European Maritime Safety Agency

FRAMEWORK FOR GENERIC RISK ASSESSMENT TOOL FOR MASS CONCEPTS

REPORT 2 OF 2

Version: 2021-0480, Rev. 0

Date: 18/12/2020

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 EMSAs Tender Specifications (EMSA, 2020a) and DNVs proposal (DNV GL, 2020d), 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 software tool

The study is currently in its final stages of Part 1 which includes the following scope of work:

a) a multi-level function map including functions potentially being re-allocated from humans to systems,

b) definitions characterizing use of automation, and a format suitable for collecting data describing such systems and their associated risks,

c) a list of hazardous conditions and events which can be linked to functions being targeted for various levels of automation, and

d) a risk model and methodology which enable identification of high-risk areas and risk reducing measures.

The framework developed in Part 1 shall accommodate assessments of a wide range of MASS concepts and application of risk acceptance criteria and principles of safety equivalence for risk reduction. The focus is on safety-related aspects, and not concerns related to cybersecurity (unless they have on safety).

Activities a) and b) are documented in Report 1/2 for Part 1. This is Report 2/2 and documents activities c) and d). The main deliverables from Report 1/2 have also been included for the sake of completeness.

RBAT workshop

A workshop was arranged to discuss and seek answers to the following questions:

Which purpose(s) shall RBAT fulfil?

Who will be the main users of RBAT?

What are the user characteristics?

How will RBAT be used in different project stages?

What are the methodological requirements?

How should the format of RBAT deliverables look like?

In addition to EMSA and DNV, participants included representatives from various Flag States in the European Union, ship owners and academia. DNV facilitated and recorded the workshop. A summary of the workshop discussions resulted in a set of key take-aways some which have been used as input for developing the RBAT framework, and some which will be brought forward as input for upcoming activities.

Hazard identification

A hazard identification (HAZID) was prepared, executed with the aim to identify all possible hazards at a generic level. Following an extensive literature review, the preparations included establishing a list of accident categories, as well as identifying a set of generic hazard descriptions, and examples of direct causes. Because the HAZID was generic (and not ship specific) the study itself was partly conducted as a desktop exercise, and partly as small workshops, in-house DNV.

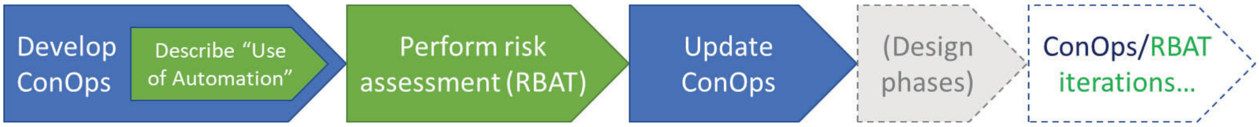
A HAZID log sheet and the other deliverables was used to develop a matrix which links failure of functions in the RBAT Function Tree to EMSA's accident categories (EMSA, 2020b) This, in turn, shall form a part of the RBAT framework and methodology.

RBAT approach

The main purpose of RBAT is to *risk assess whether increased or new ways of using automation and remote operation is as safe or safer than conventional shipping*.

Furthermore, it is being developed to help the user meet the objectives a *preliminary risk analysis* (DNV GL, 2018) which is commonly applied during the concept development stages as a *screening approach*[1] (IMO, 2018). The purpose is to screen out the concept's less critical aspects, so that more resources can be devoted to those areas which deserve additional attention when further maturing the operational solutions and the vessel's or infrastructure's design. Such attention may be provided in form of identifying the needs for more detailed risk analysis or implementation of technical and operational risk control measures.

