierarchy. The implication is that unsafe conditions/modes associated with failures in the higher-level system are not specifically addressed. The function Detect vessels/objects is actively supervised by a remote operator.

Table 14: Use of automation for Short-sea Cargo at a low abstraction level

USE OF AUTOMATION					
Control function	Control action	Performing agent	Supervision category	Supervising agent	Other systems and roles involved (onboard, onshore)
Mission Phase: Transit to location					
Operation: Navigate through enclosed/sheltered waters					
Perform collision and grounding avoidance	Detect vessels/objects	Situational awareness system	Active supervision	Remote operator	-Surroundings mapping -Object detection

Table 15 shows the use of automation for the Ro-Pax at the same abstraction level as in Table 13.

Table 15: Use of automation for Ro-Pax at a high abstraction level

USE OF AUTOMATION					
Control function	Control action	Performing agent	Supervision category	Supervising agent	Other systems and roles involved (onboard, onshore)
Mission Phase: Arrival in port					
Operation: Perform docking					
Perform navigation	N/A	Autonomous Navigation System	Active supervision	Bridge crew	- Situational awareness system - Voyage planning system - Collision and grounding avoidance system

5.3.2 Part 2: Perform hazard analysis

Part 2 involves performing the hazard analysis, and experiences from the testing was that this part of the analysis became very similar to each other regardless of the abstraction level the test was performed at. Another experience from the testing was that the severity more than often turned out to be multiple fatalities. This is illustrated in Table 17, Table 16 and Table 18. This is not surprising for the tested functions. RBAT does not consider consequences after successful mitigation (residual losses). Instead, it considers how severe a potential outcome can become, and then that determines how effective the

mitigations must be to reduce the risk to an acceptable limit. So, for the selected cases involving navigation failures and collision with passenger carrying vessels, multiple fatalities can be expected. However, currently, RBAT does not systematically consider operational limitations and restrictions. Such an assessment may have differentiated the severities more between various scenarios.

Table 16 shows the hazard analysis for the Small Passenger Ferry where the control parameters for autonomous function “Perform navigation” are within range but incorrect. This error will not necessarily lead to an alarm and will thus affect the mitigation analysis. This is further described in sub-chapter 5.3.3.

Table 16: Hazard analysis for Small Passenger Ferry

HAZARD ANALYSIS				
Guideword	Causal factor(s)	Worst-case outcome	Accident category	Severity
Mission phase: Transit to location				
Operation: Navigate through enclosed/sheltered water				
Control parameters are within range but incorrect	Systematic/systemic failure	Collision with other vessel	Collision	Multiple fatalities

Table 17 shows the hazard analysis for the Short-sea Cargo Vessel where the autonomous function “Detect vessels/objects” is not provided because of a random hardware failure. When determining where the failure occurs, one must assume a failure in both the “performing agent” and the systems described in “Other systems and roles”. This results in more systems being the subject of a failure at a higher abstraction level.

Table 17: Hazard analysis for Short-sea Cargo Vessel

HAZARD ANALYSIS				
Guideword	Causal factor(s)	Worst-case outcome	Accident category	Severity
Mission Phase: Transit to location				
Operation: Navigate through enclosed/sheltered waters				
Not provided	Random HW failure	Collision with passenger ferry, pleasure craft.	Collision	Multiple fatalities

Table 18 shows the hazard analysis for the Ro-Pax where the autonomous function “Perform navigation” is not provided because of a random hardware failure. In this case the severity is lower than in Table 16 and Table 18, and thus illustrates how the mission phase and operation can have a mitigating effect on severity.

Table 18: Hazard analysis for Ro-Pax

HAZARD ANALYSIS				
Guideword	Causal factor(s)	Worst-case outcome	Accident category	Severity
Mission Phase: Arrival in port				
Operation: Perform docking				
Not provided	Random HW failure	Collision with quay or grounding	Grounding/stranding	Single fatality or multiple serious injuries

5.3.3 Part 3: Perform mitigation analysis

Step 3 is to perform the mitigation analysis. As a first step in this part of the analysis the user will have to evaluate whether the system has self-recovery capacities or not. In the test cases this was always assumed to be the case if the selected function has redundant capabilities. Control systems will also usually have internal self-recovery capacities built into the software. Self-recovery capacities should be described in detail in the vessel’s ConOps.

Another experience from testing is that to reduce the number of possible failure scenarios, one must assume that all the systems involved in a mitigation layer will be unavailable when moving to the next mitigation layer, in case the previous fails. This makes it hard to obtain more than 2 independent mitigation layers, especially when performing the analysis at a high abstraction level.

Table 19 shows the mitigation analysis for the small passenger ferry with passive supervision and where the failure does not result in an alarm. The vessel will then have to rely on self-recovery capacities to avoid a collision, as no other independent mitigation layers will be triggered.

Table 19: Mitigation analysis for Small Passenger Ferry

MITIGATION ANALYSIS					
Internal mitigation layer (self-recovery capacities)	1st independent mitigation layer	2nd independent mitigation layer	3rd independent mitigation layer	Mitigation effectiveness	Risk level
Mission Phase: Transit to location					
Operation: Navigate through enclosed/sheltered waters					
Yes	None available	None available	None available	Moderate	High

Table 20 shows the mitigation analysis for the Short-sea Cargo Vessel. This analysis is performed at low level where object detection is not provided because of a random hardware failure. Because of active supervision and the fact that object detection is not defined as a required system for many of the MRC's, there are – in this case – several available independent mitigation layers.

Table 20: Mitigation analysis for Short-sea Cargo

MITIGATION ANALYSIS					
Internal mitigation layer (self-recovery capacities)	1st independent mitigation layer	2nd independent mitigation layer	3rd independent mitigation layer	Mitigation effectiveness	Risk level
Mission Phase: Transit to location					
Operation: Navigate through enclosed/sheltered waters					
Yes	Intervention from RCC	MRC01 Keep position	Drop anchor	Very high	Medium

5.3.4 Step 4: Perform risk evaluation

As illustrated in Figure 30, Figure 31, and Figure 32, a risk evaluation was performed for each case, where the risk level for each assessed scenario was identified. In RBAT, risk is a function of how effective the mitigations are, and how severe a potential worst-case outcome is. The risk is evaluated per scenario, meaning *causal factor-> unsafe condition-> (failed) mitigations-> worst-case outcomes.* The scenarios can be found in Appendix A where the full analysis is documented. As can be seen, albeit with some variations between the matrices, the risks tended group themselves in two different areas, either on the No effect/Medium-High area or the Catastrophic/Medium-Very high area. The first grouping is due to the scenarios not resulting in any losses while the second is due to not being able to qualify enough mitigations. The latter is a combined effect of doing the analysis on a high abstraction level, meaning that a large number of systems are listed as being involved in performing the control function, and the qualification criteria of mitigation layers having to be independent of the initiating event and each other. Sub-chapter 5.4 addresses this in detail, including suggestions for updates to the RBAT.

		Severity					
		No effect	Negligible	Minor	Significant	Severe	Catastrophic
Effectiveness	Low						
	Moderate						
	Medium	MP3-01-F01, MP3-01-F02					
	High	MP1-01-F08, MP1-01-F09, MP1-01-F10, MP1-01-F11, MP1-01-F12, MP1-01-F13, MP1-01-F14, MP1-01-F15				MP3-01-F03, MP3-01-F04, MP3-01-F05, MP3-01-F06, MP3-01-F07	MP1-01-F01, MP1-01-F02, MP1-01-F03, MP1-01-F04, MP1-01-F05, MP1-01-F06, MP1-01-F07, MP2-01-F05, MP2-01-F06, MP2-01-F07
	Very high						MP2-01-F01, MP2-01-F02, MP2-01-F03, MP2-01-F04, MP2-01-F08, MP2-01-F09
	Extremely high						

Figure 30: Risk evaluation of Concept A – Short-sea cargo

		Severity					
		No effect	Negligible	Minor	Significant	Severe	Catastrophic
Effectiveness	Low						
	Moderate						MP2-O1-F05
	Medium	MP3-O1-F1, MP3-O1-F2					MP1-01-F01-F23
	High						MP4-O1-F1
	Very high						MP2-O1-F01, MP2-O1-F02, MP2-O1-F03, MP2-O1-F04, MP2-O1-F06, MP2-O1-F07
	Extremely high						

Figure 31: Risk evaluation of Concept B – Small passenger ferry

		Severity					
		No effect	Negligible	Minor	Significant	Severe	Catastrophic
Effectiveness	Low						
	Moderate	MP2-01-F01, MP2-01-F02, MP2-01-F03, MP2-01-F04					
	Medium	MP1-01-F11, MP1-01-F12				MP1-01-F13	MP1-01-F01-F07, MP1-01-F14
	High						MP4-01-F01, MP4-01-F02, MP4-01-F03, MP4-01-F04
	Very high						
	Extremely high						

Figure 32: Risk evaluation of Concept C – RoPax ferry with assistant solutions

5.4 Updates made to the RBAT framework

The testing provided valuable insights about the strengths and weaknesses of RBAT. Some were obtained from the specific test activities suggested in the Third Report (DNV, 2022) while others emerged spontaneously. Table 21 provides a full summary of the updates made to the RBAT method description (see chapter 6) based on the experiences from the testing.

Table 21: Updates made to RBAT based on experiences from testing

ID	Topic	Test activities	Experiences	Updates
E-01	Abstraction levels/ multi-level function map	The breakdown of a mission into operational and functional goals should appear logical to the user and guide him/her towards identifying items to be analysed at a level of detail which matches the concepts maturity. As part of the case studies, evaluate how many layers of the Mission Model and Function Tree need to be represented in the (Excel) log sheet.	The “Mission phases” serve a purpose by being almost completely generic for most vessel types, and so it provides a framework for ensuring that the user takes all operational contexts into consideration when deciding which functions to address. “Operations” and “Key functions” (highest function level) has the most similarities. However, because functions are likely to analysed one (or more) levels down, this does not seem to represent an issue.	See other Test activities and Experiences on abstraction levels below. No updates or changes made.
E-02	Abstraction levels/ multi-level function map	Evaluate whether the "Control function" column shall be used to document which "Key function" (main function) in the Function Tree the control action belongs to, or if it shall be used to document the "parent" function of the control action (i.e., the function on the next level up).	Current experiences indicate that the analysis can be done for functions at any level in the Function Tree (assuming it can be allocated to a single performing agent). This in turn indicate that there is only need for one column (in the Excel sheet). According to the definitions, the “Control action” term can be used to define the specific actions taken by the “Control function”, e.g., if “anchor vessel” is a control function, “lower anchor” is a control action. In this sense, control actions are “sub-functions” of the control functions.	For now, both terms are kept as part of the method. “Control function” is used to label function types (read: “key functions”), while “Control action” is used for describing how the control function is being applied or executed in a specific situation. In other words, if the analysis is done at the highest level possible in the RBAT function tree, the “Key functions” become the control functions. No updates or changes made.

ID	Topic	Test activities	Experiences	Updates
E-03	Abstraction levels/ multi-level function map	Check if RBAT can be applied on different abstraction (function) levels, e.g., a high level in the initial concept phases and a more detailed level later. Also consider if it is possible to use the initial phase as a screening, to select which functions to analyse more in detail later.	RBAT can be used on different function levels, as already indicated in the method description. However, the analysis should not be done at a level which is so high that it cannot distinguish who is the performing agent. So, this dictates the upper level of abstraction to be used. I.e., if it is not possible to allocate the control function to a single performing agent, the function needs to be split up to distinguish who is responsible for what. In case a control function is being analysed where a sub-control system is the performing agent, (systemic/systematic) failures in the main control system can cascade down and cause failures in the sub-systems. Because this will be the case for all sub-systems, such failures can be handed separately, e.g., when doing the analysis on higher level.	Control functions should be decomposed to the level where it is possible to allocate the function to a single performing agent. This is already part of the RBAT method description. However, in some cases it may also be necessary to do more detailed analysis and on a function level where sub-control systems are the performing agent. Guidance has been added about how unacceptable risk levels when performing the analysis on a high abstraction level calls for more detailed analysis to be done. This will help reveal which function is driving the risk and how proposed mitigations may only adress failures in part of the previously (higher level) assessed function.
E-04	Abstraction levels/ multi-level function map	As above.	The implications from doing the analysis on a high function level is that one has to assume that failures in any of the involved systems may represent the “Causal factors”, which in turn limits the number of mitigation layers which confidently can be	Method updated to describe how the criticality (risk) ranking in RBAT can be used to determine the need for more detailed analysis.

ID	Topic	Test activities	Experiences	Updates
			nominated as effective and independent of the initiating event. I.e., it will be difficult to demonstrate independence between the systems performing the control function and the systems required for performing the mitigation layers. The criticality of a high-level function typically will be the same as its most critical subfunction. However, if the scenario is considered acceptable when analysed on a high function level, this is OK. If not, the function can be analysed at a lower level to identify which scenario is critical and implement risk control. This implicates that RBAT can be used as a screening method.	
E-05	Performing agent	N/A – Experience emerged during testing.	Unsafe condition/mode shall always refer to failures in the control system listed as the performing agent. Consequently, this failure in combination with not effective “Fault Detection Isolation and Recovery (FDIR) within the performing agent is also what creates the demand for the 1st mitigation layer. The other systems shall be assumed to function as intended, including any essential continuous functions. See also ID E-34 below about “Not followed/ rejected”.	Method description updated to include experience.

ID	Topic	Test activities	Experiences	Updates
E-06	“Not followed/ rejected”	N/A – Experience emerged during testing.	Only when using the guideword “Not followed/ rejected” can any one of the systems listed under “Other systems/roles” be assumed to cause the unsafe condition/mode. This is expected to highlight the criticality of any common essential system and demonstrate the need for furthermore detailed and separate analysis of these systems.	Method description updated to include experience. See also ID E-34.
E-07	Operational restrictions/ limitations	N/A – Experience emerged during testing.	Operational restrictions or limitations (e.g., weather conditions, speed limits) can have significant impact on the severity level.	RBAT updated to include a feature (excel column) which allows operational restrictions and limitations to be systematically recorded so that they (if documented) can be assumed and taken into consideration when ranking the severity level. Method description updated to state that the operational limitations should not be used as a way of arguing for not including certain design features (e.g., still design for bad weather, even though the vessel shall not sail in certain conditions). Furthermore, in case such restrictions and limitations are not documented (e.g., in the ConOps) they should not be taken into consideration as part of the ranking

ID	Topic	Test activities	Experiences	Updates
				and instead be proposed as risk control measures.
E-08	ConOps/ required input	N/A – Experience emerged during testing.	RBAT benefits from clear descriptions of the system architecture (e.g., hierarchies, system overview), including the relationships and interactions between various systems and functions. Must highlight system dependencies. This may imply that RBAT is best suited for the analysis of preliminary design (ref. Circ. 1455).	Method description updated to require that the system architecture needs to be known and used as input to RBAT. In addition to a function tree/list, a system hierarchy and system/function matrix is useful. This can be made part of the tool.
E-09	Preventive analysis/ measures	N/A – Experience emerged during testing.	This part of RBAT is intended to capture measures which are already implemented to prevent the causal factors and unsafe condition/mode from occurring in the first place. Because RBAT is not concerned with frequencies for initiating events, it has no direct effect on the results. As such it primarily serves the purpose of capturing such measures in case this is found useful by project stakeholders. The current method description may also not be clear how this is different from defining “Operational limits”.	Method description updated to clarify the scope of “Prevention analysis” and make sure it distinguishes it from defining “Operational limitations and restrictions”.
E-10	Risk ranking	Check whether the method only must include conditions which are unsafe, i.e., they influence safety. If	In principle, both options can be applied. Option (1) has the benefit of reducing the number of items to be included in the	The current method description opens for both options, which the test team also argued for. Software solutions may

ID	Topic	Test activities	Experiences	Updates
		the worst-case condition has a severity with "No effect" they (1) may also not have to be recorded. Alternatively, they (2) are recorded but not included in the Mitigation Analysis. If the first approach is chosen, the severity index does not have to include the "No effect" level.	assessment, which makes it more auditable and readable. The downside is that it is not as transparent and traceable in terms of knowing which risks have been addressed and not. Option (2) has opposite pros and cons to that of Option (1).	benefit in limiting the downsides of Option 2. No updates or changes made.
E-11	Multi-ship	N/A – Experience emerged during testing.	The assessment does not directly handle multi-ship scenarios. This can however be evaluated indirectly, e.g., by making judgements about how an incident on one vessel creates supervision demands which influences the supervision/ monitoring capacity of other vessels. For example, in case there are only two operators present in a control room, and both must actively supervise at least two vessels during normal operations for certain mitigation layers to be qualified as effective, this is not valid in case one vessel requires the complete attention of one operator.	Method description updated to explain how multi-ship scenarios can be assessed by running sensitivities using the supervision category. This can be solved with a software feature. For this purpose, the ConOps must clearly describe the manning and operational philosophy, including the use of supervision and fleet status in case of abnormal situations on one or more vessels.
E-12	Accident category	Under "Accident category" check whether it is sufficient to only use the main categories and not the sub-categories. "Worst case outcome" should in any case describe what happens (e.g., "collision with kayak")	Seems sufficient to only use the main categories if the worst-case outcome described what happens.	Incorporate this experience into the methodology and RBAT.

ID	Topic	Test activities	Experiences	Updates
		as a way of having transparency on the severity level. So, the sub-categories may become too detailed.		
E-13	Unsafe conditions/ modes	Check if the guidewords for Unsafe conditions/ modes are fit-for-purpose, i.e., if they have an influence on ranking severity/mitigations or risk control. Also check whether it is sufficient to use the main or sub-category guidewords.	The guidewords have an impact on how severity for the worst-case outcome is ranked. For example, for the control function “Provide propulsion” the guideword “Not providing leads to a hazardous event” can be used to identify “Grounding” as a worst-case outcome. While if the guideword “Providing leads to hazardous event” can be used to identify “Collision” or “Impact” as a hazardous event. These events may have different severities. Both the main- and sub-categories (guidewords) can in principle be applied. However, different guidewords under the same main category can produce different scenarios and severity levels, which indicate that they should be considered. The current method description states that the unsafe conditions/ modes shall be user defined. The experience from the testing shows that using the generic guidewords identified for RBAT is very useful when it comes to identifying the full risk picture, and therefore the use of these rather than	For now, both the unsafe condition/mode main categories as well as the guidewords are brought forward as part of the method and RBAT. How apply them as part of the software will be explored further as part of RBAT’s Part 3.

ID	Topic	Test activities	Experiences	Updates
			totally different user defined ones is recommended. What should be user defined, is a concretization of the guideword for the specific control function/ action being analysed. For example, if the guideword “too late” is used in analysis of a function/control action concerned with steering, concrete conditions of the type “Change of course too late” should be used. The disadvantage of using all the guidewords always, is that the number of detailed risks to be analysed becomes very large. Since the guidewords partly overlap and effects of the different unsafe conditions identified often may be the same, there are usually possibilities for merging unsafe conditions identified via different keywords and thereby reducing the number of risks to be analysed. This practice is encouraged but the decision to merge, should be taken on a case-by-case basis.	
E-14	Unsafe conditions/ modes	N/A – Experience emerged during testing.	There is currently no guideword for “Too little/ too much”.	Method description updated to include “Too little/ too much”.

ID	Topic	Test activities	Experiences	Updates
E-15	Unsafe conditions/ modes	N/A – Experience emerged during testing.	The guidewords “Control parameters within range, but incorrect” and “Control parameters out of range” represent systematic/systematic failures which can manifest themselves as unsafe conditions/modes represented by the other guidewords.	Method description updated to exclude “Control parameters within range, but incorrect” and “Control parameters out of range” as separate guidewords. Guidance updated to explain how they are examples of systematic/systemic failures, and what the implications are for mitigation layer performance requirements.
E-16	Failure categories/ causal factors	N/A – Experience emerged during testing.	As part of the assessment, there is no difference between systematic and systemic failures, and both have in common that they may result in unsafe conditions/ modes without generating an alarm or warning (“unannunciated failures”). The difference seems to be that they may require different risk control measures, in particular when it comes to preventing the introduction of weaknesses that could lead to such failures. This however is something which can be investigated in case the risk becomes unacceptable. As such, as a generic guideword in the tool, systemic and systematic failures can be combined into one.	Method description updated to explain that systematic/systemic failures can be combined into one category when applied as a causal factor for RBAT scenarios.

ID	Topic	Test activities	Experiences	Updates
E-17	Failure categories/ causal factors	N/A – Experience emerged during testing.	For systematical/ systemic failures, potential unsafe conditions/modes due to “incorrect output” (undetected/ unannunciated failures) should always be considered. When it comes to the influence on risk, this is one of the main things which separates it from the other failure categories. The combination of such failures and “passive supervision” is likely to result in mitigation layers which depend on human intervention to not be available.	To ensure that RBAT is successful at capturing the implications of undetected/ unannunciated failures, a column dedicated for stating this is included. The link between systematic/systemic failures, undetected/ unannunciated failures, and supervision category can possibly be automated as part of the software.
E-18	Failure categories/ causal factors	N/A – Experience emerged during testing.	The method does not currently specify whether (1) the Causal factor category «operator failure» only applies for control actions where a human is the performing agent, or (2) if it also applies for cases where the operator makes an error when preparing/configurating/maintaining the system.	The method description is updated to specify option (1). Option (2) is covered by the “systematic/systemic failures” category.
E-19	Failure categories/ causal factors	N/A – Experience emerged during testing.	“Systemic/systematic failures” also represent scenarios where the system does not fail but is incapable/insufficient when it comes to providing required functionality. E.g., a vessel does not have sufficient thrust and/or maneuverability to handle strong currents in a specific area.	The method description is updated to specify the noted “Experience”.
E-20	Failure categories/ causal factors	N/A – Experience emerged during testing.	If each of the Causal Factor categories are to be addressed for each Unsafe condition/mode relevant to the Control action, this may generate a very large number of units (i.e., Excel rows). In	The method description is updated to specify the noted “Experience”.

ID	Topic	Test activities	Experiences	Updates
			principle, it is only necessary to differentiate between Causal factors if they either have an impact on the severity of the scenario and/or the qualification of Mitigations.	
E-21	Failure categories/ causal factors	N/A – Experience emerged during testing.	It should be possible for the RBAT user to describe concept specific (examples) of what the causal factors can be (and not just the generic categories).	Experience to be implemented as part of the software.
E-22	Minimum risk conditions (MRC)	Compile a list of already known MRCs/mitigation layers to be included as part of the case studies (already done as part of developing cases). Check to what extent they will overlap with existing contents in the Mission Model and/or Function Tree. Ensure that the final solution does not cause additional confusion.	MRC should be considered a desired operational state to which the system (vessel) should transition when experiencing an abnormal situation with potential for experiencing (further) losses if continuing its normal operation. Entering an MRC can be achieved by use of mitigation layers realized by a single function or several different functions. The same or additional functions may also be responsible for recovering the system to a normal or degraded (but safe) operation. The control functions typically required to bring the system into an MRC in case of emergencies are already included in the RBAT function tree.	The method description is updated to specify the difference between MRCs and mitigation layers.
E-23	Auxiliary/ supportive systems	Check whether the risk contribution from failures in supportive functions (auxiliary, utility etc.) must be included as separate control actions,	Such system will be listed under “Other systems/ roles involved” like all the other systems. If such systems are identified as	No updates or changes made. See however ID E-34.

ID	Topic	Test activities	Experiences	Updates
		or if they can be covered through Causal Factors.	being essential, their control functions will be analysed separately.	
E-24	Essential continuous functions/ Propulsion/ steering (manoeuvring)	Check whether propulsion and steering should be analysed as separate functions (from e.g., navigation).	The primary difference between navigation and manoeuvring functions is that they are performed by different systems. At a high (and combined) function level the unsafe conditions /modes will manifest themselves in similar scenarios. The implication from doing the analysis on a high level is that it becomes impossible to take credit for fully *independent* mitigation layers in scenarios where the navigational systems fail, but the propulsion/steering functions are still operational (e.g., manual remote operation).	Covered by ID E-34.
E-25	Essential continuous functions	N/A – Experience emerged during testing.	Examples of essential continuous functions include propulsion, steering, power generation, and integrated automation systems.	Method description and list of definitions updated to exemplify and defined what is meant by essential continuous functions.
E-26	Severity index	N/A – Experience emerged during testing.	RBAT only includes a severity index for safety (this is the original scope of RBAT).	The method is updated to include indexes for losses related to asset, uptime, and environment.
E-27	Internal mitigation layer	N/A – Experience emerged during testing.	During testing “Internal mitigation layer” was always set to “Yes”. If this is the case in real projects, the column for indicating this serves no purpose. It also has	The assessment of “Internal mitigation” (self-recovery capacity) is kept for now and brought forward for further testing during Part 3. The method description is

ID	Topic	Test activities	Experiences	Updates
	Self-recovery capacity/ Redundancy		implications when it comes to the risk matrix.	updated to further specify how to perform this assessment. “Internal mitigation” is re-named to Fault Detection, Isolation, and Recovery (FDIR)
E-28	Supervision	Capture difference in active and passive supervision when the error is not detected.	The difference between active and passive supervision seems to play a role in case of unannunciated failures. If the control function is actively supervised, there is a chance for the operator to observe that something is wrong and make sense of what needs to be done. This, in turn, will make it possible to qualify mitigation layers.	The method description is updated to better specify the role and importance of active supervision in case of unannunciated systemic/systematic failures, and that this needs to be paid particular attention to when qualifying the mitigation layers. A functionality of the RBAT-tool could be to raise a flag for the user in case a passive supervision is planned for critical unannunciated systemic/systematic failures.
E-29	Supervision	The type of supervision and supervising agent may not be constant but can potentially vary across scenarios. For example, an onboard operator may actively supervise an operation, but if a failure happens on one of the systems involved, an alarm is raised in the RCC where the control room operator is responsible for passively supervising the system and act upon	They way RBAT is structured now the supervising agent is nominated for normal operations. But the assessment may reveal that who detects (and acts) on an unsafe condition may depend on what the causal factor is. This means that the user may have to go back and change the type of supervision and who the supervising agent is. All though this creates a need for iterations and updates, it also indicates that RBAT can generate valuable insights.	The method description is updated to specify the need for iterations on nominating who is supervising the control action in case RBAT reveals that this is different than what was originally imagined. Solutions for how the software can be designed to make this an easy task should be explored.

ID	Topic	Test activities	Experiences	Updates
		demand. As such, it may not always be possible to identify who the supervising agent of a control action is before the scenario has been identified. As part of the case studies, check and make note of how different scenarios reveal different aspects of supervision. Compare this with how supervision is defined in RBAT and explained as part of the methodology.		
E-30	Exposure rate	Check if there is a need to incorporate "Exposure rate" systematically into the method. This refers to exposure of the hazards or enabling conditions which need to be present for the accident to occur (presence of other vessels, weather conditions etc.). The exposure rate can be used to adjust the risk level. This is similar to what is done in the automotive industry (ISO 26260).	The idea of exposure rate came up when the method was finalized and drafted into the Third Report. The ambition for the first test was therefore limited to exploring whether this would be a useful feature. It appears as if the exposure to hazards varies significantly, but this is currently not reflected in the risk evaluation. As such, scenarios which are rated similarly in terms of severity and mitigation effectiveness may have very different risk levels.	The need for adjusting the risk level based on hazard exposure rates shall be further explored during Part 3 of RBAT.
E-31	Independent mitigation layers	Check if it possible to evaluate independence between mitigation layers without knowing what caused the previous mitigation layer to fail.	Independence must be verified for all other systems than those performing essential continuous functions.	Covered by ID E-33 and E-34.

ID	Topic	Test activities	Experiences	Updates
		Do we have to assume that all systems involved in performing the previous mitigation layer are unavailable?		
E-32	Independent mitigation layers	N/A – Experience emerged during testing.	Some mitigations layers/ minimum risk conditions may be followed up by a recovery action to return to normal operations or abort mission. This is also reflected in the RBAT accident model and list of definitions.	Recoveries following mitigations are described as part of creating the list of mitigations. Method description updated to further specify the difference between mitigations and recovery actions.
E-33	Independent mitigation layers	N/A – Experience emerged during testing.	Following the principle of *independence* outlined in the tested method (see the Third Report), demand for a 2nd independent mitigation layer must assume that the 1st independent mitigation layer is not working (at all), and not that it has "run out". If the latter is done, then the scenarios can in principle be plentiful and becomes guesswork. As such, the 2nd (or any subsequent) mitigation layer must be able to respond to the initiating event, and not to a scenario where the 1st independent mitigation layer was successfully initiated, before eventually failing. For example, assume that the initiating event is a drive-off and that the 1st mitigation layer is to bypass the DP system	Method description updated to capture the Experience.

ID	Topic	Test activities	Experiences	Updates
			by taking manual control of the thrusters. If this fails, it must be assumed that the drive-off is still occurring and the 2nd independent mitigation layer must cope with this.	
E-34	Independent mitigation layers	N/A – Experience emerged during testing.	The principle of mitigation layers having to be *independent* (see the Third Report) from the initiating event and of each other appears to make it difficult to qualify more than one or two mitigation layers in addition to being redundant or capable of performing self-recovery (i.e., FDIR). For worst-case outcomes ranked as “severe” or “catastrophic” the risk then becomes unacceptable. Testing showed that when performing the analysis on a higher level this effect is more likely than when doing it on a lower level. The reason is that some *essential continuous functions (and systems)* are involved in several control actions as well as mitigations. Steering, propulsion, power generation and distribution, are examples of such functions. The implication is that when strictly adhering to the principle of independence, these essential continuous functions cause the risk matrix to be overly conservative.	The method description is updated to suggest that the essential continuous functions should be assumed to be functional across the scenario (also as part of the relevant mitigation layers). Essential continuous functions must be analysed separately to check for available mitigations more thoroughly. If the risk is still assessed as unacceptable, alternative approaches needs to be considered (e.g., qualifying the control function as having sufficient integrity, and thus not having to rely on mitigation layers to ensure a sufficient level of safety). The principle of considering independence still apply to other functions/systems than those essential to normal operations. The justification for this solution is that in case a failure in an autonomy function (i.e., a performing agent) occurs at the same time as a failure in the one of the

ID	Topic	Test activities	Experiences	Updates
				essential continuous functions, this represent a dual failure scenario which is less likely than scenario where a failure in an essential continuous function is the sole cause of the initiating event (which can occur during any part of the normal operation). Furthermore, should such a failure occur during a critical phase of the mission's normal operation, the consequences will be equally severe. This means that if the risks associated with scenarios where failures in the essential continuous functions represent the initiating event are acceptable, the risks associated with dual failure scenarios are also acceptable.
E-35	Independent mitigation layers	N/A – Experience emerged during testing.	See ID E-34.	The method description is updated to rename "Independent mitigation layers" to "Mitigation layers".
E-36	Risk matrix	Test the risk matrix based on the severity of the worst-case outcome and mitigation effectiveness.	See ID E-34.	See ID E- 27 and E-34.
E-37	Abnormal situations	Loss of communication link (and other abnormal situations) as an "Operation" is a scenario which in principle can occur in all Mission Phases. This was already known,	The current solution is to group such scenarios as operations under a Mission phase called "Abnormal situations". Severity will be based on the "worst-case "principle", i.e., while the specific context is	No updates or changes made.

ID	Topic	Test activities	Experiences	Updates
		but it needs to be explored how to account for this when doing the analysis. E.g., how to define the context? This will be different if it occurs during Transit than Harbour Manoeuvring.	not defined by a mission phase, the worst possible context is chosen (e.g., loss of communication link in traffic dense areas).	
E-38	Function types	As part of the case studies, evaluate if the assessment can distinguish between: • Sub-function(s) performed in an iterative manner, e.g., navigation w/ collision avoidance o One case where the sub-functions are remotely controlled o One case where the sub-function is remotely monitored (supervised) o One case where the sub-functions are unsupervised • Sub-function(s) performed in a sequential manner, e.g., cargo handling • Sub-function(s) which has a continuously demand/presence, e.g., integrated monitoring and control	Overall, RBAT appears to be sensitive to most of the listed variations of sub-functions. In particular, the type of supervisory control can potentially have a significant impact on the results (risk levels). Furthermore, as explained as part of several other experiences, RBAT is sensitive to essential continuous functions, and have the possibility to highlight the criticality of these, assuming the analysis is used correctly. RBAT did not seem sensitive to whether a function is continuous or sequential. However, this may have an impact on how to structure the control functions and actions when populating RBAT with input. Sub-functions required as a response to abnormal and unsafe events were successfully covered part of the mitigation analysis.	Covered by several other experiences.

ID	Topic	Test activities	Experiences	Updates
		• Sub-function(s) required as a response to an abnormal and potentially unsafe event	See also the results from the testing in Appendix A.	
E-39	RBAT software requirement	N/A – Experience emerged during testing.	The user needs to have quick access to information about the mitigation layers. Some information can be directly linked, e.g., names of mitigation layers as drop-down lists.	Include Experience as part of preliminary software requirements.

6 STEP-BY-STEP GUIDEANCE TO THE RBAT METHODOLOGY

The current RBAT methodology consists of five main parts:

1. Describe use of automation (and remote control)
2. Perform hazard analysis
3. Perform mitigation analysis
4. Perform risk evaluation
5. Address risk control

The following sub-chapters presents these five main parts as consisting of 20 steps.

6.1 Part 1: Describe use of automation (and remote control)

The purpose of describing the use of automation (UoA) and remote control is to:

- Identify which functions are affected by automation or remote-control
- Understand how these functions are allocated to different *agents* (human or software)
- Check how the affected functions are supervised, and by which agents
- Know where the different agents are located (locally on vessel/site or remote)
- Map which other systems and other roles (personnel) are involved in performing the control action

This process should preferably be done as an integrated part of developing and documenting the *Concept of Operations* (ConOps). It is therefore an advantage if the ConOps adopts the terminology and principle of modelling functions using hierarchical goal structures, as explained in Step 1 and 2 below.

The UoA's *context* (e.g., geography, environmental conditions, infrastructure etc.) is expected to be described in the ConOps. In addition, the manning and operational philosophy should be outlined for all parts of the vessel's mission, including the use of supervisory control and fleet modes in case of abnormal situations on one or more vessels.

USE OF AUTOMATION						
Control function	Control action	Performing agent	Supervisory control category	Supervisory control agent	Other systems and roles involved	Operational limitations and restrictions
Mission phase: Arrival in port						
Operation: Perform port/harbour manoeuvring						
Propulsion	Reduce speed when approaching dock	Onboard autonomy system	Active	Safety operator	Automation system - Thruster system - Autopilot - Electric drive control	Maximum transit speed is 5 knots
...	…	...	...	...	…	…

Figure 33: Use of Automation module in RBAT

6.1.1 Step 1: Describe the vessel's mission (operational goals)

The first step of the process is to describe the vessel or fleet of vessels *mission*. The term mission refers to a set of mission phases, operations and functions the vessels perform to achieve their *operational goal(s).*

A mission can be described as consisting of three levels organized as a *hierarchical goal structure*, e.g.:

Mission: Safe and timely transport of cargo from Port X to Port Y

Mission phase: Arrival in port

Operation: Perform docking

The three levels can be described as follows:

- The overall mission goal(s), i.e., the commercial, political (e.g., defence) or public intentions which have contributed to and justifies the vessel concept development and operation. A (simplified) example can be “Safe and timely transport of cargo from one Port X to Port Y”.
- The mission phases, i.e., subdivisions of the mission are typically characterized by a recognizable shift in where the vessel is located in terms of geographical surroundings, or the start and end of one or more operations. An example can be “Arrival in port”.
- The operations, i.e., activities performed as part of a mission phase in order to achieve the mission goal. An example can be “Perform docking”.

The mission phases and operations are the study nodes under which the functions to be analysed are listed. Together with the details provided in the ConOps, they form the operational context (circumstances) under which the functions are required to perform. Considerations of the context is an important part of understanding the severity of potential accident scenarios (Step 9) and which mitigation layers can be qualified as effective for preventing losses from unsafe conditions/ modes (Step 14).

The generic RBAT mission model (Appendix B) can be used as a starting point. Descriptions can be added and/or re-phrased if needed. Emergency responses should be included as separate Operations.

Figure 33 shows how mission phase (grey row) and operations (golden row) are included as *nodes* in RBAT.

6.1.2 Step 2: Describe the automated and/or remotely controlled functions (functional goals)

The second step of the process is to describe the functions which are subject to or affected by automation and remote control. This includes identifying:

- the *control functions* required to successfully carry out the operations in each mission phase, and
- the *control actions* allocated to various (human or software) agents involved in performing the control function

Control functions and actions make up the *functional goals* of the hierarchical goal structure (letters in **bold**):

Mission: Safe and timely transport of cargo from Port X to Port Y

Mission phase: Arrival in port

Operation: Perform docking

Control function: Perform manoeuvring

Control action Y: Adjust speed

Control action Z: Adjust heading

The generic RBAT Function Tree (see Appendix C) can be used as a starting point for this process. For each operation described in Step 1, review and identify which of the (highest level) *key functions*[3] are required to achieve a successful outcome. Then, for each relevant key function, drill down the tree branches to a sub-function level which matches the current maturity of the concept. As a minimum, the functional goals shall be broken down to the level where automation can be made sense of, i.e., it shall be possible distinguish which parts of the function are allocated to different (human or system) agents (see Step 3).

The lower-level functions in the RBAT Function Tree should primarily be considered as suggestions. Functions can be re-phrased and/or added on a need-to basis. The list of verbs provided in Appendix D can be useful for this purpose.

When identifying and describing functions it is important to not only include those exerting direct control. Care should be taken to also consider functions which serve more supportive purposes (often across several other functions), such as auxiliary functions and functions required for system monitoring. If such functions are present across several mission phases and operations, they can be grouped under a separate study node to avoid unnecessary duplication of the assessment. This is particularly important for what is referred to as essential continuous functions. See Step 6 for further explanation.

Functions which involve exchange and interaction with external agents or systems should also be considered for inclusion, such as those provided by surrounding infrastructures, e.g., navigational aids.

Figure 33 shows the columns in RBAT used to describe control functions and actions (i.e., functional goals).

It is helpful if the ConOps includes functional block diagrams (Figure 34) illustrating the relationships and dependencies between the affected control actions (both internal and external).

Important: The level of function decomposition has an impact on the assessed criticality of the control actions. When doing the analysis on a (relatively) high function level, the function adopts the criticality of the most critical sub-function. This is normally addressed in Step 20 as part of risk control.

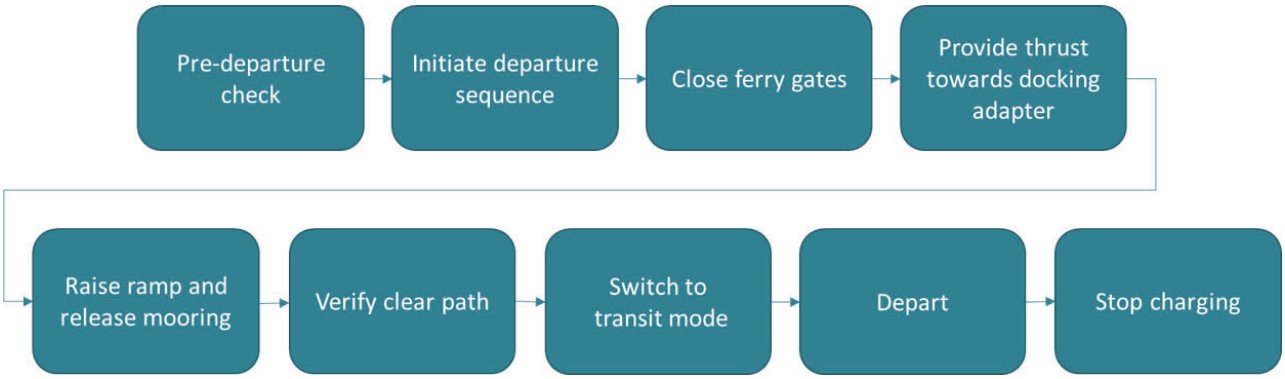


Figure 34: Example of control actions illustrated in a functional block diagram format

6.1.3 Step 3: Describe how control functions are allocated to agents

The third step of the process is to describe how control functions are allocated to different *agents* by indicating who is responsible for performing the various required control actions.

Agents can be a computerized system (i.e., software) or a human operator and only one agent can be listed as responsible for performing a control action under normal operations. However, depending on which level of detail control actions are described, cases may come up where more than one agent is involved. In principle,

[3] In RBAT, key functions are the highest layer of functions in the Function Tree.

this calls for further decomposing the control action until it can be distinguished which agent is the performing agent. If this appears as being too detailed, the agent making the decision should be nominated. Other agents can alternatively be described in the column titled “Other systems and roles involved” (see Step 5).

The geographical location of the agent shall also be indicated either by using nomenclature pre-fixes, such as “R” for Remote and “O” for onboard (vessel), or by including the actual location of the agent as part of the title. Alternatively, the location can be explained elsewhere, e.g., in the ConOps. This, however, is less preferable as it assumes that the analyst(s) and reviewers are familiar with this content.

Figure 33 shows how the control action “Reduce speed when approaching dock” is allocated to the performing agent “Onboard autonomy system”.

6.1.4 Step 4: Assign responsibility for supervisory control

The fourth step of the process is to indicate if and how control actions are supervised, and by which agent. *Supervisory control* is a role with an explicit responsibility to monitor system performance and detect anomalies so that the desired outcome can be achieved through implementation of corrective responses. Examples of anomalies can be system failures and malfunction, or external conditions which exceed pre-defined criteria for what are considered operational limits (e.g., weather conditions). In case a control system does not have the capacity to withstand or self-recover from a failure, the designated supervisory agent is responsible for ensuring that mitigation layers are effective, as described in Steps 13 and 14.