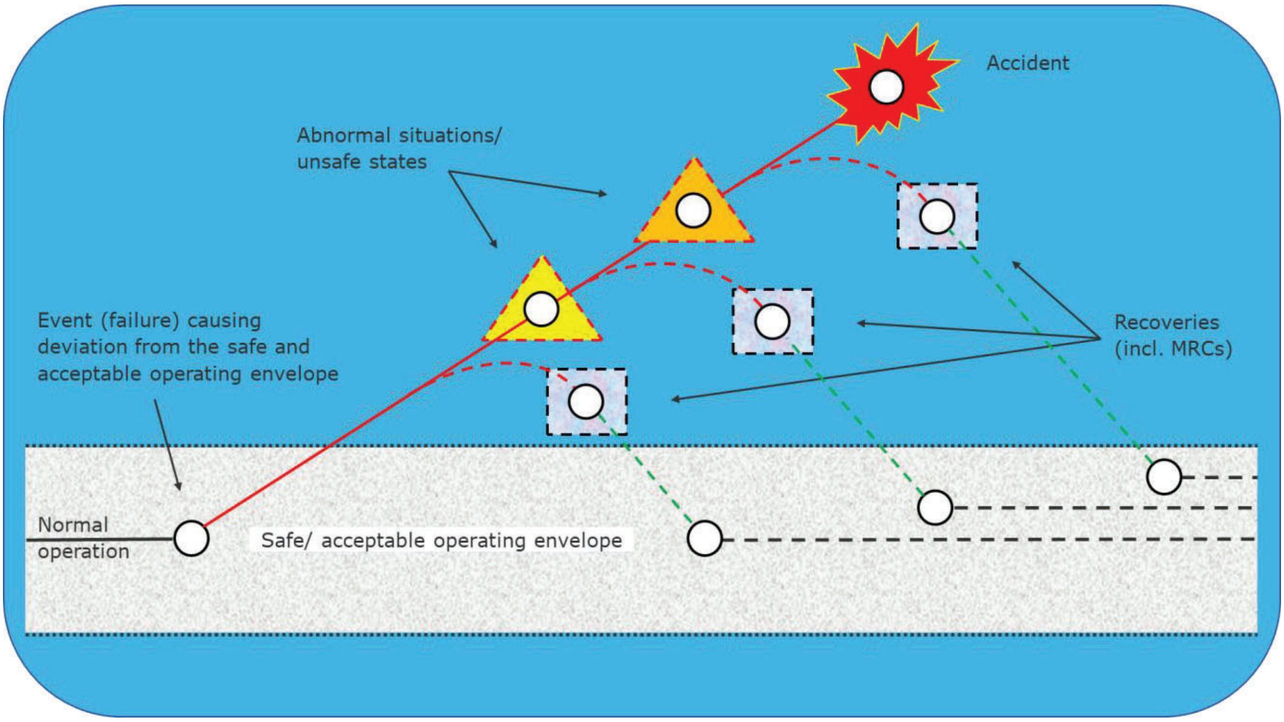
The Concept of Operations (ConOps) document is intended to be RBAT's main input and efforts have been made to ensure that the RBAT framework matches the expected format and contents of such reports (LR, 2017; DNV GL, 2018; ABS, 2020). Most of the class society guidelines expects that the ConOps describes the vessel(s) mission and associated operations. This includes descriptions of the planned voyage phases, the various operational modes and envelopes, as well as the functions involved. Explanations should be provided about which functions shall be assigned to either automation or humans, and in what context (modes, situations). This is often the most detailed part of the ConOps and the part which is commonly matured the latest. The RBAT Mission Model and Function Tree, as well as definitions explaining use of automation, are tools which can be of support when developing the ConOps and ensure that it is ready to use as input to RBAT. It is therefore recommended to start preparing parts of the input to RBAT already as part of writing the ConOps. Not only will this provide confidence that the ConOps takes all aspects of the vessel mission and functionality into account, it also avoids the risk of having to redo work in case there is a significant mismatch between the ConOps and RBAT terminology or structure. Both the ConOps and risk assessment should be updated at suitable milestones, e.g. when all recommendations about improvements in design have been implemented. A rough outline of the process is illustrated in the figure below.


Develop ConOps
Describe "Use of Automation"
Perform risk assessment (RBAT)
Update ConOps
(Design phases)
ConOps/RBAT iterations...

RBAT risk model

A risk model has been developed specifically to accommodate the objective of RBAT. It builds on knowledge extracted from DNV GL's class guideline (2018), the SAFEMASS project (DNV GL 2020a; 2020b), hazard analysis techniques used in the aviation industry (SAE, 1996; 2010), as well as recent publications on MASS risk assessments (Ramos et al., 2019 ;2020). This knowledge has been used to create an illustration for explaining accident causation, which is further translated into an event sequence diagram. The figure below illustrates an accident as events (e.g. failures) causing the system to deviate from its normal and safe operational state, and into an abnormal unsafe state. Unless recovery actions are successful at brining the system back into a safe an acceptable operating envelope, the situation may escalate into an accident.

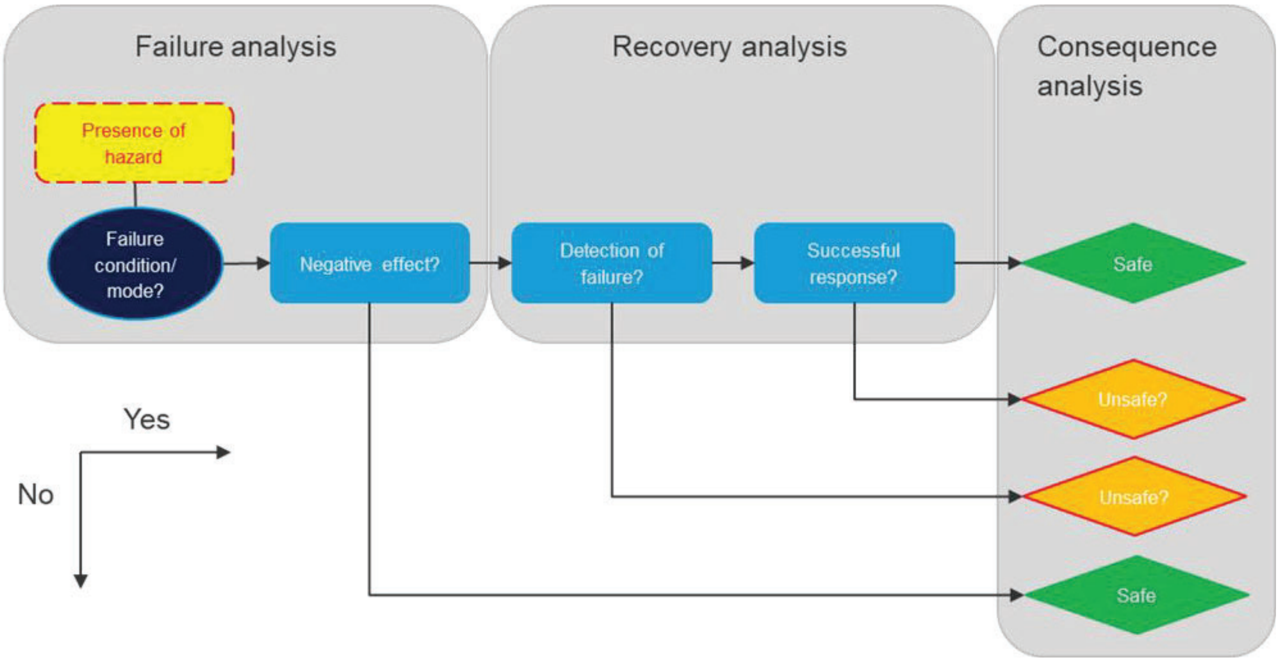
[1] *Screening approach* as per in REF MSC-MEPC.2/Circ.12, para 3.1.2


Accident
Abnormal situations/ unsafe states
Event (failure) causing deviation from the safe and acceptable operating envelope
Recoveries (incl. MRCs)
Normal operation
Safe/ acceptable operating envelope

A generic event sequence diagram has been developed following the same logic as used in the accident model described above. The diagram serves three main purposes. One is to provide a structure for the data collection and analyses table intended to be used as part of applying RBAT. The table includes columns for capturing data about each of the event in the diagram (a more detailed explanation is given later in the Ex. summary). The second is to form a logic structure for the quantification of risk levels. As per now, the risk associated with a function failure can be described as:

*Frequency of failure condition/mode * Probability of recovery failure * Severity of worst-case outcome*

The third purpose is to support informed decision-making about implementation of risk control measures targeted at either reducing failure frequencies, improving means for recovery, or mitigating consequences.