An important principle is that the supervisory agent cannot be the same as the agent performing the control action(s) being supervised.

The supervisor has an overriding authority of the control action performance and is responsible for its outcome.

Supervisory control can be performed by either a software or human agent. It is important to consider the strengths and weaknesses of both agents before assigning supervision responsibilities. In cases where humans are the supervising agent of a control action they will often rely on a system for monitoring and detection, while analysis, decision-making and implementation of actions require cognitive efforts and manual actions. A software agent will perform all actions. As such, the supervisor is the agent responsible for making decisions about interventions.

Three different categories of supervisory control are defined in RBAT:

- *Active human supervisory control*: A human agent is responsible for continuously[4] monitoring the automated performance of a control action with the purpose of being able to successfully intervene at any stage based on judgements about how to best act upon the situation. Because active supervision provides an opportunity for the human agent to continuously create situational awareness, it can be beneficial in cases where there is limited time available to intervene.
- *Passive human supervisory control*: A human agent is responsible for being available[5] to monitor the automated performance of a control action and successfully intervene upon requests (e.g., an alarm) generated by the system according to pre-defined parameters. Because passive supervision (often) requires the human agent to obtain situational awareness about the events preceding the request, it is best suited for cases where there is sufficient time available to intervene.
- *Software supervisory control*: A software agent is responsible for continuously monitoring the performance of a control action with the purpose of being able to successfully intervene on demand,

[4] ‘Continuously’ implies that the agent is responsible for, and expected to, direct his/her/its attention to a function for as long as it is being executed.

[5] ‘Available’ implies that the agent is responsible for, and expected to, be in close enough proximity to intervene upon a demand from the system.

without involvement of a human agent, for example if pre-defined parameters are exceeded, or there is disagreement in voting between separate functions/components.

- *No supervisory control*: No agent is responsible for monitoring the performance of a control action.

It is important to emphasize that the supervisory control categories represent a specific operational responsibility. This means that if an operator is responsible for actively supervising a control action, this must be reflected in job descriptions, procedures, routines, etc. Selection of supervisory control categories should therefore be based on the overall philosophy about monitoring and control described in the ConOps, which also include a more detailed description of the supervisory roles. Such descriptions should consider the influence from factors such as fleet size, manning level, competencies, human-software interfaces (e.g., information representation) when assigning supervision responsibilities to human agents. A preliminary solution for supervisory control should therefore be decided upon and described before commencing with the hazard and mitigation analysis (Part 2 and 3). The hazard analysis may however provide insights which may call for the initial supervisory agent and type of control to be revised.

Figure 33 shows how the “Safety operator” is responsible for actively supervising the control action “Reduce speed when approaching dock”.

6.1.5 Step 5: Identify other systems and roles involved

The fifth step of the process is to identify other systems and roles which are required to perform the control action, in addition to the performing and supervising agents. These are systems which in case of failure causes incorrect performance or unavailability of the intended control action. This step benefits from clear descriptions of the system architecture (e.g., in the ConOps), including the relationships and interactions between various systems. Examples are system hierarchies, block diagrams, and system/function matrices.

6.2 Part 2: Perform hazard analysis

The purpose of the hazard analysis is to:

- Identify unsafe conditions/modes associated with control actions (Step 6)
- Identify causal factors which may initiate the unsafe conditions/modes (Step 7)
- Describe the worst-case outcomes from (unmitigated) unsafe conditions/modes (Step 8)
- Rank the worst-case outcomes severity (Step 9)
- Describe relevant operational restrictions and limitation (Step 10)

HAZARD ANALYSIS						
Unsafe condition/mode	Causal factor category	Specific concerns	Worst-case outcome	Accident category	Severity	Level
Mission phase: Arrival in port						
Operation: Perform port/harbour manoeuvring						
Vessel fails to reduce speed (Not provided)	Systematic/ systemic	Failures in the autonomy system or sensors.	Impact with dock in transit speed	Contact with shore object	Single serious or multiple injuries	Significant
...	...	...	...	...	...	...

Figure 35: Hazard analysis module in RBAT

6.2.1 Step 6: Identify unsafe conditions/ modes associated with control actions

The sixth step of the process is to identify unsafe conditions/ modes associated with the various control actions identified in Step 2. Unsafe conditions/ modes manifest themselves as incidents where a system is operating outside its normal (and safe) operating envelope due degraded performance (e.g., failures) or exceeding its capabilities which, if left unmitigated, has the potential to cause an accident (i.e., losses).

Identification of unsafe conditions/modes is done by assigning guidewords (see Table 22) found relevant and credible to the control action under consideration. What characterizes a condition or mode as *unsafe* depends on the severity of worst-case outcomes (see Step 9). If it is evident that the worst-case outcome from a potential unsafe condition/mode is *negligible* it does not require mitigation layers to be acceptable (see Step 17 and 18). The user can opt to not record such items, as a way of improving the readability and overview of the analysis. On the other hand, recording all items will provide (e.g., reviewers) with transparency and trust that the relevant unsafe conditions/modes have been addressed. In such a case, the user can still save time by not having to include them as part of the mitigation analysis.

As can be read in the table, the category described as “Incorrectly provided control actions leads to an unsafe condition/ mode” refers to control parameters either being out of range, or within range but invalid or incorrect. This refers to unsafe conditions or modes caused by systematic or systemic failures which may

fail to be detected an annunciated to human operators. A more detailed explanation regarding the implications of such failures is provided as part of Step 12.

Important: All the unsafe conditions/ modes refer to failures in the system or role identified as the "Performing agent", normally a control system (software) or human operator. The other systems involved shall be assumed to function as intended, including any *essential common functions* such as power generation and distribution. The exception is in the case of the unsafe conditions/ modes "Not followed/ rejected". If this guideword is relevant, it indicates that the performing agent fails to exert control due to failure in any one of the other systems required to perform the control actions (see Step 5). This will create similar scenarios across most, or all the operations essential continuous functions are involved.

Instead of repeating the same scenario, essential continuous functions must be identified and analysed separately to check for available mitigations and varying degrees of severity more thoroughly, across different mission phases and operations. This requires the functions to be broken down to the level where the performing agent does not issue commands to control systems which can be identified as performing agents of other sub-functions. If the risk is still assessed as unacceptable, alternative approaches needs to be considered (e.g., qualifying the control function as having sufficient integrity, and thus not having to rely on mitigation layers to ensure a sufficient level of safety).

Table 22: Unsafe condition/mode categories and guidewords

Categories	Guidewords
Not providing the control action leads to an unsafe condition/ mode	Not provided
Providing the control action leads to an unsafe condition/ mode	Provided when not required
	Incapable/not fit for purpose
Incorrectly provided control actions leads to an unsafe condition/ mode - *Control parameters are out of range* - *Control parameters are within range, but invalid or incorrect*	Too early/late or in wrong of order
	Too much/ too little
	Stops too soon
	Applied too long
Control action not being followed leads to an unsafe condition/ mode	Not followed/Rejected

6.2.2 Step 7: Identify causal factors which can trigger unsafe conditions/ modes

The seventh step of the process is to identify causal factors which can trigger the unsafe condition/ mode. While unsafe condition/mode shall describe *why* the system is unsafe, the causal factors shall describe *how* the system became unsafe. These can be *internal failures* in the vessel's or RCC's systems or *insufficient capabilities* when it comes to handling external hazards (e.g., unfamiliar objects or strong currents). Hazards external to the vessel, relevant for the operation in question, should therefore always be considered when identifying failures which represents insufficient capabilities.

The following categories have been defined to represent causal factors:

- random (hardware) failures,
- systematic failures,

- systemic failures,
- operator failures,
- failures due to environmental conditions,
- failures due to deliberate actions.

See Appendix E for a more detailed explanation of these categories.

Note that the risk associated with the system not being capable to handling external hazards (waves, winds, current, traffic etc.) is covered by the "systematic/systemic failures" category.

A second note is that the "Operator failure" category only applies when a human is identified as the performing agent. Cases where the operator makes an error when preparing/configurating/maintaining the system is covered by "Systematic failures".

Although the causal factor categories overlap and correlate[6] to some extent, somewhat depending on which function level they are applied, they are useful as a guide to identify a wide range of failures that may pose risk. Concept specific concerns regarding the various causal factors categories can be noted down so that they can be targeted for risk control (see Step 20). This, however, depends on how much information is available about the system, including its planned operations and operating conditions.

Furthermore, when doing the analysis on a high function level there are often many systems involved, each which can potentially fail and be the cause of the unsafe condition/ mode. When being specific, the number of potential causes can become very high, and it is not a goal to make a complete list.

6.2.3 Step 8: Describe the worst-case outcomes from unmitigated unsafe conditions/ modes

The eight step of the process is to determine the worst foreseeable outcome of an unsafe condition/mode in case there is no mitigation available (this includes Fault Detection, Isolation and Recovery, FDIR, see Step 11). In RBAT, worst-case outcomes assume the contextual presence of a credible *hazard*. For example, loss of steering (an unsafe condition) close to shore (a hazard) results in a grounding (a worst-case outcome).

The description should include the hazard itself as well as the location, and not just the type of accident. For example, instead of only stating "grounding", it should also be specified which surface the vessel is grounding onto, such as a reef or sandbank (hazard and location). Or, instead of only stating "fire", it should be specified what is burning and where, such as diesel fire (hazard) in the machinery (location). This will help deciding (and auditing) which level of severity should be selected (see Step 9).

In case an argument is made that a hazard is not present, e.g., through operational restrictions, this must be clearly stated either as part of the prevention analysis (Step 16) or in the comments for addressing risk control (Step 20).

Finally, an accident main category is assigned to each worst-case outcome, using the taxonomy in the list below (Table 23). This is done by matching the worst-case outcome against the accident main category which includes the most suitable accident sub-categories.

[6] E.g., operator failure is a result of human errors caused by performance shaping factors (PSFs), such unannunciated failures with no alarms being presented.

Table 23: Accident main and sub-categories

General

- No effect on safety
- Injuries/loss of life (general)

Loss of control

- Loss of directional control
- Loss of propulsion power
- Loss of electrical power
- Loss of communication link
- Loss of containment
- Loss of stability
- Loss of control (other)

Collision

- Collision with other ship
- Collision with multiple ships

Contact

- Contact with floating object
- Contact with flying object
- Contact with shore object

Damage to/ loss of ship equipment

Hull failure

Fire/explosion

- Fire
- Explosion

Grounding/stranding

- Grounding
- Stranding

Capsize/listing

- Capsize
- Listing

Flooding/foundering

- Massive flooding
- Progressive flooding
- Foundering

Non-accidental event

- Acts of war
- Criminal acts
- Illegal discharge
- Other

Missing vessel

The accident categories are mutually exclusive and only one shall be assigned to each worst-case outcome. To help with this, the following principles apply:

- *Injuries/loss of life* shall only be used when this happens outside any of the other accident categories. For example, in the case of the crew being exposed to a disease.
- *Loss of control* shall only be used when there are no hazards present which are required to cause an accident.
- *Damage to/ loss of ship equipment* shall only be used when this occurs in absence of the other accident categories.
- *Hull failure* shall only be used in case this occurs without being the direct cause of other accident categories (e.g., capsize or foundering).

6.2.4 Step 9: Rank the worst-case outcome severity

The ninth step of the process is to rank the worst-outcome severity. For impact on safety and the external environment, this is done by assigning a degree of severity using the index in Table 24 and Table 25.

When it comes to the indexes for asset damages (Table 25) and delays or downtime (Table 27) each company can adjust the scales and add specific monetary values for each level to calibrate what they consider to be acceptable losses.

The limits for what define acceptable levels of risk is presented in the risk matrix shown as part of Step 17 (Table 32).

Table 24: Severity index for worst-case outcomes in terms of peoples' safety

Severity	Effects on human safety
Negligible	Single minor injury
Minor	Single injury or multiple minor injures
Significant	Single serious or multiple injuries
Severe	Single fatality or multiple serious injuries
Catastrophic	Multiple fatalities (more than one)

Table 25: Severity index for worst-case outcomes in terms of environmental impact

Severity	Effects on environment
Negligible	Spills onboard vessel or emissions with no noticeable effect on the environment
Minor	Spills or emissions with a brief effect on the environment surrounding the vessel
Significant	Spills or emissions with a temporary effect on the environment limited to a confined area
Severe	Spills or emissions with a long-lasting effect on the environment reaching some distant areas
Catastrophic	Spills or emissions with a permanent effect on the environment reaching a widespread distant area

Table 26: Severity index for worst-case outcomes in terms of damage to ship

Severity	Effects on ship[7]
Negligible	Superficial damage
Minor	Local equipment damage
Significant	Non-severe ship damage
Severe	Severe ship damage
Catastrophic	Loss of ship

[7] Here "ship" also extends to include assets required for remote control, such as remote-control centres and other infrastructure (if relevant).

Table 27: Severity index[8] for worst-case outcomes in terms of delays and downtime

Severity	Effects uptime[9]
Negligible	< 2 hours delay
Minor	< 1 day delay
Significant	1 – 10 days downtime
Severe	10 – 60 days downtime
Catastrophic	> 60 days downtime

6.2.5 Step 10: Describe operational restrictions and limitations

The tenth step of the process is to describe any operational restrictions and limitations associated with the control function and action being analyzed. This can be maximum allowed speed limits, type of supervisory control required for various traffic densities or situations, prohibited sailing areas, weather condition and sea state sailing restrictions, and more.

Assumptions about operational restrictions and limitations are important because they can have an impact on the potential severity of worst-case outcomes as well as influence which mitigation layers are available in different mission phases. This in turn can have a direct influence on the risk level, and to what extent it is considered acceptable.

It is important to note however that any such operational measures should not be used as a way of arguing for not including certain design features. For example, even though a ship is never meant to sail in poor weather conditions, it should still be designed to cope with such conditions (to a reasonably extent).

Furthermore, in case such restrictions and limitations are not documented (e.g., in the ConOps) they should not be taken into consideration as part of the ranking and instead be proposed as risk control measures (see Step 20).

[8] Scale is adopted from DNV-RP-203 Technology Qualification (DNV, 2021b).

[9] Uptime is a measure of system reliability, expressed as the percentage of time a machine, typically a computer, has been working and available. Uptime is the opposite of downtime (source: https://en.wikipedia.org/wiki/Uptime).

6.3 Part 3: Perform mitigation analysis

The purpose of the mitigation analysis is to:

- Check whether Fault Detection, Isolation and Recovery (FDIR) is planned to be part of control functions' design (Step 11)
- Determine how failures are detected during operations (Step12)
- Identify which mitigation layers are in place to prevent the unsafe condition or mode from resulting in losses (Step 13).
- Assess and determine whether mitigation layers can be qualified as effective in achieving their intended purpose (Step 14).
- Rank how effective the mitigations are at preventing potential losses (Step 15).
- Identify measures which are in place to prevent the direct cause of an unsafe condition or mode from occurring (Step 16, optional)

In RBAT "mitigations" refer to 1) a control function's ability to self-recover from, or withstand[10], a failure event and 2) whether additional *mitigation layers* implemented to prevent any further losses are successful. Mitigation layers may involve entering a minimum risk condition (MRC) as a measure to stay as safe as possible while attempting to regain the desired level of control. MRCs should be considered a desired operational state to which the system (vessel) should transition when experiencing an abnormal situation with potential for experiencing (further) losses if continuing its normal operation. Entering an MRC can be achieved by use of mitigation layers realized by a single function or several different functions. The same or additional functions may also be responsible for recovering the system to a normal or degraded (but safe) condition.

Summarized, in this context mitigations can involve the following types of responses:

- Withstanding or recovering from a failure before it turns into an unsafe condition/ mode (i.e., FDIR)
- Re-entering to a normal (safe) operating envelope by regaining control of an unsafe condition/ mode
- Enter a state of emergency response and abort further operations to prevent escalation

The role of mitigation layers is illustrated in the RBAT accident model (see Appendix F).

[10] RBAT adopts the term Fault Detection, Isolation and Recovery (FDIR) for this capability.

MITIGATION ANALYSIS							
Fault detection, isolation & recovery (FDIR)	Detection	1st mitigation layer	2nd mitigation layer	3rd mitigation layer	4th mitigation layer	Mitigation effectiveness	Risk
Mission phase: Arrival in port							
Operation: Perform port/harbour manoeuvring							
Yes	Annunciated failure detectable by human supervisors	Emergency stop (MRC3)	Drop of emergency anchor (MR C4)	None	None	High	M
…	…	…	…	…	…	…	…

Figure 36: Mitigation analysis module in RBAT

6.3.1 Step 11: Check for Fault Detection, Isolation and Recovery (FDIR)

The eleventh step is checking whether Fault Detection, Isolation and Recovery (FDIR[11]) is part of the control functions design and can (for the assessed scenario) prevent losses when the unsafe condition/mode is caused by random hardware failures, and some (but not all) other types of failure causes.

A binary assessment of FDIR is part of the input used to rank mitigation effectiveness (see Step 15) – "Yes" if FDIR is planned for and "No" if not. If "Yes", this need to be based on what is documented in technical reports (e.g., ConOps or a Safety Philosophy). If the use of FDIR is not documented anywhere, the assessment is "No" and an action to implement FDIR as part of the design can be noted down as a potential risk control measure (see Step 20).

When doing the assessment, it is important to be aware of typical challenges associated with FDIR mechanisms that are implemented in the performing agent responsible for the control action being analysed:

a) Built-in FDIR mechanisms may be vulnerable to common cause related problems, e.g., a weakness in software may lead to an unsafe condition and at the same time inhibit functionality needed for detection and/or recovery. Some examples of such scenarios are included below

   - Logic intended for handling of a specific possible failure situation may as a side-effect disable one or more FDIR mechanisms implemented in another part of the software. Such negative influence may occur due to dependencies in the software internal dataflow that has not been identified and therefore not explored in verification and validation activities.
   - A memory overwrite may occur e.g., when specific and input combination and or input sequence is received in a part of a software which is not robust with that input. If the memory overwrite should occur, this could negatively affect other parts of the software using the part of the memory that is overwritten. Memory-overwrite often leads to software crash which in some operational scenarios may be mitigated through use of a hardware watchdog automatically initiating a

[11] Wikipedia includes a useful article about FDIR, see https://en.wikipedia.org/wiki/Fault_detection_and_isolation

reboot. However, memory overwrite may also have more subtle effects which may be harder to detect and mitigate.

- Specific parts of software may under certain input conditions use too much processing time and thereby slow down or inhibit FDIR mechanisms in other parts of the software. This is particularly relevant in software applications utilising multitasking, but the problem may also occur in single task applications, e.g., the software execution may stay too long in an internal loop.

b) Some types of unannunciated failures may only be detected at higher levels in the system that have a broader overview of the system state and the current operational mode, for example by comparing output from different controllers in functionally diverse subsystems, comparing measurement from physical processes with expected performance, or through operator observation of system behaviour.

   - Systemic failures caused by missing or inadequate system requirements are example of failures that may be difficult to detect through FDIR mechanisms built into the performing agent.
   - Note that unannunciated failures also may be a challenge for some software supervisors that are considered independent of the performing agent, see subchapter 6.3.4 regarding functionality in mitigating measures.

These challenges are the reason why FDIR mechanisms built into the performing agent being analysed are considered to provide only a moderate level of risk mitigation.

Regarding the common cause challenges described in a) above, it should be noted that it may be possible to decompose function into subfunctions and analyse these subfunctions and control actions at a more detailed level. This may typically lead to identification of a hierarchy of more low-level performing agents supporting the top-level performing agent that perform the top-level control actions. If the lower level performing agents are located at different physical controllers, these performing agents may potentially act as supervisors for each other. In such an architecture the top-level performing agent may also be located at a separate controller and act as a supervisor for all lower level performing agents. Thus, through decomposition of a high-level function additional more detailed independent mitigating layers may be identified. Such a distributed system architecture may reduce the number of FDIR mechanisms considered vulnerable to common cause, however it may not remove the problem completely.

A highly integrated system architecture where several performing agents are sharing hardware and resources like memory and processor time will in principle be more vulnerable to common cause issues than a physically distributed one. Note however that there are controllers certified for usage in highly safety critical systems in other industries that can provide so called time and space partitioning, sometimes also referred to as logical separation. Such controllers allow tasks of different criticality to execute on the same hardware as unwanted interference through timing, memory or I/O is prevented by the certified controller hardware in combination with the certified commercial of the shelf software provided by the controller vendor.

6.3.2 Step 12: Determine how the failure is detected

The twelfth step of the process is to determine how the failure is detected so that the supervisor responsible for performing the required interventions can make sense of the unsafe condition/ mode. This is done by choosing the most suitable category for failure detection suggested in Table 28.