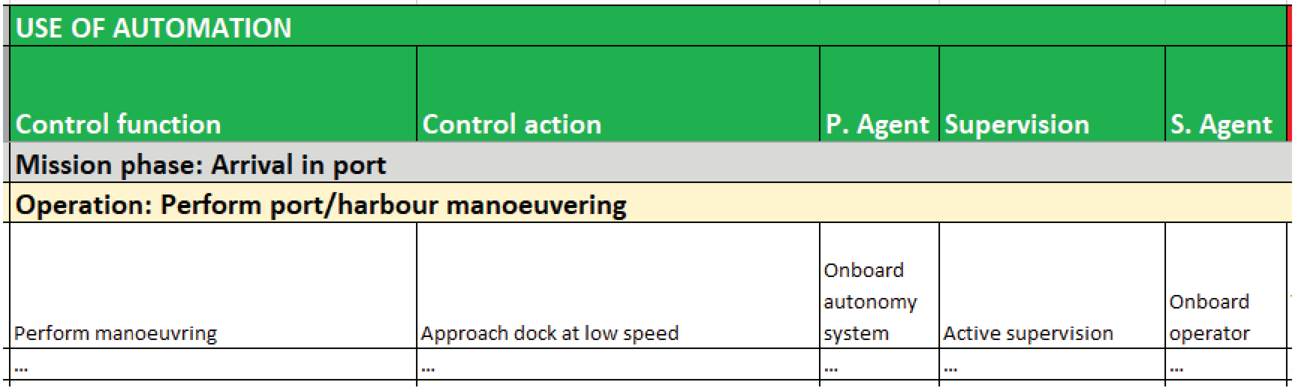


Step-by-step guidance

The report describes a detailed step-by-step guidance for how to apply the RBAT methodology which consists of five main parts and 14 steps. These are presented below, together with their respective modules in RBAT, currently set up using an Excel worksheet. In RBAT the figures are indeed linked and should therefore be read from left to right.

Part 1: Define Use of Automation

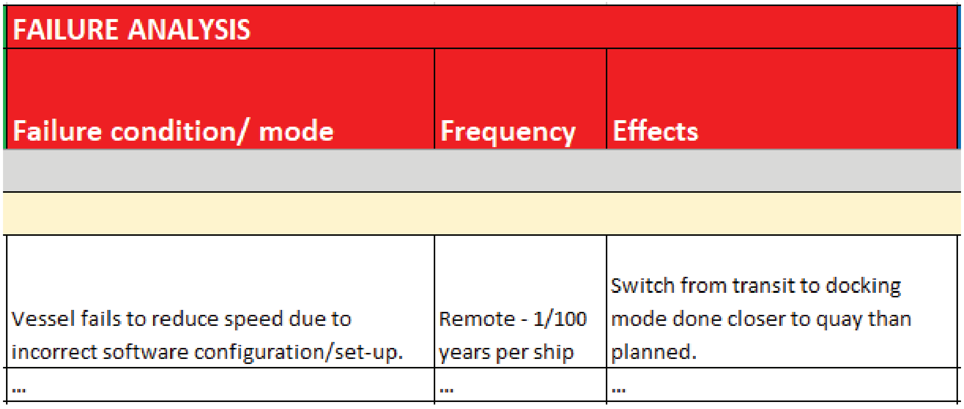
- Step 1: Describe the vessel(s) mission (operational goals)
- Step 2: Describe the automated and/or remotely controlled functions (functional goals)
- Step 3: Describe how control functions are allocated to agents
- Step 4: Assign responsibility for supervision of control actions



USE OF AUTOMATION				
Control function	**Control action**	**P. Agent**	**Supervision**	**S. Agent**
Mission phase: Arrival in port				
Operation: Perform port/harbour manoeuvering				
Perform manoeuvring	Approach dock at low speed	Onboard autonomy system	Active supervision	Onboard operator
…	…	…	…	…

Part 2: Perform failure analysis

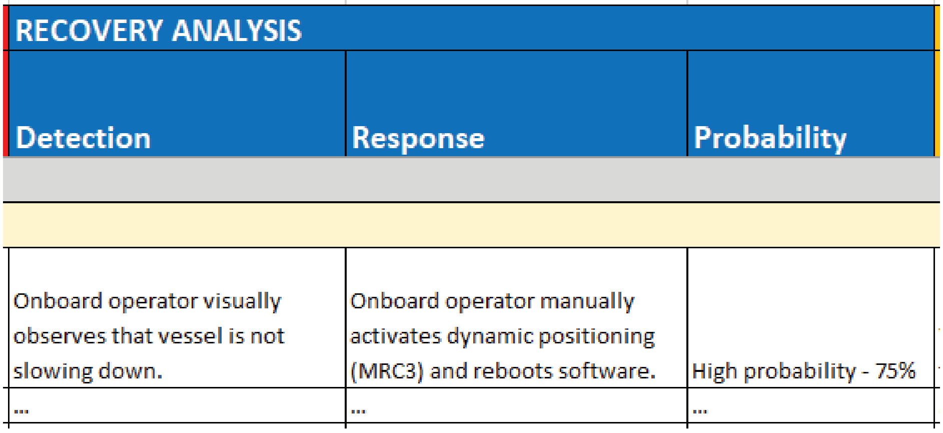
- Step 5: Identify and describe failure conditions/ modes
- Step 6: Assign a frequency for the failure conditions/ modes occurrence
- Step 7: Determine the effects from failure conditions/ modes



FAILURE ANALYSIS		
Failure condition/ mode	**Frequency**	**Effects**
Vessel fails to reduce speed due to incorrect software configuration/set-up.	Remote - 1/100 years per ship	Switch from transit to docking mode done closer to quay than planned.
…	…	…

Part 3: Perform recovery analysis

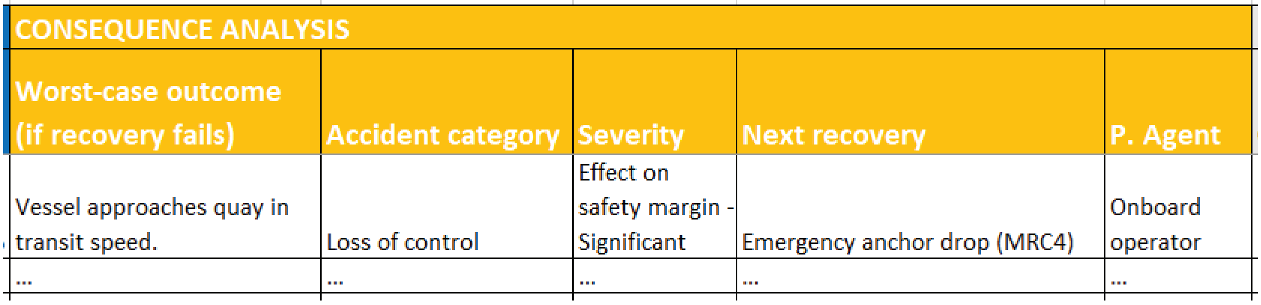
- Step 8: Assess how failure conditions/ modes can be detected
- Step 9: Assess how failure conditions/ modes shall be responded to
- Step 10: Assign a probability for recovery being successful



RECOVERY ANALYSIS		
Detection	Response	Probability
Onboard operator visually observes that vessel is not slowing down.	Onboard operator manually activates dynamic positioning (MRC3) and reboots software.	High probability - 75%
...	...	...