Failures may not manifest themselves as detectable anomalies, e.g., in case they are a result of control parameters being within range of incorrectly defined parameters. This may cause a scenario where no control signal is sent which demand automatic activation of mitigation layers and/or the operators are unable to intervene due to unannunciated failures. As such, it is important to systematically check for these types of

failures and how they impact the availability and qualification of mitigation layers (see Step 14), due to how this is determined by which supervisory control (see Step 4) is required for successful detection.

The final RBAT software can incorporate functions which automatically cross checks whether the detection category corresponds with what is noted as implications for supervisory control. This will help to ensure that mitigation layers which rely on human intervention are not incorrectly qualified.

Table 28: Categories for failure detection

Detection category	Description	Implications on supervisory control
Annunciated failure detectable by human supervisors	Operator(s) can easily make sense of the unsafe condition/ mode via system generated cues, such as notifications, warnings, or alarms.	Successful human intervention can be expected with both active and passive human supervisory control.
Unannunciated failure detectable by human supervisors	Operator(s) are not presented with any system generated cues but can easily make sense of the unsafe condition/ mode by observing the system, vessel, or its operating environment.	Successful human intervention can only be expected with active human supervisory control.
The failure is only detectable for software supervisor	Operator(s) are unable to make sense of the unsafe condition/ mode both due to cues being unavailable, misleading, incomplete, presented too late to make decisions about how to intervene.	Successful intervention can only be expected with software supervisory control (i.e., automated responses to events, not relying on manual activation).
Failure is undetectable by both human and software	Neither software nor humans can detect and make sense of the unsafe condition/ mode.	Successful intervention cannot be expected by neither software nor humans.

6.3.3 Step 13: Nominate mitigation layers which can prevent losses

The thirteenth step of the process is to identify which mitigation layers are in place to prevent the unsafe condition or mode from resulting in an accident (and losses). This is done by nominating potential 1st, 2nd, 3rd and 4th mitigation layer(s) for each combination of unsafe condition/ mode and causal factor(s) (see Figure 36). Preferably, a preliminary set of mitigation layers have already been described *prior* to using RBAT, e.g., as part of drafting the first version of a ConOps. If new mitigation layers are identified as part of the process, these are added to the list of existing ones, and then nominated in the analysis. RBAT requires mitigation layers to be described in a specific manner. This is explained in Appendix G.

It is important that the demand for a 2nd mitigation layer must assume that the 1st mitigation layer have not been effective in mitigating the unsafe condition/mode effects, and not that it has “run out”. If the latter is done, then the scenarios can in principle be plentiful and becomes guesswork. As such, the 2nd (and any subsequent) mitigation layer must be able to respond to the initiating event, and not to a scenario where the 1st mitigation layer was successfully initiated, before eventually failing. For example, assume that the initiating event is a drive-off and that the 1st mitigation layer is to bypass the DP system by taking manual control of the thrusters. If this fails, it must be assumed that the drive-off is still occurring and the 2nd mitigation layer must cope with this.

6.3.4 Step 14: Qualify the nominated mitigation layers

The fourteenth step of the process is to assess and qualify the nominated mitigation layers against a set of performance criteria which characterises them as effective in accident prevention. This includes:

Functionality: The mitigation layer's design and intended use makes it effective at preventing the unsafe condition or mode from resulting in (safety) losses.

Integrity: The mitigation layer is available, its condition is intact, and it can be relied upon to work under the expected circumstances.

Robustness: The mitigation layer will remain functional after the unsafe condition or mode has occurred, taking any disturbances and/or accidental loads into account.

Independence:

- of the event which initiated the unsafe condition/ mode
- of each other (in case a mitigation fails)

A mitigation layer cannot depend on an agent which has already failed as part of the accident scenario. This means that it cannot depend on the performing agent of the failed control action or on the supervisory agent responsible for a preceding mitigation layer to function successfully.

Systems performing essential continuous functions across the failed control action and (several) mitigation layers, and for which independence cannot be demonstrated, must be identified, and analysed separately.

Human involvement: A final criterion is that the mitigation layers are designed and implemented in such a way that it ensures successful human-automation interaction.

Additional guidance for assessing functionality, independence, and human involvement is provided below in sub-chapters 6.3.4.1, 6.3.4.2, and 6.3.4.3.

How to perform the qualification:

The qualification itself is qualitative and based on the knowledge available at the time RBAT is used. The conclusions are binary – a mitigation layer is either qualified or disqualified based on the user(s)[12] judgement.

In principle, a mitigation layer can be considered qualified when the user(s) feels confident that all the above-mentioned criteria are fulfilled, across any causal factors identified as relevant.

If knowledge is available which indicates that one or more of the criteria cannot be met, the mitigation layer is disqualified and shall be removed from the RBAT mitigation analysis (i.e., it shall not be taken credit as part of risk evaluations, Step 17).

It is acknowledged that limited information may be available about the mitigation layers, particularly in the preliminary design stage. In cases where assumptions must be made about the mitigation layers' performance and pre-requisites, these should be noted down (e.g., as part of a Safety Philosophy) so that they can be used to update the concept and included as part of verification and validation (V&V) efforts at a later stage.

In case a mitigation layer disqualifies, a comment should be made about why. If a risk is found unacceptable (see Step 17), disqualified mitigation layers can then be re-visited as the design matures and more knowledge is obtained. The approach therefore benefits from being conservative in the early

[12] *Users* here also includes potential reviewers and approvers.

stages, by not having to disqualify mitigation layers at a later stage which potentially may result in unacceptable risks.

6.3.4.1 Additional guidance on functionality

Consideration related to efficiency of mitigation layers allocated to software supervisors is included below.

A software supervisor that shall be capable of detecting and mitigating critical effects of all possible failure causes in a specific performing agent, may need to be equally advanced as the performing agent and be functionally diverse, or rely on another performing agent that is equally advanced and functionally diverse. This is to be able to detect and act upon output that is within expected range and timing but still wrong. A typical example where latter strategy is used, is for position reference systems where outputs from positioning systems utilising different principles are compared to each other, for example output from GPS may be compared to output from Inertial Navigation Systems (INS) and other position reference sources. Consequently, critical failures in one of the position reference systems can be detected and handled regardless failure cause. See also discussion about functional diversity in the independence section below

In some cases, a relatively simple software supervisor can detect and mitigate critical effects of all possible failure causes in the performing agent. A typical example is Emergency Shutdown Systems (ESD systems). Such systems are not monitoring output from the performing agent directly. Instead, failures in the process control system are detected indirectly through the ESD system monitoring the status of the process being controlled while using its own sensors. If critical parameter limits are exceeded, the ESD system will shut down the process being controlled.

Most software supervisors will typically be capable of acting based on alarms from the performing agent. Further, even if there are no alarms, supervisors may be capable of detecting and acting upon an abnormal situation in the performing agent based on not receiving data, receiving data out of range, receiving data that are unexpected from a statistical perspective, receiving data too late, receiving data out of sequence etc. However, many software supervisors will not be capable of detecting wrong output that is within expected range and timing if the problem is persistent, and in such cases an additional human supervisor is typically needed to mitigate the residual risk.

Some software supervisors may also have very strong capabilities when it comes to detecting that a problem is present, but less capability for independent mitigation. Regardless failure cause and even if there are no alarms, a supervisor in an autonomy system may through monitoring of the ships motion be able to detect that there are critical problems in one or more of the other performing agents involved in the manoeuvring function. This resembles ESD systems in that failures are detected indirectly through monitoring of the process being controlled. The supervisor may try to identify and isolate the failing performing agent based on trend analyses or similar, for example it may decide to exclude a thruster from being used based on available statistics. It may also initiate a “stay in position” command as an attempt at bringing the ship to safe state. However, such measures may rely on the same performing agents that may have failed, and consequently such mitigations may only be considered effective for specific failure causes. Such a supervisor may also have the authority to cut power to the thrusters as a subsequent option if other measures are not effective. In that case the mitigation measure would be independent of the performing agents having failed. However, whether such a measure would lead to safe state will be highly dependent on type of operation and operational phase.

6.3.4.2 Additional guidance on independence

Additional guidance about how to assess mitigation layer independence is provided in Table 29 below.

Table 29: Perspectives on mitigation layer independence

Perspective	Descriptions	Examples
Composition	This perspective, is used to evaluate whether there are any physical or software components used in the mitigation layer that may be affected by failures in components where an unwanted event has manifested itself.	A mitigation layer that relies on thrusters being reversed will not be independent if the initiating event occurred in the thruster itself or in the thruster control system. Two different types of software applications executed on the same controller will typically be dependent because they will share hardware and software components[13] A system may have several and different types of sensors which can trigger a safety function representing a mitigation layer. However, if the same controller and actuators is used regardless type of initiation, there may only be one fully mitigation layer available.
Environment	This perspective evaluates whether there are items outside the system and/or external events that may act upon the system, cause an unsafe condition/ mode and impair the mitigating layer.	• Loss of cooling in control rooms • Fire • Water ingress or flooding • Lightning strike • Radio communication jamming • Electrostatic discharge • Unexpected wind or wave conditions
Structure	This perspective looks at the relationships and bonds among the system constituents and between the system constituents and the environment.	Two systems/functions that are otherwise considered independent may both rely on the Power Management System being operational. An equipment specific protection mechanism may have the authority to reduce capacity to prevent equipment damage in a situation where the mitigation layer requires full capacity from that equipment to be effective. An operator may depend on alarms from the main control system to understand that a failure has occurred, and that activation of a mitigation layer is needed. If an unexpected scenario for which no alarm has been defined should occur (i.e., an un-

[13] Note that there are safety controllers that provide so called logical separation. In such cases the Commercial Of The Shelf (COTS) hardware and software components such as the operating system have been qualified for use in high-integrity systems and designed in such a way that individual software tasks cannot negatively influence each other through timing, memory space or I/O.

Perspective	Descriptions	Examples
		annunciated failure), the mitigation layer may not be activated in time to prevent a mishap.
Mechanisms	This perspective evaluates dependencies that may introduced through systems/functions or components having common requirements, common design, or common implementation*.	The controllers in a redundant control system are typically not independent of each other if a failure has systematic or systemic causes. This is since the two controllers typically will have common requirements, common design, and common implementation. Consequently, they will react in the same way to unexpected input: values, input combinations or input sequences. Two different GPS based positioning references systems may have different design and implementation. However, in case of unexpected input the systems may still fail in the same way as the functional requirements for such systems may be very similar**.

*Avoiding these kinds of dependencies may require some form of diversification, as described below.

** It is common to combine information from positioning references based on different principles to mitigate this kind of common cause through functional diversity as discussed below.

1) Functional diversity involves solving the same problem in different ways.

- This kind of diversity reduces the likelihood, that functional requirements which are inadequate for one or more operational scenarios will lead to dangerous systematic or systemic faults.
- Use of functional diversity may in some cases also lead to use of design diversity as discussed below, but not always.

2) Design diversity involves the use of multiple components, each designed in a different way but implementing the same function. E.g., one may use a CPU in combination with a Field Programmable Gate Array (FPGA).

This kind of diversity may be used to detect, isolate and recover from systematic failures introduced at software design and coding level, as well as in hardware design and manufacturing. It may also be used to detect random hardware faults.

This kind of diversity is not effective against systematic/systemic failures introduced in functional requirements specifications in the same way as functional diversity. It should be noted that software and hardware in controller(s) comparing and/or merging information from diverse functions and/or diverse components may introduce common mode failures.

6.3.4.3 Additional guidance on human involvement

For a mitigation layer to be qualified as effective, it must be designed and implemented in such a way that reliable human-automation interactions can be expected, assuming that operator actions are required.

This is assessed by asking whether it is possible for the operator(s) to:

- Detect and observe (perceive) the situation (information acquisition)?
- Make sense of the situation and predict future outcomes (information analysis)?
- Select a course of action among several alternative options (decision making)?
- Execute activities required to achieve the desired outcome (implementation of actions)?

Answers to these questions are found by determining whether one or more hindrances are present (see Table 30) and if their effect(s) on human-automation interaction is so negative that the required operator action(s) can be argued to fail.

During the design process the hindrances will concern technical *performance shaping factors* (PSFs) such as alarms, control panels and other human-software interfaces (HMI), communication systems, automation design, equipment performance and tolerances, and more.

Particular attention should be devoted to examining dependencies between the system failures which initiates the unsafe condition/ mode, and the systems operators rely on to perform actions required for mitigation layers to be successful. For example, in case a software-related error causes an unannunciated failure, the chances for an operator to act diminishes significantly.

Towards and during the operational phase the influence from other non-technical PSFs will emerge, such as procedures, training, and supervision. Although such factors can have a positive effect on human performance, they should not be an excuse to allow sub-optimal solutions at the earlier design stages.

If there are uncertainties about whether successful human-automation interaction can be expected, a more detailed analysis of the required operator actions should be done prior to qualifying the mitigation layer. For this purpose, it is recommended to use a recognized human reliability analysis technique (Blackett et al., 2022), or a similar risk analysis method based on task analysis.

Table 30: Hindrances for successful human-automation interaction

Information processing stages	Hindrances
Information acquisition *Perception of sensory information about the situation*	• There is no information available • There is too much information available • Information can easily be missed • Information can easily be misperceived (e.g., misheard, misread) • Information is misleading (e.g., expected but incorrect)
Information analysis *Making sense of the situation and predicting future events*	• Information analysis requires large amounts of information to be interpreted and memorized/recalled • Information analysis requires significant interpretations of uncertainties in parameters (incl. future events) • Information analysis requires understanding complex dependencies between different parameters • Information analysis requires factoring in the impact of unpredictable events (e.g., environment)
Decision-making *Selecting a course of action among several possible alternative options*	• The decision basis is insufficient and/or unclear • There are too many paths, options, goals and/or they are contradicting, conflicting, or competing • How to prioritize paths, options, goals is unclear • The plan (e.g., a procedure) does not match the situation • Outcomes from decisions are uncertain
Implementation of action(s) *Executing activities required to achieve desired outcome*	• Opportunities for successfully exerting control is limited, e.g., due to being remotely located • There is insufficient time (or other required resources) available to successfully perform the required actions • Expected amount of training and experience is not likely to raise and maintain required skills at an adequate level • There are few or no feasible opportunities to recover and correct an erroneous action.

6.3.5 Step 15: Rank the mitigation layers effectiveness

The fifteenth step of the process is to rank how effective the mitigation(s) is/are at preventing losses, using the index provided in Table 31. For control systems the thinking behind the index is as follows:

- For a control function that is not fully redundant, the effectiveness is considered *Low*. There may mitigation measures that can prevent losses from some types of random hardware failures, but the function being analyzed is not fully hardware fault tolerant nor fully tolerant to systematic/ systemic faults.
- A standard critical control system used in the maritime industry is expected to be redundant. This implies that there is least one internal mitigation (i.e., FDIR) that can prevent losses from various types of random hardware failures. There may also be mitigation measures that can prevent losses from some types of systematic faults, but for such systems there will typical be types of systematic/systemic faults that cannot be mitigated without external intervention. Thus, the effectiveness of the internal mitigations in the system should be classified as *Moderate*.
- A mitigation layer will increase the strength of the mitigating measures by one level. For example, an independent emergency function that can mitigate a control failure in a standard control system will raise the strength from Moderate to Medium. A further strengthening to High will require a second independent mitigation, and so on.

Note: In case of a control function with low capacity for self-recovery (FDIR) is combined with one mitigation layer capable of preventing losses regardless of failure cause, the total effectiveness should be considered on a case-by-case basis.

Table 31: Effectiveness of Mitigations

Effectiveness		Description
Extremely high	Very high	At least four effective mitigation layers can for the assessed scenario prevent losses *regardless* of what caused the unsafe condition/ mode.
Very high	High	At least three effective mitigation layers can for the assessed scenario prevent losses *regardless* of what caused the unsafe condition/ mode.
High	Medium	At least two effective mitigation layers can for the assessed scenario prevent losses *regardless* of what caused the unsafe condition/ mode.
Medium	Moderate	At least one effective mitigation layer can for the assessed scenario prevent losses *regardless* of what caused the unsafe condition/ mode.
Moderate	*FDIR not available*	FDIR mechanisms built into the performing agent can prevent losses when the unsafe condition/mode is caused by single random hardware failure or by some types of systematic or systemic failures*.
Low	Low	No or limited capacities for fault detection, isolation, and recovery are available, however (if present), for the assessed scenario these are expected to have a limited effect.

*The list below contains some examples of effects that may be caused by systematic or systemic failures, which FDIR functionality realized within the performing agent being analyzed typically may be capable of detecting and mitigating.

The list is by no means exhaustive:

- Software crash or software hang up.
- Expected data not being received in internal communication
- Data received in internal communication being out of range, corrupted, or out of sequence
- Date received in internal communication being received too late.
- Internal tasks performing too slow
- Internal data that are unexpected from a statistical point of view, e.g., temporarily unexpected variations in received data
- Internal commands that are illegal in the current system state
- Stack overruns

6.3.6 Step 16: Identify prevention measures (optional)

An (optional) sixteenth step of the process is to identify any measures which exist to *prevent* the occurrence of unsafe conditions/ modes. This includes activities which provide assurance that the required performance can be expected, such as maintenance, testing and inspection for technical equipment. As with mitigation layers, only measures which already have been documented prior to the assessment should be included.

Prevention layers should not be mistaken for operational limitations and restrictions.

6.4 Part 4: Perform risk evaluation

The purpose of performing risk evaluation is to compare the risk level for each assessed scenario against a set of risk acceptance criteria to determine the need for risk control.

6.4.1 Step 17: Determine risk level for each assessed scenario

The seventeenth step of the process is to determine the risk level for each assessed scenario, i.e., each combination of:

Causal factor-> unsafe condition/ mode-> mitigation layers -> worst-case outcome

As shown in Table 32, in RBAT the level of risk is a function of how severe the worst-case outcome of an unmitigated unsafe condition/ mode is, combined with how effective the mitigation layers are at preventing accidental (safety) losses. At this stage in the process, worst-case outcome severity has already been ranked in Step 9 and mitigation layer effectiveness has been ranked in Step 15.

As requested by EMSA, it is here recommended that the "as low as is reasonably practicable" (ALARP) principle is applied for risk evaluation[14]:

- High (red region): Risk cannot be justified and must be reduced, irrespectively of costs.
- Medium (yellow ALARP region): Risk is to be reduced to a level as low as is reasonably practicable.
- Low (green region): Risk is negligible, and no risk reduction is required.

The term *reasonable* is interpreted to mean cost-effective. Risk reduction measures should be technically practicable, and the associated costs should not be disproportionate to the benefits gained. How to perform cost-benefit assessments is extensively explained in the FSA guideline and therefore not repeated here.

Table 32: Risk as a measure of worst-case outcome severity and mitigation layer effectiveness

Effectiveness of risk mitigation layers	Severity				
	Negligible	Minor	Significant	Severe	Catastrophic
Low	Medium	High	High	High	High
Moderate	Low	Medium	High	High	High
Medium	Low	Medium	Medium	High	High
High	Low	Low	Medium	Medium	High
Very high	Low	Low	Low	Medium	Medium
Extremely high	Low	Low	Low	Low	Medium

6.4.2 Step 18: Alternative approaches for determining risk levels

The eighteenth step of the process is to explore alternative justifications for determining risk levels. While this is not expected to be a standard part of using RBAT, cases may arise where arguments for lowering the risk level appears to be justifiable.

When comparing the risk picture associated with a specific function and corresponding risk mitigation layers to relevant acceptance criteria, the following alternatives for risk evaluation can be considered:

[14] MSC-MEPC.2/Circ.12/Rev.2, chapter 4.

1. Operational restrictions such as speed limits and weather restrictions may be used to reduce the Severity of operational scenarios. Use of such measures must be clearly stated as an assumption in RBAT and documented in relevant reports (e.g., Safety Philosophy).
2. It may be possible to follow, e.g., the automotive industry in evaluating exposure rate to the relevant hazard. If it can be argued that the Hazard is relevant less than 10% of the average operational time per year, the required level of mitigations may be reduced by one level. If the hazard is relevant less than 1% of the average operational time per year, the required level of mitigation may be reduced by two levels.
3. If the initiating event[15] is not related to software control, it may be possible to argue for a lower probability than what has been generally anticipated for control functions. In that case fewer independent risk mitigation measures may be required to meet the acceptance criteria. For such events the classical type of risk matrix shown in Table 33 can be used as a starting point to determine the initial risk picture before looking at available mitigation layers.
4. It should be possible to argue that a single mitigation will increase the effectiveness of the mitigation by more than one level. One example may be that if it can be demonstrated than an emergency stop function for machinery has a Performance Level (PL) = *d* performance according to the ISO 13849 safety standard for machinery, this would be considered a two-level increase.
5. It should also be possible to demonstrate that safety critical control functions performing more complex functionality than emergency stop has a better performance than what is anticipated in the scheme above. Such claims should be substantiated in an Assurance Case or similar. More advanced forms of risk analysis, carefully selected components, and sharper development processes than what traditionally has been applied in the maritime may be required to substantiate such claims.

The pursuit of any such alternative approaches needs to be thoroughly argued for and carefully documented. As it is not within the scope of RBAT to suggest how this is done in practice, each user must determine what is the best possible approach to meet the expectations of approvers and other stakeholders.

Table 33: Example of classical risk matrix

			Severity				
Probability of failure per year			Negligible	Minor	Significant	Severe	Catastrophic
Frequent	>=1		Medium	High	High	High	High
Probable	>=1/10	To <1	Low	Medium	High	High	High
Occasional	>=1/100	To <1/10	Low	Medium	Medium	High	High
Remote	>=1/1000	To <1/100	Low	Low	Medium	Medium	High
Very remote	>=1/10000	To <1/1000	Low	Low	Low	Medium	Medium
Improbable		<1/10000	Low	Low	Low	Low	Medium

6.4.3 Step 19: Run sensitivities to check for supervisory control effects

The nineteenth step in RBAT is to run sensitivities to check for effects in changes to how supervisory control is used. Supervisory control has a direct impact on the risk level through which mitigation layers can be relied

[15] Causal factor(s) initiating the event which results in an unsafe condition/ mode

on and qualified for certain scenarios. This is explained in Step 4 and Step 12 (see Table 28). Requirements when it comes to supervisory control are in turn a result of the:

- number of vessels compared to number of available operators (vessel-supervisor ratio),
- when and how vessels require attention during normal operation (operational philosophy),
- the degree of automation in specific functions, and
- the reliability of automated systems.

A wish to assess the impact from multi-vessel concepts on the risk level is assumed to be the driving incentive for running sensitivities on effects from changes in supervisory control. RBAT, as a starting point, does not directly handle multi-vessel scenarios. This can however be evaluated indirectly, e.g., by making judgements about how an incident on one vessel creates supervision demands which influences the supervision/ monitoring capacity of other vessels. For example, in case there are only two operators present in a remote-control room, and both must actively supervise at least two vessels during normal operations for certain mitigation layers to be qualified as effective, this is not valid in case one vessel requires the complete attention of one operator.

Implications from multi-vessel effects on supervisory control is illustrated in Figure 37, Figure 38 and Figure 39. Assuming there is only one operator available to supervise two vessels, the concept illustrated in Figure 37 could potentially dis-qualify mitigation layers which require active supervisory control to be successful in the mission phases “Arrival in port” and “Depart from port”. This is because one operator alone will have difficulties following two vessels simultaneously. For the concept illustrated in Figure 38 this is solved logistically by not having the two vessels entering a mission phase requiring active supervisory control at the same time. Figure 39 shows a concept like the one in Figure 37. However, this has solved the supervision conflict by enabling passive supervisory control throughout all the mission phases. This means that none of the mitigation layers require active supervisory control to perform successfully (and thus to be qualified).

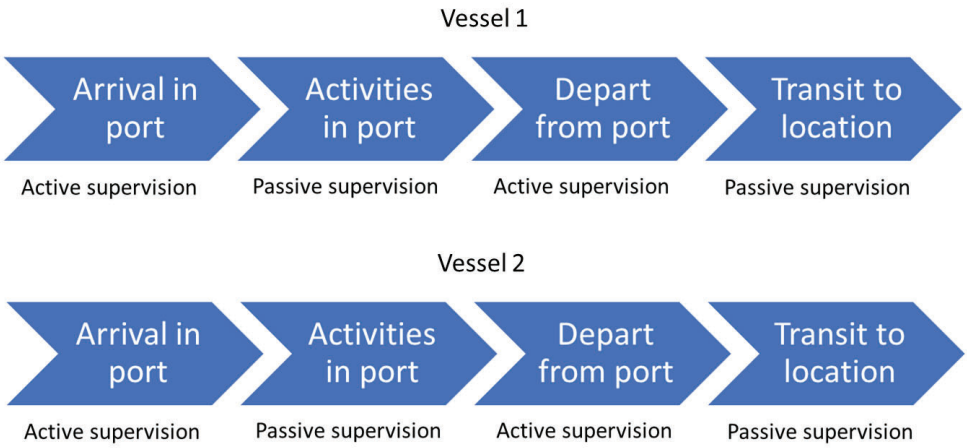


Figure 37: Two vessels simultaneously entering the same mission phases – mixed supervisory control

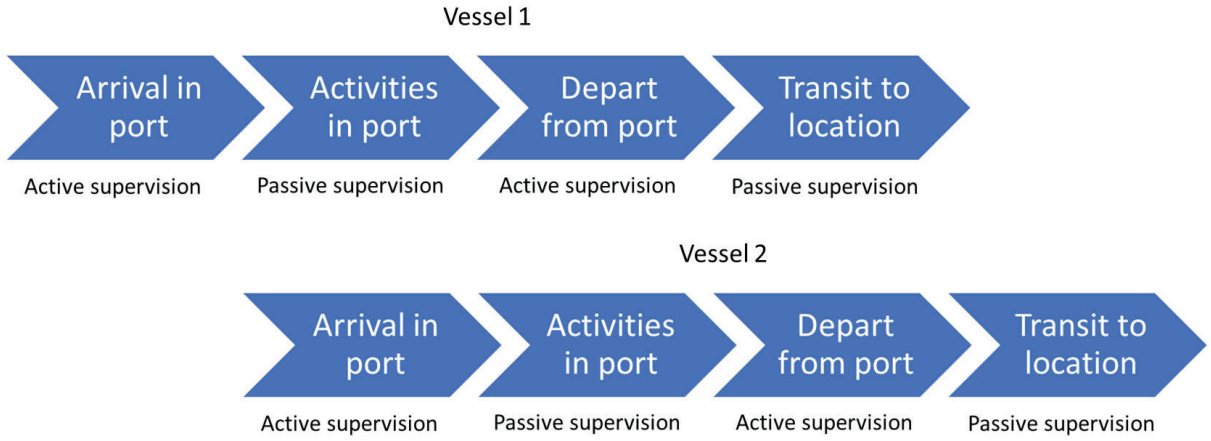


Figure 38: Two vessels simultaneously entering different mission phases – mixed supervisory control

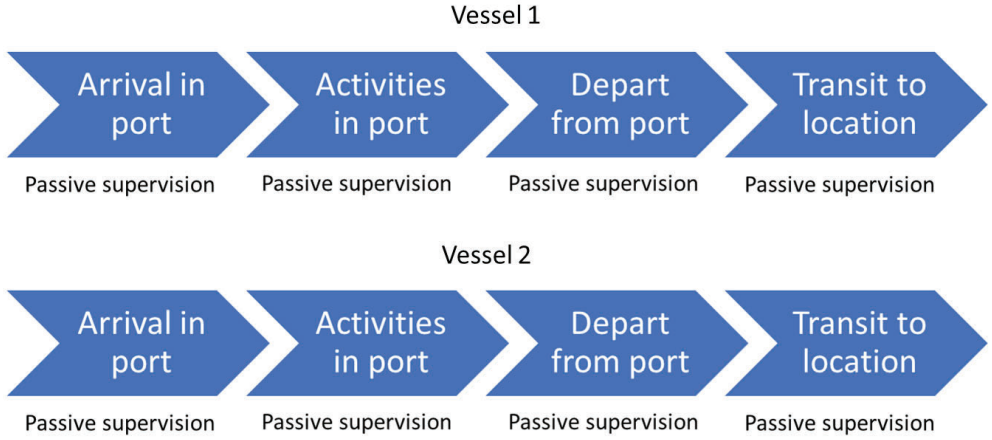


Figure 39: Two vessels simultaneously entering the same mission phases – passive supervisory control

Possibilities to incorporate a feature which provides an overview of supervision across phases and with multiple vessels shall be explored as part of Part 3 in the RBAT project. This shall be combined with a feature which can automatically demonstrate functional dependencies between the following entries:

- Supervision categories (active and passive human, or software supervisory control)
- Systematic/systemic failures potentially being unannunciated to the operator
- Detectability categories for unsafe conditions indicating the required type of supervisory control

6.5 Part 5: Address risk control

The purpose of risk control is to ensure that unacceptable (high) and tolerable (medium) risks are made as low as reasonably practicable (ALARP).

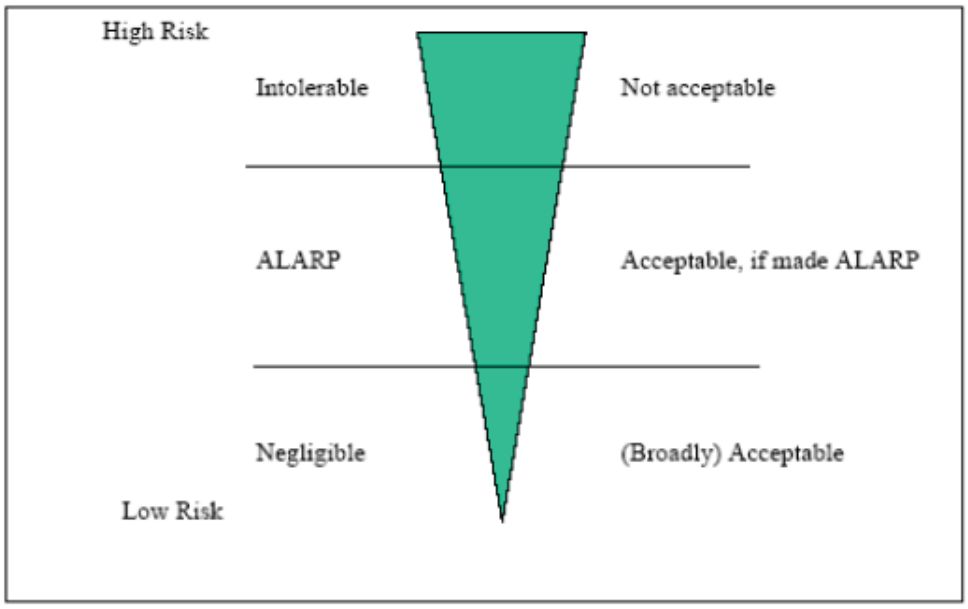


Figure 40: ALARP principle (IMO, 2018)

6.5.1 Step 20: Identify and document risk control measures

The twentieth and final step of the process is to identify risk and document control measures (RCM). This is done by recording actions and any necessary comments in a column dedicated for this purpose (Figure 41). In the case of RBAT, risk control measures can include:

- Updating the design by introducing FDIR and/or qualifying additional mitigation layers as effective so that they can be taken credit for as part of the risk evaluation.
- Removing or reducing the hazard associated with the control function, e.g., the fewer or less flammable hazards onboard, the less severe accident outcomes.
- Introduce operational restrictions which reduces the hazards potential impact, e.g., not allowed to sail close to shore in certain weather conditions or in high speed through traffic dense areas.
- Improving the control functions integrity (and thus reducing its failure frequency) through design, component manufacturing and maintenance processes backed up by thorough assurance cases.

An elaborate description of generic RCM attributes (categories) can be found in the FSA guideline (IMO, 2018) and is therefore not described in any more detail here.

Important: If the analysis is done on a high function level, it will adopt the criticality of the most critical sub-function. In some cases, it may therefore be necessary to perform a more detailed risk analysis to confidently identify which control functions and actions are the most critical and should be targeted for risk control measures. This can be done using RBAT, but also other risk analysis techniques such as Failure Mode and Effect Analysis (FMEA) may be relevant.

RISK CONTROL	
Comments (incl. Assumptions)	**Actions**
Dropping the emergency anchor requires manual actions.	Verify that there will be enough time available for the onboard safety operator to drop anchor.
...	...

Figure 41: Comments and actions addressing risk control

6 REFERENCES

Blackett, C., Farbrot, J. E., Øie, S., & Fernander, M. (2022). *The Petro-HRA Guideline*. Halden: Institutt for Energiteknikk.

DNV GL (2020a). Proposal for A functional study developing a Risk-Based Assessment Tool for MASS (RBAT MASS). DNV GL doc No: 1-1HPDRGR-M-N-ADSS-1.

DNV GL (2020b). Framework for generic risk assessment tool for MASS concepts. Report 1 of 2. Report No.: 1, Rev. 0.

DNV (2021a). Risk-based assessment tool for MASS: Framework for generic risk assessment tool for MASS concepts. Report 2 of 2 (for Part 1 of the RBAT study).

DNV (2021b). Technology Qualification. Recommended Practice: DNV-RP-A203. Edition September 2021

DNV (2022a). Risk-based assessment tool for MASS (RBAT): Specific test cases on the risk assessment tool – Third report. Report 1 of 2 (for Part 2 of the RBAT study).

DNV (2022b). Software Development Plan and Requirements for RBAT. DNV doc No. 10252115-05.

DNV GL (2017). Risikovurdering: Skipsstøt mot Sukkerbiten. (Risk assessment: Skip impact at Sukkerbiten).

DNV GL (2020a). Framework for generic risk assessment tool for MASS concepts. Report 1 of 2. Report No.: 1, Rev. 0.

DNV GL (2020b). Proposal for A functional study developing a Risk-Based Assessment Tool for MASS (RBAT MASS). DNV GL doc No: 1-1HPDRGR-M-N-ADSS-1.

EMSA (2020). Invitation to tender No. EMSA/OP/10/2020 for the functional study developing a Risk-Based Assessment Tool for MASS (RBAT MASS).

Endsley, M.R. (1995). "Toward a theory of situation awareness in dynamic systems". Human Factors. 37 (1)

International Electrotechnical Commission, IEC (2000). IEC 61839 Nuclear power plants – Design of control rooms – Functional analysis and assignment. First edition.

International Electrotechnical Commission, IEC (2009). IEC 60964 Nuclear power plants – Control rooms – Designs. Edition 2.0.

International Electrotechnical Commission, IEC (2013). IEC 60050-351 International Electrotechnical Vocabulary (IEV) - Part 351: Control technology.

International Electrotechnical Commission, IEC (2018). IEC 60812 Failure modes and effects analysis (FMEA and FMECA).

International Electrotechnical Commission, IEC (2020). IEC 61226 Nuclear power plants – Instrumentation, control and electrical power systems important to safety – Categorization of functions and classification of systems. Edition 4.0.

International Maritime Organization, IMO (1974). The International Convention on Standards of Training, Certification and Watchkeeping for Seafarers (STCW)

International Maritime Organization, IMO (2018). MSC-MEPC.2/Circ.12/Rev.2 – Revised guidelines for formal safety assessment (FSA) for use in the IMO rule-making process.

International Standard Organisation, ISO (2000). ISO 11064 Ergonomic design of control centres – Part 1: principles for the design of control centres. First edition.

International Standard Organisation, ISO (2009). ISO 31000:2009(E) Risk management – Principles and guidelines. First edition.

ISO/IEC/IEEE 15288:2015 Systems and software engineering -- System life cycle processes.

Kystverket (2022). Kystinfo. Retrieved from https://kystinfo.no/

Leveson, N.G. & Thomas, J.P. (2018). STPA Handbook. Downloaded from: https://psas.scripts.mit.edu/home/get_file.php?name=STPA_handbook.pdf

Lovdata (2019). Lov om havner og farvann (havne- og farvannsloven). Retrived from https://lovdata.no/dokument/NL/lov/2019-06-21-70

Marine Traffic (2022). Retrieved from https://www.marinetraffic.com/

NORCE (2022). Kystvarslingssenteret. Retrived from https://www.kystvarslingssenteret.no/point-histcast-01/

Norsk Klimaservicesenter (2022). Observasjoner og væstatistikk. Retrieved from https://seklima.met.no/

Parasuraman, R., Sheridan, T.B., Wickens, C.D. (2000). A model for types and levels of human interaction with automation. IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans 30, 286–297. https://doi.org/10.1109/3468.844354.

SAE Aerospace (1996). Guidelines and methods for conduction the safety assessment process on civil airborne systems and equipment. Aerospace Recommended Practice ARP4761. First edition.

Sheridan T. B., Parasuraman R. (2006). Human-automation interaction. In Nickerson R. S. (Ed.), Reviews of human factors and ergonomics (Vol. 1, pp. 89–129). Santa Monica, CA: Human Factors and Ergonomics Society.

Telenor (2022). Dekningskart. Retrieved from https://www.telenor.no/dekning/#dekningskart

APPENDIX A
Results from testing RBAT

CONCEPT A - SHORT SEA CARGO VESSEL

	USE OF AUTOMATION						HAZARD ANALYSIS					PREVENTION ANALYSIS	MITIGATION ANALYSIS					
ID	Control function	Control action	Performing agent	Supervision category	Supervising agent	Other systems and roles involved (onboard, onshore)	Unsafe condition/mode	Causal factor(s)	Worst-case outcome	Accident category	Severity	Performance requirements (criteria, limits, boundaries etc.)	Internal mitigation layer (self-recovery capacities)	1st independent mitigation layer	2nd independent mitigation layer	3rd independent mitigation layer	Mitigation effectiveness	Criticality
MP1-01	**Operation: Perform harbour manoeuvring**																	
MP1-01-F01	Perform navigation	Observe surroundings to make sure that docking area is clear	Situational awareness systems	Active supervision	Remote operator	- Surroundings mapping - Object detection - Object identification	Not provided	Random HW Failure	Collision with small boat	Collision	Multiple fatalities	Low speed, dedicate quay ara, waring signs	Yes	RCC Intervention	Emergency Anchoring		High	High
MP1-01-F02								Systematic/Systemic Failure	Collision with small boat	Collision	Multiple fatalities	Low speed, dedicate quay ara, waring signs	Yes	RCC Intervention	Emergency Anchoring		High	High
MP1-01-F03							Incapable/not fit for purpose	Systematic/Systemic Failure	Collision with small boat	Collision	Multiple fatalities	Low speed, dedicate quay ara, waring signs	Yes	RCC Intervention	Emergency Anchoring		High	High
MP1-01-F04							Control parameters out of range	Systematic/Systemic Failure	Collision with small boat	Collision	Multiple fatalities	Low speed, dedicate quay ara, waring signs	Yes	RCC Intervention	Emergency Anchoring		High	High
MP1-01-F05							Control parameters are within range but incorrect	Systematic/Systemic Failure	Collision with small boat	Collision	Multiple fatalities	Low speed, dedicate quay ara, waring signs	Yes	RCC Intervention	Emergency Anchoring		High	High
MP1-01-F06							Stops too soon	Random HW Failure	Collision with small boat	Collision	Multiple fatalities	Low speed, dedicate quay ara, waring signs	Yes	RCC Intervention	Emergency Anchoring		High	High
MP1-01-F07								Systematic/Systemic Failure	Collision with small boat	Collision	Multiple fatalities	Low speed, dedicate quay ara, waring signs	Yes	RCC Intervention	Emergency Anchoring		High	High
MP1-01-F08		Provide steering to manoeuvre vessel to quay	Propulsion and motion control system	Active supervision	Remote operator	- Propulsion, steering and auxiliary	Not provided	Random HW Failure	Collision with quay	Collision	No injuries, only inconvenience/ discomfort (if any)	No people allowed at the quay during docking (restriced area)	Yes	RCC intervention	Emergency Anchoring		High	Low
MP1-01-F09								Systematic/Systemic Failure	Collision with quay	Collision	No injuries, only inconvenience/ discomfort (if any)	No people allowed at the quay during docking (restriced area)	Yes	RCC intervention	Emergency Anchoring		High	Low
MP1-01-F10							Incapable/not fit for purpose	Systematic/Systemic Failure	Collision with quay	Collision	No injuries, only inconvenience/ discomfort (if any)	No people allowed at the quay during docking (restriced area)	Yes	RCC intervention	Emergency Anchoring		High	Low
MP1-01-F11							Control parameters out of range	Systematic/Systemic Failure	Collision with quay	Collision	No injuries, only inconvenience/ discomfort (if any)	No people allowed at the quay during docking (restriced area)	Yes	RCC intervention	Emergency Anchoring		High	Low
MP1-01-F12							Control parameters are within range but incorrect	Systematic/Systemic Failure	Collision with quay	Collision	No injuries, only inconvenience/ discomfort (if any)	No people allowed at the quay during docking (restriced area)	Yes	RCC intervention	Emergency Anchoring		High	Low
MP1-01-F13							Too early/late or in wrong of order	Random HW Failure	Collision with quay	Collision	No injuries, only inconvenience/ discomfort (if any)	No people allowed at the quay during docking (restriced area)	Yes	RCC intervention	Emergency Anchoring		High	Low
MP1-01-F14								Systematic/Systemic Failure	Collision with quay	Collision	No injuries, only inconvenience/ discomfort (if any)	No people allowed at the quay during docking (restriced area)	Yes	RCC intervention	Emergency Anchoring		High	Low
MP1-01-F15							Stops too soon	Random HW Failure	Collision with quay	Collision	No injuries, only inconvenience/ discomfort (if any)	No people allowed at the quay during docking (restriced area)	Yes	RCC intervention	Emergency Anchoring		High	Low