Part 4: Perform consequence analysis

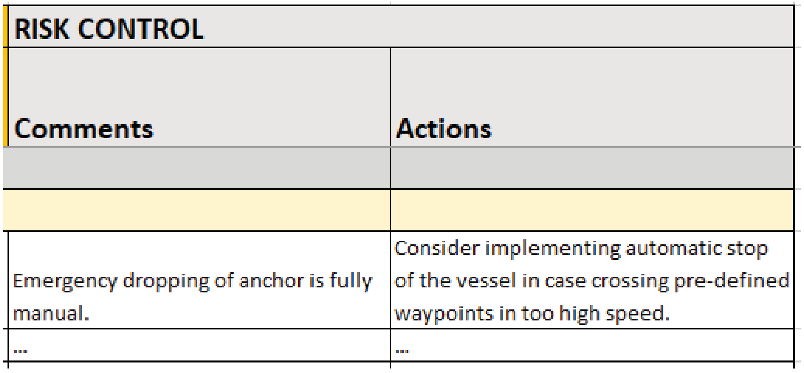
- Step 11: Describe the worst-case outcomes
- Step 12: Rank the worst-case outcome severity
- Step 13: Identify the next recovery (in case the previous one fails)



CONSEQUENCE ANALYSIS				
Worst-case outcome (if recovery fails)	Accident category	Severity	Next recovery	P. Agent
Vessel approaches quay in transit speed.	Loss of control	Effect on safety margin - Significant	Emergency anchor drop (MRC4)	Onboard operator
...	...	...	...	...

Part 5: Address risk control

- Step 14: Identify and document risk control measures



RISK CONTROL	
Comments	**Actions**
Emergency dropping of anchor is fully manual.	Consider implementing automatic stop of the vessel in case crossing pre-defined waypoints in too high speed.
...	...

Aggregated analyses

The current version of RBAT is limited to addressing risks and control measures per function. It is however set up to create opportunities for using the captured data to perform aggregated analyses, particularly if supported by suitable software features. It is proposed that the following opportunities should be explored as part of the further developments of RBAT:

- *Human involvement.* RBAT collects data which can be used for controlling potential impacts on human performance induced by being required to perform control actions and supervision for multiple vessels. Examples include excessive workload, increased task complexity, having to deal with multiple and potentially conflicting task goals, and limited time available causing a lack of situational awareness.

- *Event sequences.* In complex system such as MASS, single failure conditions/ modes may not appear to be critical, but in combination with others they may prove to be catastrophic. For worst-case outcomes which do not directly result in an accident, RBAT ranks severity in terms of effect on safety margin. This feature can be used to check how combinations of failures can cause accidents.

- *Accident contribution.* By keeping track of which accident categories various functions contribute to, also across the vessel's mission phases and operations, it is possible to consider whether additional attention should be devoted on certain functions, for example in terms of equipment reliability/availability, supervision, as well as inspection and maintenance.

Recommendations for Part 2 of RBAT

The following recommendations have been noted for Part 2 of the RBAT study:

- Preliminary testing of RBAT performed as part of the method development has brought forward some indications that a separate definition for supervision by a machine agent may be needed.

- A significant part of the failure conditions/modes will result from software failures or limitations. Challenges related to predicting software failure modes as well as frequencies need to be explored and understood so that a suitable approach for risk ranking can be developed.

- It should be considered to add a column in RBAT for describing failure causes. This may be helpful for determining failure frequencies as well as pinpointing the most suitable recovery actions.

DEFINITIONS

Terms	Definitions
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 machine (computer) responsible for performing or supervising control actions.
Annunciated failure	An annunciated failure condition is one which fails ‘actively’, i.e. in such a manner as to inform crew of the failure, either by virtue of indicators or via vessel behaviour obviously attributable to it (adapted from Kritzinger, 2017).
Automation	The execution by a ‘machine’ *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 ½ for Part 1 of RBAT (DNV GL 2020c).
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 machines for the accomplishment of a functional goal (adapted from IEC, 2000).
Control action	Acquisition or analysis of information, decision-making, or implementation of physical actions performed as part of a control function.
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.
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 GL, 2019).
Failure cause	Set of circumstances that leads to failure (IEC, 2018).

Terms	Definitions
Failure condition	A condition with an effect on the vessel and its occupants (if present), both direct and consequential, caused or contributed to by one or more failures, considering relevant adverse operation or environmental conditions (SAE, 1996).
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 GL, 2019).
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 machine (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).
Functional hazard analysis	A systematic, comprehensive examination of functions to identify and classify failure conditions according to their severity (SAE, 1996).
Function tree	Hierarchical breakdown of high-level key functions into a set of sub-functions.
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.