MP2	**Mission Phase: Transit to location**																	
MP2-01	**Operation: Navigate through sheltered waters**																	
MP2-01-F01	Perform collision and grounding avoidance	Detect vessels/objects	Collision and grounding avoidance system	Active supervision	Remote operator	- Collision risk assessment - Dynamic path planning	Not provided	Random HW failure	Collision with passenger ferry, pleasure craft	Collision	Multiple fatalities	Vessel is following route defined for the fleet of autonomous vessels.	Yes	Keep position	RCC intervention	Emergency Anchoring	Very high	Medium
MP2-01-F02								Systematic/Systemic Failure	Collision with passenger ferry, pleasure craft	Collision	Multiple fatalities	Vessel is following route defined for the fleet of autonomous vessels.	Yes	Keep position	RCC intervention	Emergency Anchoring	Very high	Medium
MP2-01-F03							Incapable/not fit for purpose	Systematic/Systemic Failure	Collision with passenger ferry, pleasure craft	Collision	Multiple fatalities	Vessel is following route defined for the fleet of autonomous vessels.	Yes	Keep position	RCC intervention	Emergency Anchoring	Very high	Medium
MP2-01-F04							Control parameters out of range	Systematic/Systemic Failure	Collision with passenger ferry, pleasure craft	Collision	Multiple fatalities	Vessel is following route defined for the fleet of autonomous vessels.	Yes	Keep position	RCC intervention	Emergency Anchoring	Very high	Medium
MP2-01-F05							Control parameters are within range but incorrect	Systematic/Systemic Failure	Collision with passenger ferry, pleasure craft	Collision	Multiple fatalities	Vessel is following route defined for the fleet of autonomous vessels.	Yes	RCC intervention	Emergency Anchoring		High	High
MP2-01-F06							Too early/late or in wrong of order	Random HW Failure	Collision with passenger ferry, pleasure craft	Collision	Multiple fatalities	Vessel is following route defined for the fleet of autonomous vessels.	Yes	RCC intervention	Emergency Anchoring		High	High
MP2-01-F07								Systematic/Systemic Failure	Collision with passenger ferry, pleasure craft	Collision	Multiple fatalities	Vessel is following route defined for the fleet of autonomous vessels.	Yes	RCC intervention	Emergency Anchoring		High	High
MP2-01-F08							Stops too soon	Random HW Failure	Collision with passenger ferry, pleasure craft	Collision	Multiple fatalities	Vessel is following route defined for the fleet of autonomous vessels.	Yes	Keep position	RCC intervention	Emergency Anchoring	Very high	Medium
MP2-01-F09								Systematic/Systemic Failure	Collision with passenger ferry, pleasure craft	Collision	Multiple fatalities	Vessel is following route defined for the fleet of autonomous vessels.	Yes	Keep position	RCC intervention	Emergency Anchoring	Very high	Medium

MP3	**Mission Phase: Activities in port**																	
MP3-01	**Operation: Perform loading/unloading**																	
MP3-01-F01		Unload cargo	Cargo handling control system	Active supervision	Dock operator and RCC	Loading/Unloading	Not provided	Random HW	Cargo will remain on vessel	No effect on safety	No injuries	No people allowed at the quay during docking (restriced area)	Yes	RCC Intervention			Medium	Low
MP3-01-F02								Systematic/Systemic Failure	Cargo will remain on vessel	No effect on safety	No injuries	No people allowed at the quay during docking (restriced area)	Yes	RCC Intervention			Medium	Low
MP3-01-F03							Provided when not required	Random HW	Damage to cargo and/or personell in proximity to the vessel	Damage to/ loss of ship equipment	Single serious or multiple injuries	No people allowed at the quay during docking (restriced area)	Yes	Abort current operation	RCC Intervention		High	Medium
MP3-01-F04								Systematic/Systemic Failure	Damage to cargo and/or personell in proximity to the vessel	Damage to/ loss of ship equipment	Single serious or multiple injuries	No people allowed at the quay during docking (restriced area)	Yes	Abort current operation	RCC Intervention		High	Medium
MP3-01-F05							Too early/late or in wrong of order	Random HW	Damage to cargo and/or personell in proximity to the vessel	Damage to/ loss of ship equipment	Single serious or multiple injuries	No people allowed at the quay during docking (restriced area)	Yes	Abort current operation	RCC Intervention		High	Medium
MP3-01-F06								Systematic/Systemic Failure	Damage to cargo and/or personell in proximity to the vessel	Damage to/ loss of ship equipment	Single serious or multiple injuries	No people allowed at the quay during docking (restriced area)	Yes	Abort current operation	RCC Intervention		High	Medium

CONCEPT B – SMALL PASSENGER FERRY

	USE OF AUTOMATION						HAZARD ANALYSIS	HAZARD ANALYSIS					PREVENTION ANALYSIS	MITIGATION ANALYSIS					
ID	Control function	Control action	Performing agent	Supervision category	Supervising agent	Other systems and roles involved (onboard, onshore)	HAZID additional remarks	Guideword	Causal factor(s)	Worst-case outcome	Accident category	Severity	Performance requirements (criteria, limits, boundaries etc.)	Internal mitigation layer (self-recovery capacities)	1st independent mitigation layer	2nd independent mitigation layer	3rd independent mitigation layer	Mitigation effectiveness	Criticality
MP1	**Mission phase: Transit to location**																		
MP1-O1	**Operation: Navigate through enclosed/sheltered water**																		
MP1-01-F01	Perform navigation		Autonomous Navigation System	Passive supervision	Remote operator	- Situational awareness system - Voyage planning system - Collision and grounding avoidance system		Not provided	Random HW failure	Collision with other vessel	Collision	Multiple fatalities	Regular maintenance and testing. Approved system according to regulations and sufficiently tested. System delivered by acknowledged supplier and updated regularly.	Yes	RCC intervention	Emergency Anchoring		High	High
MP1-01-F02									Systematic/Systemic Failure	Collision with other vessel	Collision	Multiple fatalities	Regular maintenance and testing. Approved system according to regulations and sufficiently tested. System delivered by acknowledged supplier and updated regularly.	Yes	RCC intervention	Emergency Anchoring		High	High
MP1-01-F03									Impact from environment - loss of cooling of control systems	Collision with other vessel	Collision	Multiple fatalities	Regular maintenance and testing. Approved system according to regulations and sufficiently tested. System delivered by acknowledged supplier and updated regularly.	Yes	Limp home/ Navigate to closest safe harbour	Emergency Anchoring		High	High
MP1-01-F04								Incapable/not fit for purpose	Systematic/Systemic Failure	Collision with other vessel	Collision	Multiple fatalities	Regular maintenance and testing. Approved system according to regulations and sufficiently tested. System delivered by acknowledged supplier and updated regularly.	Yes	RCC intervention	Emergency Anchoring		High	High
MP1-01-F05								Control parameters out of range	Systematic/Systemic Failure	Collision with other vessel	Collision	Multiple fatalities	Regular maintenance and testing. Approved system according to regulations and sufficiently tested. System delivered by acknowledged supplier and updated regularly.	Yes	RCC intervention	Emergency Anchoring		High	High
MP1-01-F06								Control parameters are within range but incorrect	Systematic/Systemic Failure	Collision with other vessel	Collision	Multiple fatalities	Regular maintenance and testing. Approved system according to regulations and sufficiently tested. System delivered by acknowledged supplier and updated regularly.	Yes				Moderate	High
MP1-01-F07								Stops too soon	Random HW Failure	Collision with other vessel	Collision	Multiple fatalities	Regular maintenance and testing. Approved system according to regulations and sufficiently tested. System delivered by acknowledged supplier and updated regularly.	Yes	RCC intervention	Emergency Anchoring		High	High
MP1-01-F08									Systemic/Systematic Failure	Collision with other vessel	Collision	Multiple fatalities	Regular maintenance and testing. Approved system according to regulations and sufficiently tested. System delivered by acknowledged supplier and updated regularly.	Yes	RCC intervention	Emergency Anchoring		High	High
MP1-01-F12	Perform manoeuvring	Provide steering to maintain course	Integrated Automation System	Passive supervision	Remote operator	- Propulsion and motion control system - Electric power system		Not provided	Random HW Failure	Collision with other vessel	Collision	Multiple fatalities	Regular maintenance and testing. Approved system according to regulations and sufficiently tested. System delivered by acknowledged supplier and updated regularly.	Yes	RCC intervention	Emergency Anchoring		High	High
MP1-01-F13									Systematic/Systemic Failure	Collision with other vessel	Collision	Multiple fatalities	Regular maintenance and testing. Approved system according to regulations and sufficiently tested. System delivered by acknowledged supplier and updated regularly.	Yes	RCC intervention	Emergency Anchoring		High	High
MP1-01-F14								Provided when not required	Random HW Failure	Collision with other vessel	Collision	Multiple fatalities	Regular maintenance and testing. Approved system according to regulations and sufficiently tested. System delivered by acknowledged supplier and updated regularly.	Yes	RCC intervention	Emergency Anchoring		High	High
MP1-01-F15									Systemic/Systematic Failure	Collision with other vessel	Collision	Multiple fatalities	Regular maintenance and testing. Approved system according to regulations and sufficiently tested. System delivered by acknowledged supplier and updated regularly.	Yes	RCC intervention	Emergency Anchoring		High	High
MP1-01-F16								Control parameters out of range	Systemic/Systematic Failure	Collision with other vessel	Collision	Multiple fatalities	Regular maintenance and testing. Approved system according to regulations and sufficiently tested. System delivered by acknowledged supplier and updated regularly.	Yes	RCC intervention	Emergency Anchoring		High	High
MP1-01-F17								Control parameters are within range but incorrect	Systemic/Systematic Failure	Collision with other vessel	Collision	Multiple fatalities	Regular maintenance and testing. Approved system according to regulations and sufficiently tested. System delivered by acknowledged supplier and updated regularly.	Yes				Moderate	High
MP1-01-F18								Too early/late or in wrong of order	Random HW Failure	Collision with other vessel	Collision	Multiple fatalities	Regular maintenance and testing. Approved system according to regulations and sufficiently tested. System delivered by acknowledged supplier and updated regularly.	Yes	RCC intervention	Emergency Anchoring		High	High
MP1-01-F19									Systemic/Systematic Failure	Collision with other vessel	Collision	Multiple fatalities	Regular maintenance and testing. Approved system according to regulations and sufficiently tested. System delivered by acknowledged supplier and updated regularly.	Yes	RCC intervention	Emergency Anchoring		High	High
MP1-01-F20								Stops too soon	Random HW Failure	Collision with other vessel	Collision	Multiple fatalities	Regular maintenance and testing. Approved system according to regulations and sufficiently tested. System delivered by acknowledged supplier and updated regularly.	Yes	RCC intervention	Emergency Anchoring		High	High
MP1-01-F21									Systemic/Systematic Failure	Collision with other vessel	Collision	Multiple fatalities	Regular maintenance and testing. Approved system according to regulations and sufficiently tested. System delivered by acknowledged supplier and updated regularly.	Yes	RCC intervention	Emergency Anchoring		High	High
MP1-01-F22								Applied too long	Random HW Failure	Collision with other vessel	Collision	Multiple fatalities	Regular maintenance and testing. Approved system according to regulations and sufficiently tested. System delivered by acknowledged supplier and updated regularly.	Yes	RCC intervention	Emergency Anchoring		High	High
MP1-01-F23									Systemic/Systematic Failure	Collision with other vessel	Collision	Multiple fatalities	Regular maintenance and testing. Approved system according to regulations and sufficiently tested. System delivered by acknowledged supplier and updated regularly.	Yes	RCC intervention	Emergency Anchoring		High	High

MP2	**Mission phase: Transit to location**																		
MP2-O1	**Operation: Navigate through enclosed/sheltered water**																		
MP2-O1-F01	Perform collision and grounding avoidance		Autonomous Navigation System	Passive supervision	Remote operator	- Collision and grounding avoidance system		Not provided	Random HW Failure	Collision with other vessel	Collision	Multiple fatalities	Regular maintenance and testing. Approved system according to regulations and sufficiently tested. System delivered by acknowledged supplier and updated regularly.	Yes	Keep position	RCC intervention	Emergency Anhoring	Very high	Medium
MP2-O1-F02									Systematic/Systemic Failure	Collision with other vessel	Collision	Multiple fatalities	Regular maintenance and testing. Approved system according to regulations and sufficiently tested. System delivered by acknowledged supplier and updated regularly.	Yes	Keep position	RCC intervention	Emergency Anhoring	Very high	Medium
MP2-O1-F03								Incapable/not fit for purpose	Systematic/Systemic Failure	Collision with other vessel	Collision	Multiple fatalities	Regular maintenance and testing. Approved system according to regulations and sufficiently tested. System delivered by acknowledged supplier and updated regularly.	Yes	Keep position	RCC intervention	Emergency Anhoring	Very high	Medium
MP2-O1-F04								Control parameters out of range	Systematic/Systemic Failure	Collision with other vessel	Collision	Multiple fatalities	Regular maintenance and testing. Approved system according to regulations and sufficiently tested. System delivered by acknowledged supplier and updated regularly.	Yes	Keep position	RCC intervention	Emergency Anhoring	Very high	Medium
MP2-O1-F05								Control parameters are within range but incorrect	Systematic/Systemic Failure	Collision with other vessel	Collision	Multiple fatalities	Regular maintenance and testing. Approved system according to regulations and sufficiently tested. System delivered by acknowledged supplier and updated regularly.	Yes				Moderate	High
MP2-O1-F06								Stops too soon	Random HW Failure	Collision with other vessel	Collision	Multiple fatalities	Regular maintenance and testing. Approved system according to regulations and sufficiently tested. System delivered by acknowledged supplier and updated regularly.	Yes	Keep position	RCC intervention	Emergency Anhoring	Very high	Medium
MP2-O1-F07									Systematic/Systemic Failure	Collision with other vessel	Collision	Multiple fatalities	Regular maintenance and testing. Approved system according to regulations and sufficiently tested. System delivered by acknowledged supplier and updated regularly.	Yes	Keep position	RCC intervention	Emergency Anhoring	Very high	Medium

MP3	**Mission phase: Transit to location**																		
MP3-O1	**Operation: Navigate through enclosed/sheltered water**																		
MP3-O1-F1	Maintain communication	Communication/data link between RCC and ferry	Integrated Automation System	Passive supervision	Remote operator	- Telecommunication system		Not provided	Random HW Failure	Rouge vessel	Loss of control	No injuries, only inconvenience/ discomfort (if any)	Regular maintenance and testing. Approved system according to regulations and sufficiently tested. System delivered by acknowledged supplier and updated regularly.	Yes	Keep position			Medium	Low
MP3-O1-F2									Systematic/Systemic Failure	Rouge vessel	Loss of control	No injuries, only inconvenience/ discomfort (if any)	Regular maintenance and testing. Approved system according to regulations and sufficiently tested. System delivered by acknowledged supplier and updated regularly.	Yes	Keep position			Medium	Low

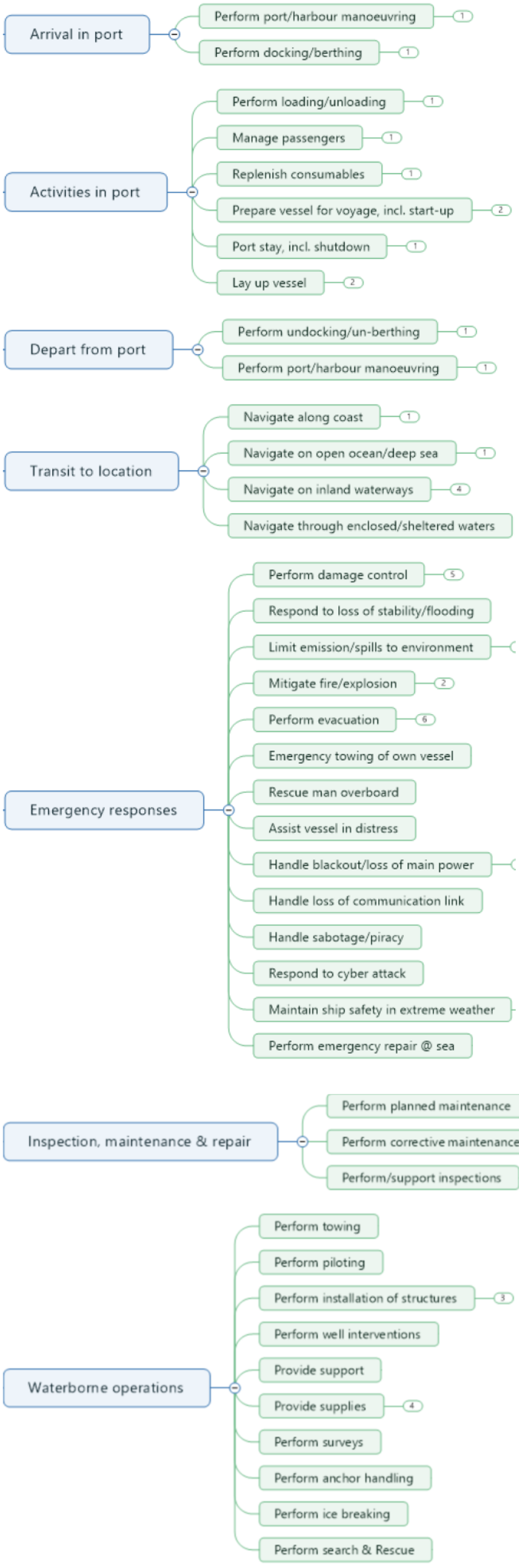
CONCEPT C – RO-PAX

	USE OF AUTOMATION						HAZARD ANALYSIS	HAZARD ANALYSIS					PREVENTION ANALYSIS	MITIGATION ANALYSIS					
ID	Control function	Control action	Performing agent	Supervision category	Supervising agent	Other systems and roles involved (onboard, onshore)	Unsafe condition/ mode	Guideword	Causal factor(s)	Worst-case outcome	Accident category	Severity	Performance requirements (criteria, limits, boundaries etc.)	Internal mitigation layer (self-recovery capacities)	1st independent mitigation layer	2nd independent mitigation layer	3rd independent mitigation layer	Mitigation effectiveness	Criticality
MP1	**Mission Phase: Arrival in port**																		
MP1-01	**Operation: Perform docking**																		
MP1-01-F01	Perform navigation	Determine vessels position and relative distance to the quay in order to determine when to decelerate	Autonomous Navigation System	Active supervision	Bridge crew	- Situational awareness system - Collision and grounding avoidance system		Not provided	Random HW failure	Collision with quay or grounding	Grounding/stranding	Single fatality or multiple serious injuries	Regular maintenance and testing. Approved system according to regulations and sufficiently tested. System delivered by acknowledged supplier and updated regularly.	Yes	Bridge crew intervention			Medium	High
MP1-01-F02									Systematic/Systemic failure	Collision with other vessel	Grounding/stranding	Single fatality or multiple serious injuries	Regular maintenance and testing. Approved system according to regulations and sufficiently tested. System delivered by acknowledged supplier and updated regularly.	Yes	Bridge crew intervention			Medium	High
MP1-01-F03								Incapable/not fit for purpose	Systematic/Systemic Failure	Collision with other vessel	Collision	Multiple fatalities	Regular maintenance and testing. Approved system according to regulations and sufficiently tested. System delivered by acknowledged supplier and updated regularly.	Yes	Bridge crew intervention			Medium	High
MP1-01-F04								Control parameters out of range	Systematic/Systemic Failure	Collision with other vessel	Collision	Multiple fatalities	Regular maintenance and testing. Approved system according to regulations and sufficiently tested. System delivered by acknowledged supplier and updated regularly.	Yes	Bridge crew intervention			Medium	High
MP1-01-F05								Control parameters are within range but incorrect	Systematic/Systemic Failure	Collision with other vessel	Collision	Multiple fatalities	Regular maintenance and testing. Approved system according to regulations and sufficiently tested. System delivered by acknowledged supplier and updated regularly.	Yes	Bridge crew intervention			Medium	High
MP1-01-F06								Stops too soon	Random HW failure	Collision with other vessel	Collision	Multiple fatalities	Regular maintenance and testing. Approved system according to regulations and sufficiently tested. System delivered by acknowledged supplier and updated regularly.	Yes	Bridge crew intervention			Medium	High
MP1-01-F07									Systematic/Systemic failure	Collision with other vessel	Collision	Multiple fatalities	Regular maintenance and testing. Approved system according to regulations and sufficiently tested. System delivered by acknowledged supplier and updated regularly.	Yes	Bridge crew intervention			Medium	High
MP1-01-F11	Embark/disembark crew & passengers	Operate ramp so that cars/passengers can leave vessel	Integrated Automation System	Active supervision	Bridge crew & deck crew	-Quay operations sequencing system		Not provided	Random HW failure	Passenger/vessels will not be able to disembark	Non-accidental event	No injuries	Regular maintenance and testing. Approved system according to regulations and sufficiently tested. System delivered by acknowledged supplier and updated regularly.	Yes	Bridge crew intervention			Medium	Low
MP1-01-F12									Systematic/Systemic failure	Passenger/vessels will not be able to disembark	Non-accidental event	No injuries	Regular maintenance and testing. Approved system according to regulations and sufficiently tested. System delivered by acknowledged supplier and updated regularly.	Yes	Bridge crew intervention			Medium	Low
MP1-01-F13								Provided when not required	Random HW failure	Passengers/crew/cars may fall off vessel	Injuries/loss of life (general)	Single fatality or multiple serious injuries	Regular maintenance and testing. Approved system according to regulations and sufficiently tested. System delivered by acknowledged supplier and updated regularly.	Yes	Bridge crew intervention			Medium	High
MP1-01-F14									Systematic/Systemic failure	Collision with other vessel	Collision	Multiple fatalities	Regular maintenance and testing. Approved system according to regulations and sufficiently tested. System delivered by acknowledged supplier and updated regularly.	Yes	Bridge crew intervention			Medium	High

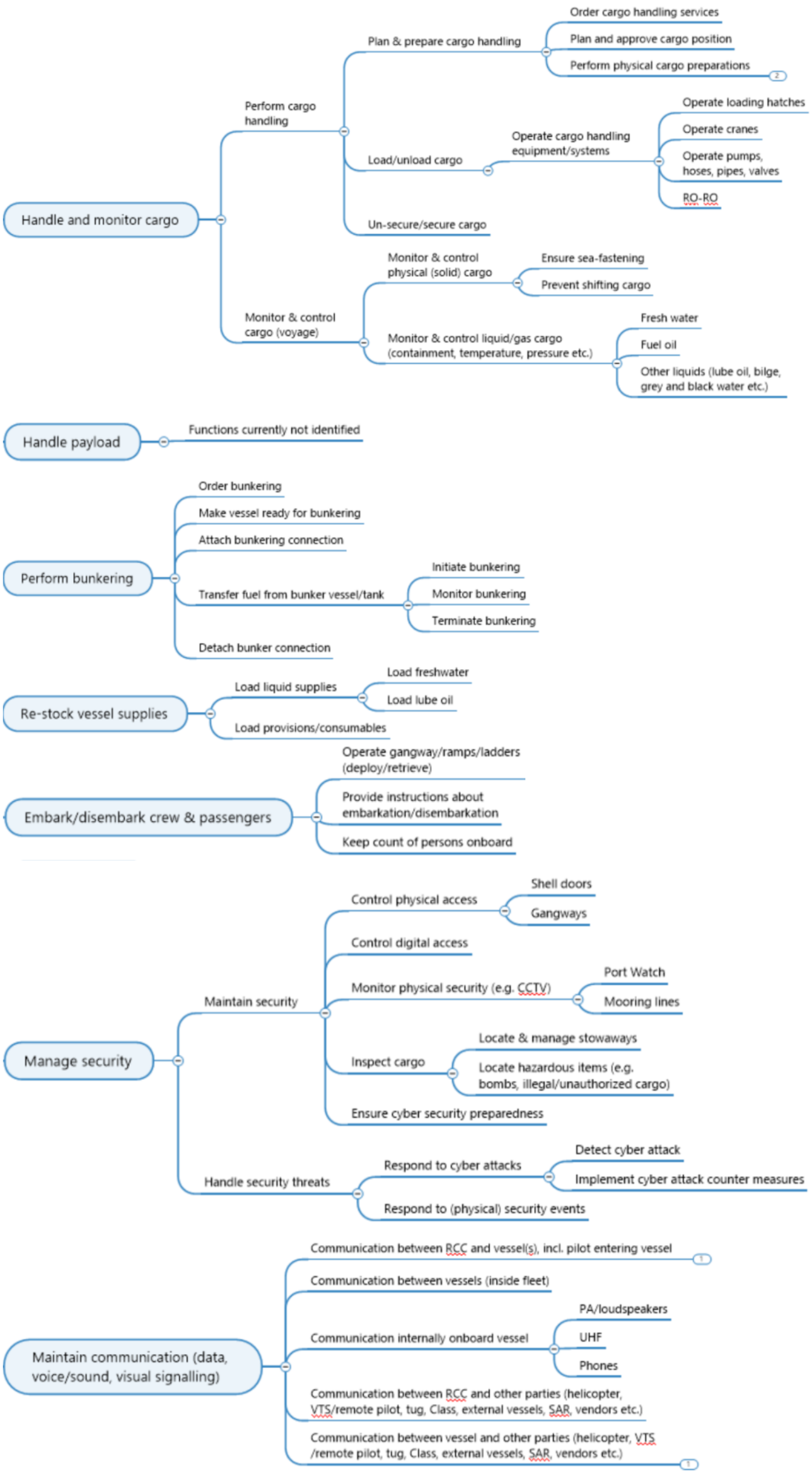
MP2	Mission Phase: Activities in port																		
MP2-01	Operation: Re-plenish consumables																		
MP2-01-F01	Perform manoeuvring	Maintain position with ramp down while charging	Integrated Autonomous System	Passive supervision	Bridge crew	- Propulsion and motion control system - Electric power system		Not provided	Random HW failure	Collision with quay	Collision	No injuries, only inconvenience/ discomfort (if any)	Regular maintenance and testing. Approved system according to regulations and sufficiently tested. System delivered by acknowlegded supplier and updated regularly.	Yes				Moderate	Low
MP2-01-F02									Systematic/Systemic failure	Collision with quay	Collision	No injuries, only inconvenience/ discomfort (if any)	Regular maintenance and testing. Approved system according to regulations and sufficiently tested. System delivered by acknowlegded supplier and updated regularly.	Yes				Moderate	Low
MP2-01-F03								Stops too soon	Random HW failure	Collision with quay	Collision	No injuries, only inconvenience/ discomfort (if any)	Regular maintenance and testing. Approved system according to regulations and sufficiently tested. System delivered by acknowlegded supplier and updated regularly.	Yes				Moderate	Low
MP2-01-F04									Systematic/Systemic failure	Collision with quay	Collision	No injuries, only inconvenience/ discomfort (if any)	Regular maintenance and testing. Approved system according to regulations and sufficiently tested. System delivered by acknowlegded supplier and updated regularly.	Yes				Moderate	Low

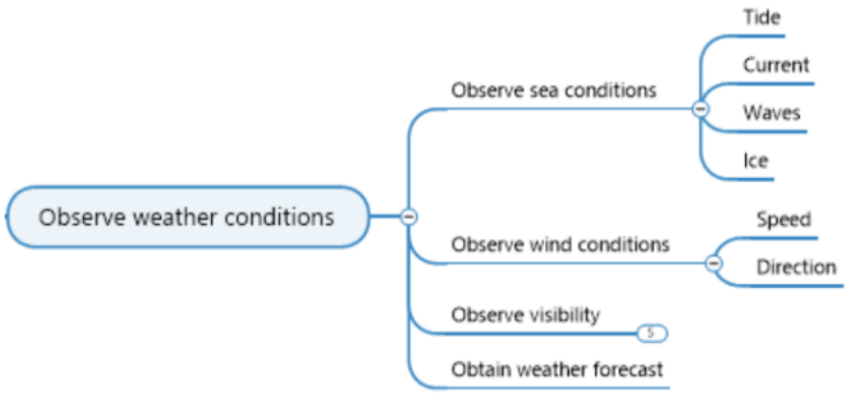
MP4	Mission Phase: Transit																		
MP4-01	Operation: Handle blackout (back-up power available)																		
MP4-01-F01	Integrated monitoring and control	Execute power blackout restart sequence	Integrated Automation System	Active supervision	Remote chief engineer	- Electric power system		Not provided	Random HW failure	Grounding in harsh weather conditions	Grounding/stranding	Multiple fatalities	Regular maintenance and testing. Approved system according to regulations and sufficiently tested. System delivered by acknowlegded supplier and updated regularly.	Yes	Remote restart by chief engineer	Drop anchor		High	High
MP4-01-F02									Systematic/Systemic failure	Grounding in harsh weather conditions	Grounding/stranding	Multiple fatalities	Regular maintenance and testing. Approved system according to regulations and sufficiently tested. System delivered by acknowlegded supplier and updated regularly.	Yes	Remote restart by chief engineer	Drop anchor		High	High
MP4-01-F03								Control parameters out of range	Systematic/Systemic failure	Grounding in harsh weather conditions	Grounding/stranding	Multiple fatalities	Regular maintenance and testing. Approved system according to regulations and sufficiently tested. System delivered by acknowlegded supplier and updated regularly.	Yes	Remote restart by chief engineer	Drop anchor		High	High
MP4-01-F04								Control parameters are within range but incorrect	Systematic/Systemic failure	Grounding in harsh weather conditions	Grounding/stranding	Multiple fatalities	Regular maintenance and testing. Approved system according to regulations and sufficiently tested. System delivered by acknowlegded supplier and updated regularly.	Yes	Remote restart by chief engineer	Drop anchor		High	High

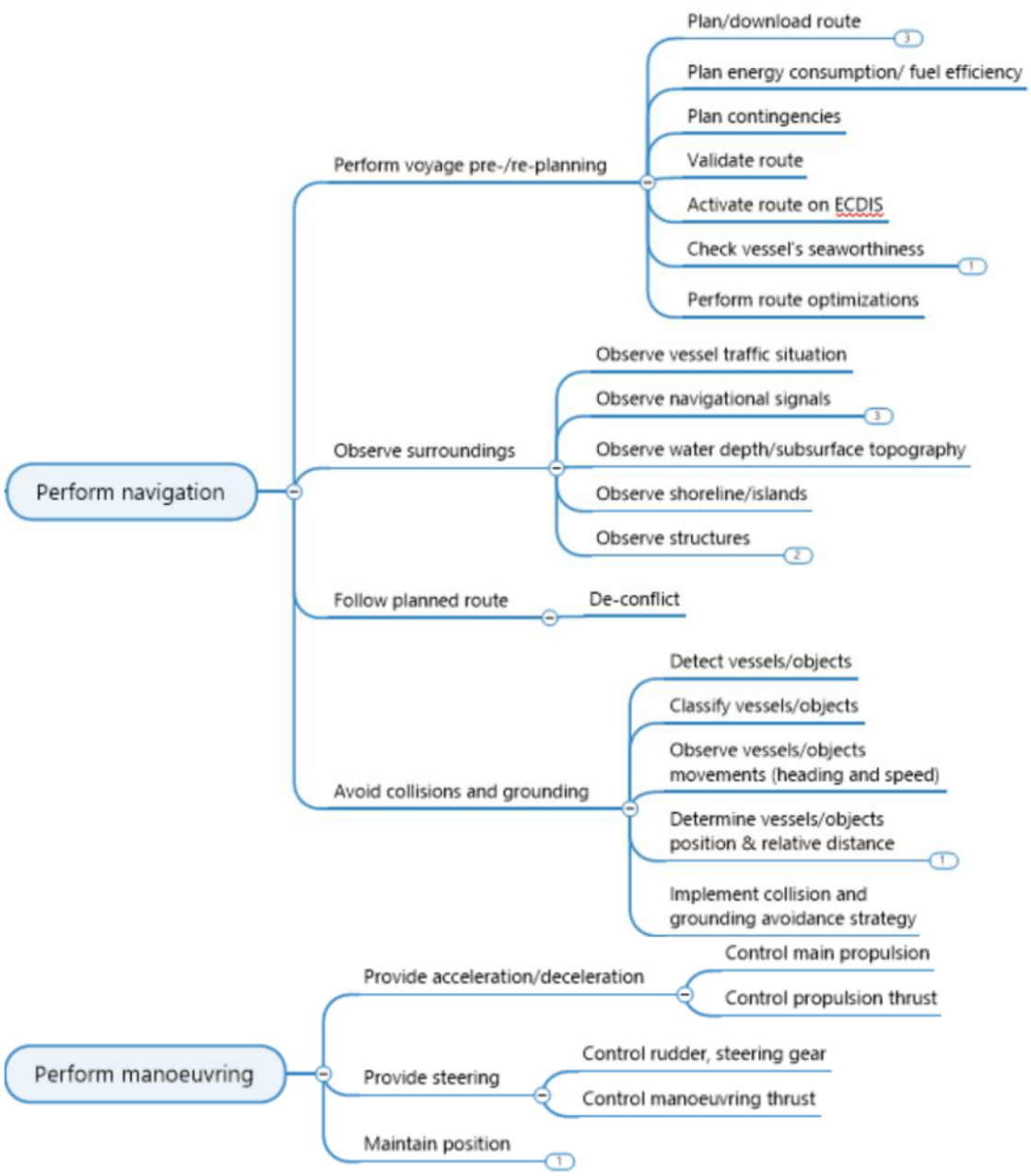
APPENDIX B
RBAT Mission Model

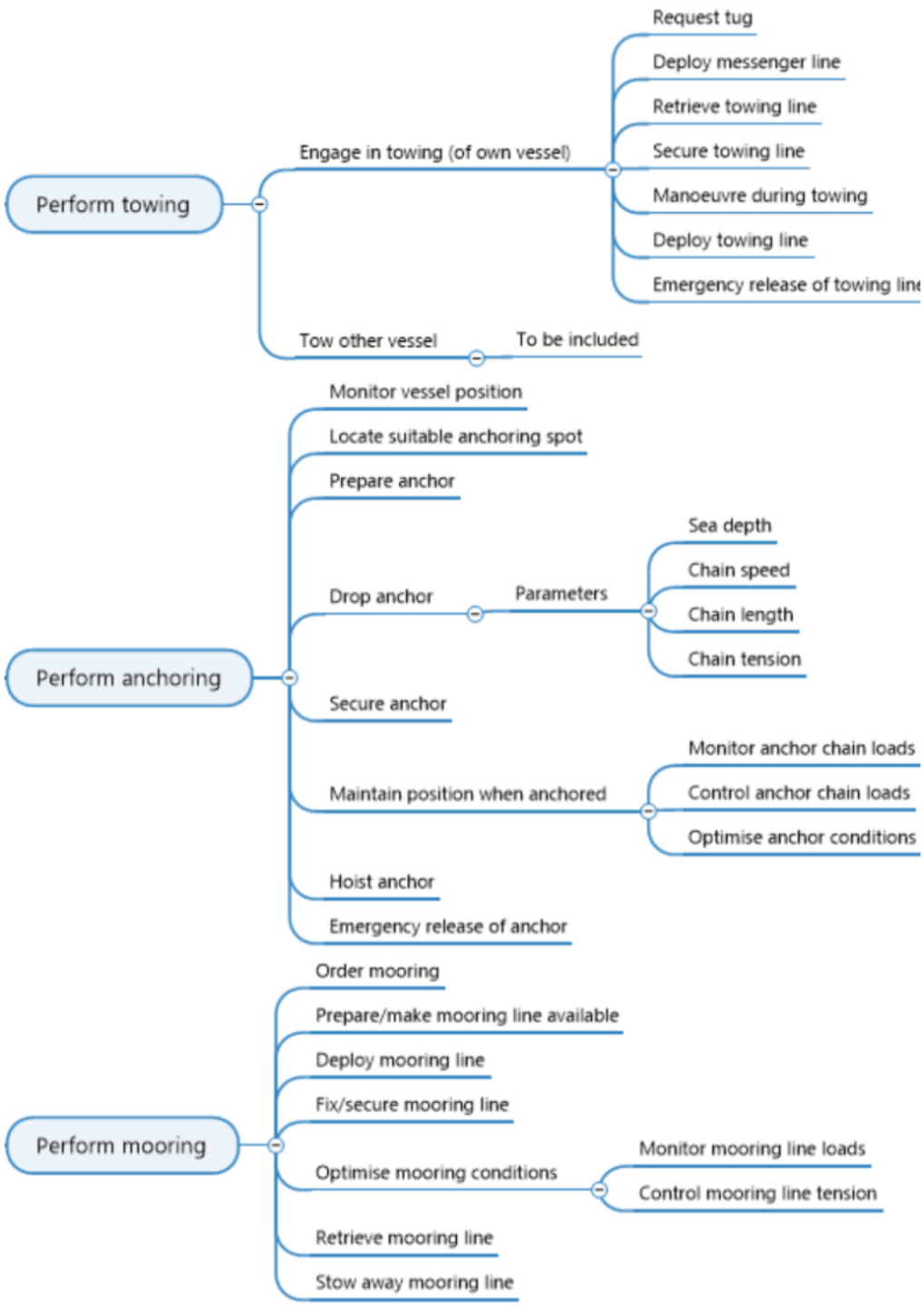


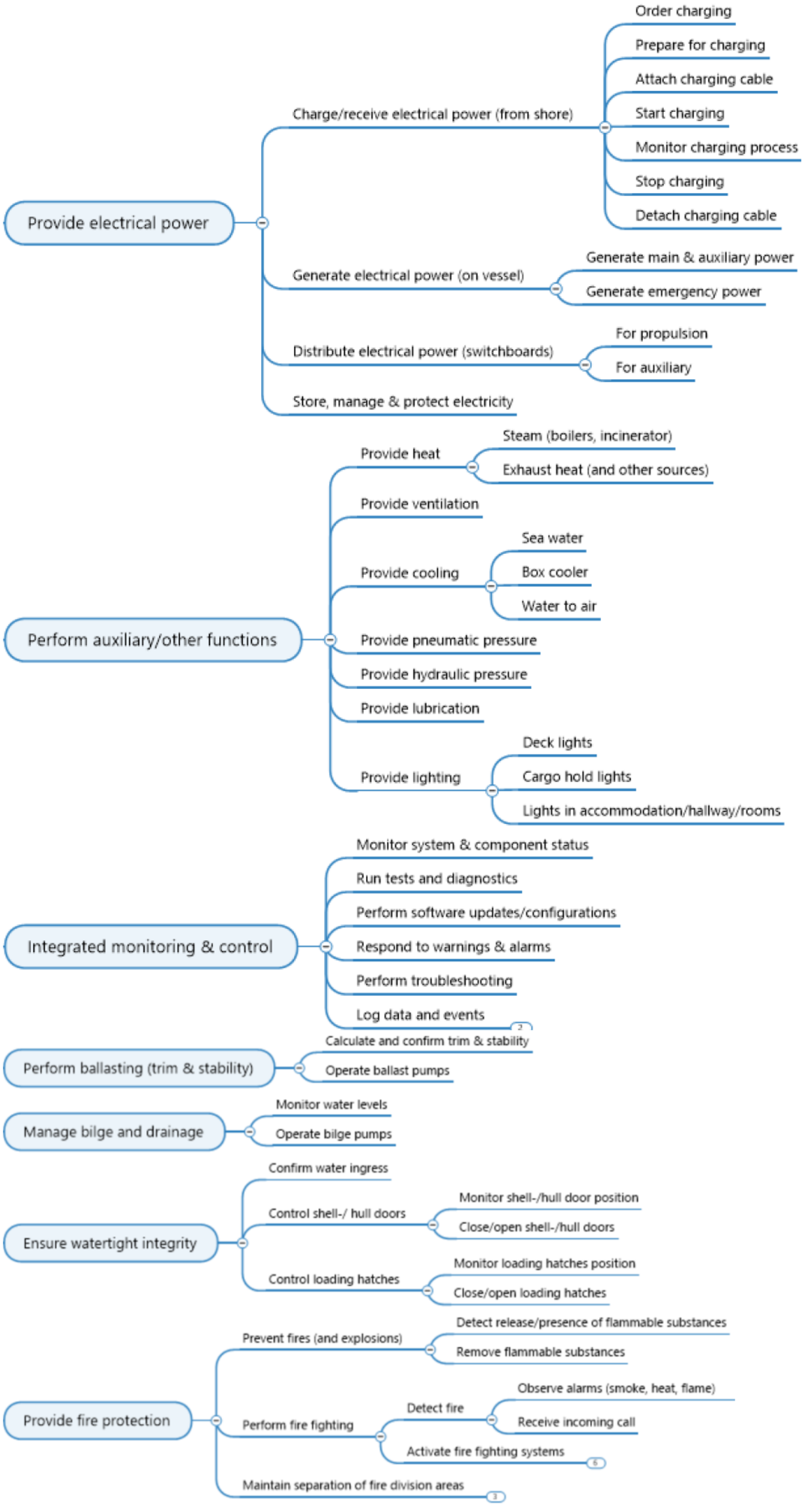
APPENDIX C
RBAT Function Tree

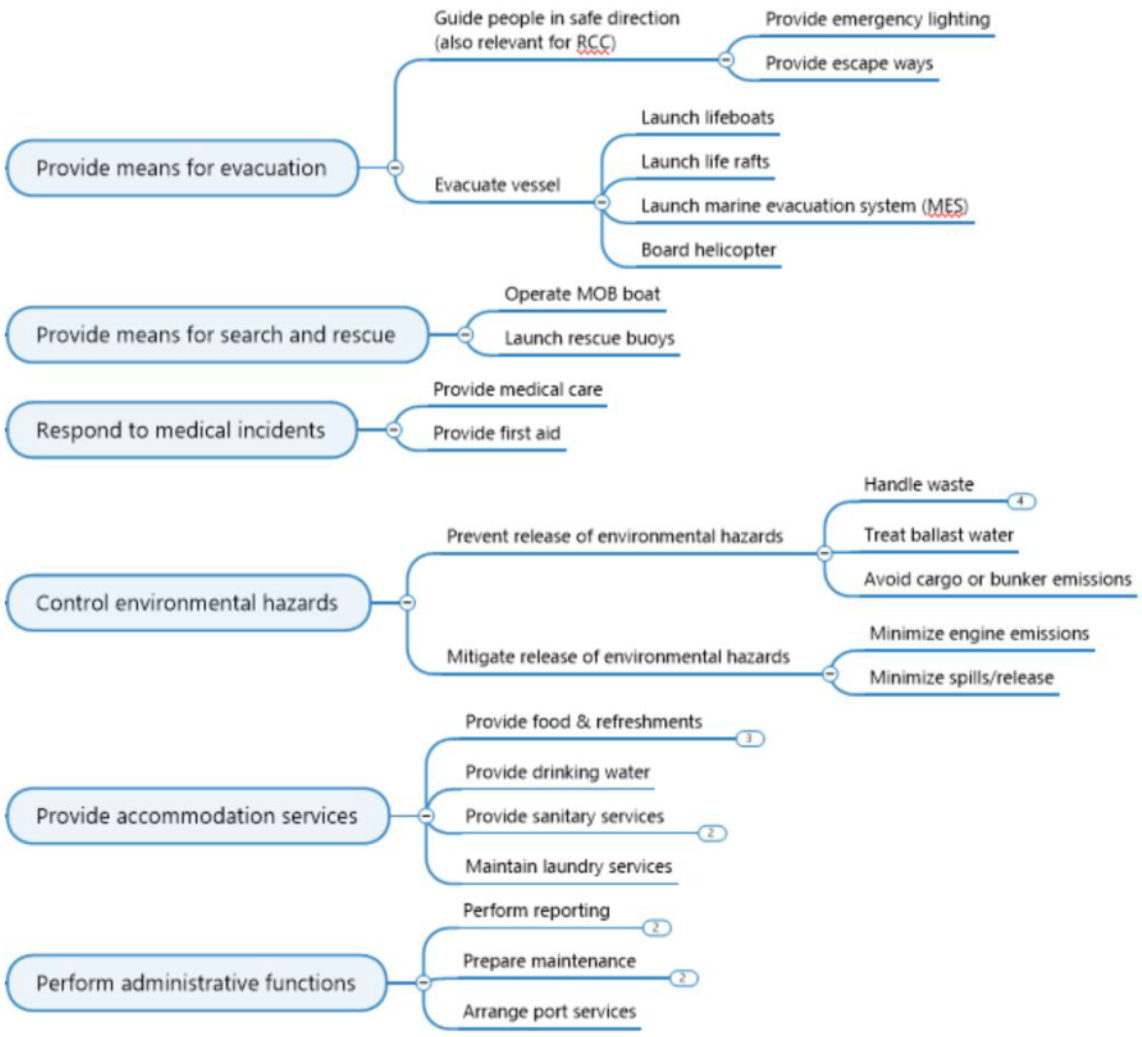



Observe weather conditions
Observe sea conditions
Tide
Current
Waves
Ice
Observe wind conditions
Speed
Direction
Observe visibility
5
Obtain weather forecast