Terms	Definitions
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 (IEC, 2018).
Initiating event	The first of a sequence of events leading to a hazardous situation or accident (IMO, 2018).
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 the highest level of functions in the Function Tree.
Minimum risk condition	A state that the ship should enter when the system experiences situations that are outside those in which it can operate normally, but is still expected to deal with in one way or another (adapted from DNV GL, 2018a).
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.
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 GL, 2019). 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 GL, 2019).

Terms	Definitions
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 GL, 2019). In quantitative terms, it is one (1) minus the failure probability.
Redundancy (of a system)	Having multiple capabilities for performing the same function, typically in parallel (DNV GL, 2019). Alternatively, Provision of more than one means for performing a function (IEC, 2018).
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 GL, 2019): — 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 d) control e) mitigation f) emergency response.
Risk control options	A combination of risk control measures (IMO, 2018).
Scenario	Possible sequence of specified conditions under which the system, item or process functions are performed (IEC, 2018).
Severity	Relative ranking of potential or actual consequences of a failure or a fault (IEC, 2018).
System	Combination of interacting elements organized to achieve one or more stated purposes, i.e. goals (IEC, 2018).
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*.

Terms	Definitions
Undetected/ unannunciated failures	An unannunciated failure is potentially a latent or passive failure condition, or one that is misleading. A failure is latent until it is made known to the crew or maintenance personnel (adapted from Kritzinger, 2017).
Worst-case outcomes	The outcome of a failure condition/mode in case recovery is unsuccessful (fails).

1 INTRODUCTION

EMSA has contracted DNV to perform a functional study for developing a Risk-Based Assessment Tool (RBAT) for MASS. As outlined in EMSAs Tender Specifications and DNVs proposal, the RBAT study consist of three parts:

- Part 1: Development of a framework for a generic risk assessment tool
- Part 2: Specific test cases on the risk assessment tool
- Part 3: Assessment of multi-function automation and software tool development

This is Report 2/2 for issued for Part 1. The main deliverables from Report 1/2 have also been included in this report, in order to have the complete RBAT framework available in a single document. This mainly consist of definitions for explaining human involvement in automation, as well as the RBAT Mission Model (Appendix A) and Function Tree (Appendix B). Nevertheless, it is recommended to first read Report 1/2, for a more complete understanding of RBAT.

1.1 Scope of work

The scope of work for Part 1 consist of developing:

e) a multi-level function map including functions potentially being re-allocated from humans to systems,

f) definitions characterizing use of automation, and a format suitable for collecting data describing such systems and their associated risks,

g) a list of hazardous conditions and events which can be linked to functions being targeted for various levels of automation, and

h) a risk model and methodology which enable identification of high-risk areas and risk reducing measures.

The framework developed in Part 1 shall accommodate assessments of a wide range of MASS concepts and application of risk acceptance criteria and safety equivalence for risk reduction. This is planned to be addressed during Part 2.

The focus is on safety-related aspects, and not concerns related to cybersecurity (unless they have implications for safety).

Activities a) and b) are documented in Report 1/2 for Part 1. This report documents activities c) and d).

1.2 Updates to the framework described in Report 1/2

Most of the framework described in Report 1/2 remains unchanged. Some improvements related to activity a) and b) have however been implemented. For a) minor updates have been made to the RBAT Mission Model and Function Tree. The current versions are therefore included as Appendices in this report. For b) this mainly concerns the definitions and table format used to describe human involvement. Report 1/2 defined human involvement in terms of performing, supporting, or supervising control actions. This has now been changed to humans either being agents responsible for supervising or performing control actions, and supervision has been divided into either passive or active supervision. The reason for excluding *support* as a separate responsibility and type of involvement was that it was difficult to distinguish it from the responsibility of *performing* a control action. As such, in cases where human agents have a more supportive role in achieving a functional goal, these are represented through control actions they are required to perform, in conjunction with other control actions performed by a machine agent. Steps 3 to 4 in sub-chapter 6.1 and 8 to 10 in sub-chapter 6.3 accounts for these updates.