Perform navigation
Perform voyage pre-/re-planning
Plan/download route
3
Plan energy consumption/ fuel efficiency
Plan contingencies
Validate route
Activate route on ECDIS
Check vessel's seaworthiness
1
Perform route optimizations
Observe surroundings
Observe vessel traffic situation
Observe navigational signals
3
Observe water depth/subsurface topography
Observe shoreline/islands
Observe structures
2
Follow planned route
De-conflict
Avoid collisions and grounding
Detect vessels/objects
Classify vessels/objects
Observe vessels/objects movements (heading and speed)
Determine vessels/objects position & relative distance
1
Implement collision and grounding avoidance strategy
Perform manoeuvring
Provide acceleration/deceleration
Control main propulsion
Control propulsion thrust
Provide steering
Control rudder, steering gear
Control manoeuvring thrust
Maintain position
1


Perform towing
Engage in towing (of own vessel)
Request tug
Deploy messenger line
Retrieve towing line
Secure towing line
Manoeuvre during towing
Deploy towing line
Emergency release of towing line
Tow other vessel
To be included
Perform anchoring
Monitor vessel position
Locate suitable anchoring spot
Prepare anchor
Drop anchor
Parameters
Sea depth
Chain speed
Chain length
Chain tension
Secure anchor
Maintain position when anchored
Monitor anchor chain loads
Control anchor chain loads
Optimise anchor conditions
Hoist anchor
Emergency release of anchor
Perform mooring
Order mooring
Prepare/make mooring line available
Deploy mooring line
Fix/secure mooring line
Optimise mooring conditions
Monitor mooring line loads
Control mooring line tension
Retrieve mooring line
Stow away mooring line


Provide electrical power
Charge/receive electrical power (from shore)
Order charging
Prepare for charging
Attach charging cable
Start charging
Monitor charging process
Stop charging
Detach charging cable
Generate electrical power (on vessel)
Generate main & auxiliary power
Generate emergency power
Distribute electrical power (switchboards)
For propulsion
For auxiliary
Store, manage & protect electricity
Steam (boilers, incinerator)
Perform auxiliary/other functions
Provide heat
Exhaust heat (and other sources)
Provide ventilation
Provide cooling
Sea water
Box cooler
Water to air
Provide pneumatic pressure
Provide hydraulic pressure
Provide lubrication
Provide lighting
Deck lights
Cargo hold lights
Lights in accommodation/hallway/rooms
Integrated monitoring & control
Monitor system & component status
Run tests and diagnostics
Perform software updates/configurations
Respond to warnings & alarms
Perform troubleshooting
Log data and events
Perform ballasting (trim & stability)
Calculate and confirm trim & stability
Operate ballast pumps
Manage bilge and drainage
Monitor water levels
Operate bilge pumps
Confirm water ingress
Ensure watertight integrity
Control shell-/ hull doors
Monitor shell-/hull door position
Close/open shell-/hull doors
Control loading hatches
Monitor loading hatches position
Close/open loading hatches
Provide fire protection
Prevent fires (and explosions)
Detect release/presence of flammable substances
Remove flammable substances
Perform fire fighting
Detect fire
Observe alarms (smoke, heat, flame)
Receive incoming call
Activate fire fighting systems
Maintain separation of fire division areas


Provide means for evacuation
Guide people in safe direction (also relevant for RCC)
Provide emergency lighting
Provide escape ways
Evacuate vessel
Launch lifeboats
Launch life rafts
Launch marine evacuation system (MES)
Board helicopter
Provide means for search and rescue
Operate MOB boat
Launch rescue buoys
Respond to medical incidents
Provide medical care
Provide first aid
Control environmental hazards
Prevent release of environmental hazards
Handle waste
4
Treat ballast water
Avoid cargo or bunker emissions
Mitigate release of environmental hazards
Minimize engine emissions
Minimize spills/release
Provide accommodation services
Provide food & refreshments
3
Provide drinking water
Provide sanitary services
2
Maintain laundry services
Perform administrative functions
Perform reporting
2
Prepare maintenance
2
Arrange port services

APPENDIX D
List of verbs

Information acquisition	Information analysis	Decision making	Action implementation
Access	Calculate	Command	Acknowledge
Detect	Classify	Conclude	Activate
Hear	Compare	Determine	Alert
Observe	Consider	Generate	Align
Read	Define	Plan	Announce
Receive	Identify	Select	Approve
Record	Integrate		Attach
Registrate	Interpret		Attain
Review	Organize		Brief
Scan	Predict		Close
Sense	Prioritize		Communicate
	Trend		Compute
	Verify		Configure
Action implementation cont.			
Continue	Extinguish	Monitor	Reset
Control	Fasten	Open	Respond
Coordinate	Fill	Operate	Secure
Cycle	Follow	Order	Stabilize
Deactivate	Guard	Perform	Start
Debrief	Illuminate	Position	Steer
Decelerate	Increase	Prepare	Stop
Decrease	Initialize	Pressurize	Stow
Depressurize	Initiate	Prevent	Test
Detach	Inspect	Proceed	Transmit
Deviate	Intercept	Program	Trim
Discharge	Interrogation	Provide	Tune
Eliminate	Isolate	Recover	Turn
Enter	Load	Remove	Unfasten
Evacuate	Maintain	Repeat	Unload
Exit	Manoeuvre	Report	Unsecure
Extend	Modify	Request	Update

APPENDIX E
Causal factors

A modern system may be subject to many different types of failures. Failures can be classified as:

- Random (hardware) failures,
- Systematic failures,
- Systemic failures,
- Operator failures,
- Failures due to environmental causes
- Failures due to deliberate actions.

Note that these categories overlap to some extent, yet they are useful as a guide to identify a wide range of failures that may pose risk.

Random hardware failures are linked to the physical properties of components. The term random is used because the exact moment a specific component will fail is unknown and does not imply that the failure happens arbitrarily. Typical failure rates for a large group of the same component can be predicted through analysis of statistics from field experience, and this makes it possible to perform Quantitative Risk Analysis (QRA) that takes into account the probability of failure for the different components in a system.

The degradation mechanisms that lead to random failures can to some extent be controlled by adjusting how components are designed produced, transported, installed, operated, and maintained. Thus, the failure rates for specific components will partly depend on the quality, operational and maintenance regimes applied. In this regard, it is important to be aware that generic failure rates for specific type of components consider all employed quality regimes equal, which is a simplification that represents an uncertainty in the calculations. Furthermore, it should be noted that the failure rates used in QRA typically excludes the run-in and wear-out periods, and therefore failures experienced in usage inside of these periods may be considered systematic failure events rather than random.

Systematic failure events are the consequence of inadequate work processes and may be introduced at all stages in the system lifecycle. Some examples are incomplete risk analysis, inadequate development of barrier strategies, incomplete requirement specifications, weaknesses in software design, programming errors, quality problems in hardware production, and inadequate planning of maintenance. It is difficult to quantify the probability of systematic failure events as they typically will be present in a system from day one, or introduced through modification, but be hidden until specific circumstances occur. This makes it difficult to compare the risks associated with different systems quantitatively, and necessitates broader risk descriptions if a comparison is to be made

A **systemic failure** is an event which occurs even if no individual component in the system has failed. This may be caused e.g., by overlooked dependencies among the technical, operational, human, and organisational elements of systems, specifications that are based on inadequate understanding of physical processes, or unexpected inputs for which no specific response has been specified. Increasing system complexity may increase the risk of systemic failures, and this is particularly relevant for systems containing software functions. It can be related to intricate dependencies and feed-back mechanisms among system components leading to nonlinear and unpredictable system behaviour. Lack of knowledge and understanding of interactions in a system increase the risk of systemic failures as it makes it difficult to implement robust barrier strategies to prevent them. Choice of simple solutions with few interacting or interdependent elements may reduce the risk of systemic failures and make systems more robust.

Operator failures occur when an operator fails to perform appropriate actions or performs an inappropriate action. The ability of an operator to perform appropriate actions and avoid inappropriate actions depends on the availability and quality of information to act on, the availability of sufficient time to act, and possession of knowledge of how to act. Therefore, the underlying causes of an operator failure may be systematic or systemic failures that involve technical, operational and organisational elements. In particular, operator failures may be dependent on system designs, operational procedures, training of the operator, and assumptions made in the risk treatment strategy. The latter includes availability of measures that realistically can be used to mitigate the risk under relevant operational conditions.

Failures due to environmental causes are caused by physical processes having negative influence on the control system. Some examples are: Lightning strike, water ingress, fire, electrostatic discharge from personnel, sensors covered by salt, and electromagnetic interference affecting communications. What is considered the environment depends on the boundaries of the system being analysed. E.g., loss of cooling in a control room may in some risk analyses be seen as an environmental cause, but not if the cooling system is a part of the system being analysed.

Failures due to deliberate actions may be caused for example by hacking, data viruses, physical sabotage, deliberate jamming of radio signals, GPS spoofing (false signals).

Regarding evaluation of possible mitigations, it should be considered that a systemic failure reflects inadequate identification of relevant requirements. Thus, systemic failure may be seen as a form of systematic failure introduced in the requirement specification phase. Mitigation of a failure scenario caused by inadequate requirements typically requires some level of functional diversity between the control functions affected by the failure and the mitigating measure.

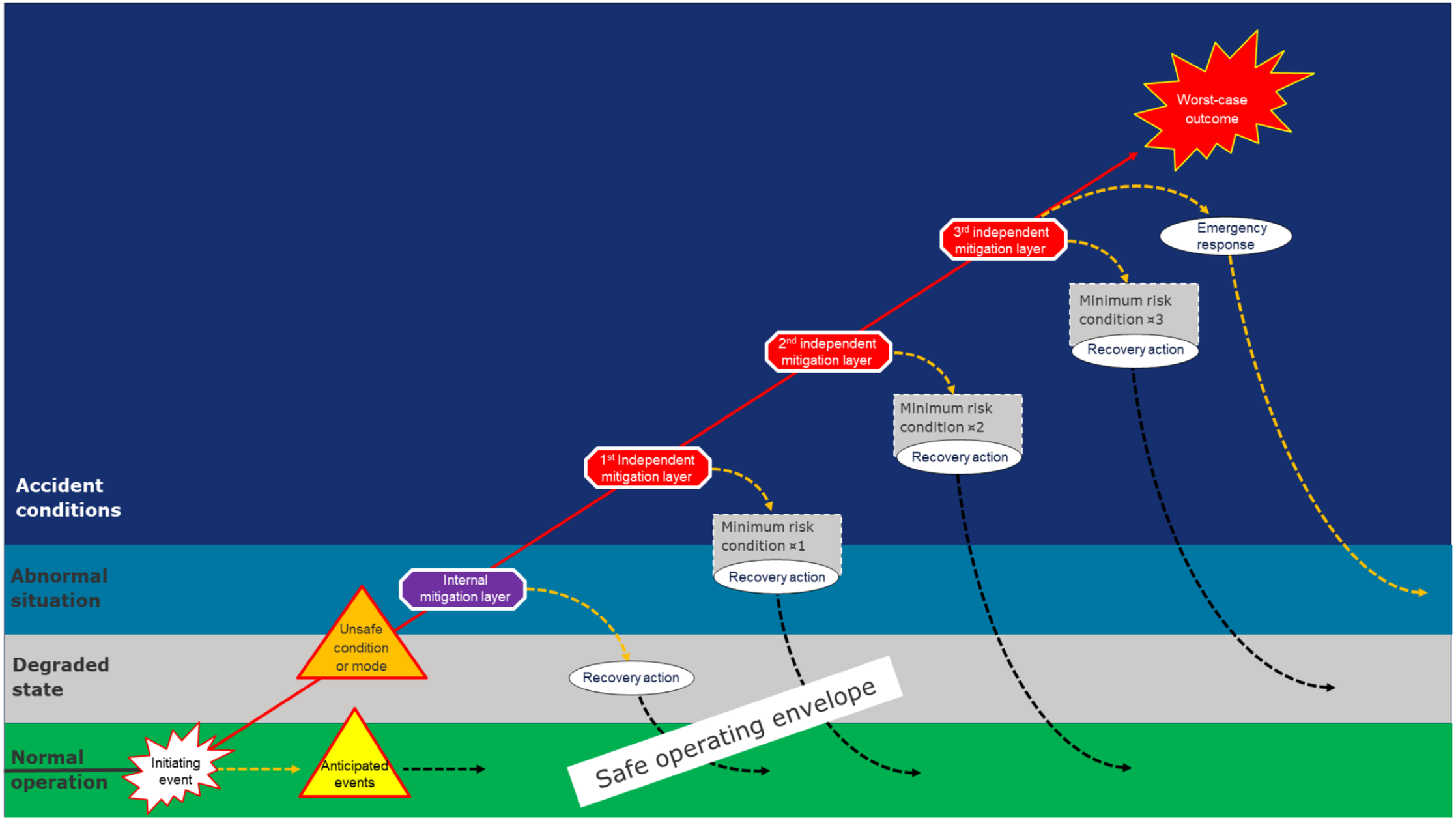
In general, all software failures are systematic or systemic in nature, although the occurrence of the input conditions revealing the weakness in the software may in some cases may be perceived as being random-like in nature. Local detection mechanisms, e.g., range checking and plausibility checks may be used to detect some of these. Other failures can only be detected at higher levels in the system that have a broader overview of the system state and the current operational mode, e.g., by comparing output from different controllers in functionally diverse subsystems, or through operator observation of system behaviour.

It will not always be possible to test a system under all relevant use scenarios, and it may even be that the test scenarios that are feasible to check are not realistic. In addition, for software functions within a system, the number of possible input combinations and possible execution paths typically prevents exhaustive testing even when using a simulated environment. This means that testing typically can only demonstrate the presence of conditions that can lead to failures and not their absence. A cautionary approach is therefore warranted to make systems robust to unforeseen conditions that it may experience. This may include fall-back solutions and use of safety margins considering worst-case scenarios.

It will in many cases not be possible to implement detection for all types of systematic/systemic failures. E.g., incomplete analysis of systems, operations, interfaces, and risks may lead to omissions in specifications evading all detection mechanisms. For safety-critical systems, there must either be an efficient fallback chain, or it must be possible to argue that activities associated with analyses, development, verification, and validation have reduced the likelihood of systematic and systemic failures to a tolerable level.

The latter approach may be challenging, e.g., the number of possible combinations of inputs to the system, and the number of possible sequences of input combinations can make it difficult to know whether specifications are complete. Thus, in practice, one often uses a combination where both a fallback chain and a rigorous development process are used to reduce residual risk to a tolerable level.

Since the effectiveness of mitigation measures varies with the type of cause, it is important to consider all failure categories mentioned at the start of this section when performing risk analysis and developing risk treatment strategies. For example, hardware redundancy in combination with voting may be an efficient mitigation against random hardware failures, but it will not be efficient if the cause is systematic or systemic. Furthermore, the use of functional diverse supporting functions may reduce risks related to systematic failures in those functions, but it may not be efficient against systematic failures in the top-level function. Operator intervention through independent means may be efficient against systematic failures in the top-level function, but additional measures may be necessary if the cause is an operator failure, fire and flooding, or deliberate actions like hacking or sabotage.


Worst-case outcome
3rd independent mitigation layer
Emergency response
Minimum risk condition ¤3
Recovery action
2nd independent mitigation layer
Minimum risk condition ¤2
Recovery action
1st Independent mitigation layer
Minimum risk condition ¤1
Recovery action
Internal mitigation layer
Unsafe condition or mode
Recovery action
Accident conditions
Abnormal situation
Degraded state
Normal operation
Initiating event
Anticipated events
Safe operating envelope

APPENDIX G
How to create a mitigation register

The mitigation layers can be initially identified by considering what the responses would be in case various failures, loss of control or accident scenarios should occur. The generic accident categories presented in Table 23 can be used as a starting point for such considerations. Alternatively, this work is done after performing the hazard analysis as part of RBAT.

Each mitigation layer should be listed with an:

- ID
- Name
- Short description

Furthermore, information necessary to evaluate the mitigation layers risk reducing effectiveness (Step 15) must be gathered. This includes:

- Applicability of the mitigation layer
    - For which incidents the mitigation layer is a planned response
    - For which mission phases the mitigation layer is applicable
    - For which mission phases the mitigation layer is NOT applicable, e.g., due to:
        - Being potentially unsafe
        - Restricting use of other mitigation layers
        - Not being relevant (i.e., effective)
- System and human involvement in the mitigation layer
    - Systems which must function and be available for executing the mitigation layer
    - Human-automation interactions required as part of the mitigation layer (see subchapter 6.3.4.3 for further explanations)
- Limitations to the mitigation layer
    - External/ environmental limitations in the mitigation layer (e.g., sea state, visibility, day/night, availability of external resources)
    - Resource limitations in the mitigation layer (e.g., time, fuel, energy reserves, manpower, etc.)
    - Limitations in the sequence mitigation layers can be introduced (e.g., a mitigation layer should only be activated after another has been exhausted)
- Transitions between and from mitigation layers (including minimum risk conditions)
    - Recovery actions taken to re-enter a normal or as safe-as-possible operational mode (in case the mitigation layer involves entering a minimum risk condition (MRC)
    - What the next mitigation(s) in the sequence is, and how to introduce it (“None” in case the mitigation is a last resort MRC)
    - Emergency response in case there are no other mitigation layers available

About DNV

DNV is the independent expert in risk management and assurance, operating in more than 100 countries. Through its broad experience and deep expertise DNV advances safety and sustainable performance, sets industry benchmarks, and inspires and invents solutions.

Whether assessing a new ship design, optimizing the performance of a wind farm, analyzing sensor data from a gas pipeline or certifying a food company's supply chain, DNV enables its customers and their stakeholders to make critical decisions with confidence.

Driven by its purpose, to safeguard life, property, and the environment, DNV helps tackle the challenges and global transformations facing its customers and the world today and is a trusted voice for many of the world's most successful and forward-thinking companies.