2 RBAT WORKSHOP

A RBAT workshop was arranged in weeks 9 and 10 of 2021. The workshop consisted of four half-day sessions, held on the 3rd, 4th, 9th, and 10th of March. The main purpose of the workshop was to present RBAT and receive feedback about the following topics:

Which purpose(s) shall RBAT fulfil?

- Design improvements?
- Assurance?

Who will be the main users of RBAT?

- Applicants?
- Approvers?
- Others?

What are the user characteristics?

- Background (education, experience)?
- Competence in risk analysis?
- Formal roles (responsibilities)?

How will RBAT be used in different project stages?

- Early concept development/ high level design?
- Detailed design?
- Commissioning/ testing?

What are the methodological requirements?

- Quantification?
- Accuracy/validity/reliability?
- Level of detail?

How should the format of RBAT deliverables look like?

- Transparency/traceability/consistency?
- Interface with other documents?

In addition to EMSA and DNV, participants included representatives from various Flag States in the European Union, ship owners and academia. The Flag States made up the majority (see Table 1). DNV facilitated and recorded the workshop.

Table 1 – Participants in RBAT workshop

Name	Organisation	Role
Sifis Papageorgiou	EMSA	Senior Project Officer
Erik Tvedt	Danish Maritime Authority	Special Adviser
Jean-Baptiste Merveille	SPF Mobilité et Transports	Attaché
Joerg Kaufmann	BSH (Federal Maritime and Hydrographic Agency)	Head of Department
Antonino Scarpato	Italian Coast Guard Headquarters	Lieutenant commander
Thomas Axelsen	Norwegian Coastal Administration	Senior Advisor
Ragnar Stangring	Wilhelmsen	Site Captain (Yara B.)
Dag Rutledal	NTNU	Phd candidate
Are Jørgensen	DNV	Senior Principal Engineer
Tore Relling	DNV	Principal Consultant

Sondre Øie	DNV	Principal Consultant

A summary of the workshop discussions resulted in a set of key take-aways (

Table 2), some which have been used as input for developing the RBAT framework, and some which will be brought forward as input for upcoming activities.

Table 2 – Key take-aways from RBAT workshop

Topic	Key take-aways
Application area	It is expected that RBAT will be applied to a wide variety of MASS concepts, both in terms of size and complexity, but also novelty. This may range from small vessels such as tugs and harbour ferries (sea busses), up to entire fleets consisting of vessels performing unique and specialized operations.
Structure and approach	Overall, the proposed RBAT structure and approach is believed to improve the quality and validity of MASS risk assessments. Using the RBAT Mission Model and Function Tree provides confidence that relevant risks will be addressed. This will also make it easier to review and check what has not been assessed/ discussed.
Users	RBAT users can be divided into two main categories; Applicants and Approvers.
Users – Applicants	The Applicant is responsible for having the risk assessment carried out and submitted for approval. This could be a shipowner or product developer. The actual task of carrying out the risk assessment can however be delegated to another party, such as a yard or consultancy. There may be several Applicant sub-groups, e.g. those carrying out and being involved in the assessment, and those using its results.
Users – Approvers	Approvers are the governmental (flag state) administrations/authorities or class societies responsible for reviewing risk assessments as part of an approval process.
User competence profile	No specific job role has been identified as a preferred user, neither for Applicants nor Approvers. It is however expected that most Applicants will have access to basic risk analysis competence, either in-house or through a contracted party. Approvers are familiar with reviewing and participating in risk assessments (e.g. workshops) as part of their job.
Training	Although the aim is to make RBAT as user-friendly and intuitive as possible, to ensure correct use and industry acceptance, it may be useful and necessary to develop a training course for how to perform the risk assessment process and use to software tool.
“Assess the assessment”	Administrations’ main use of RBAT will be to “Assess the assessment”. This requires that RBAT is transparent, e.g. that justifications behind risk identification and rankings can be understood. It also requires that RBAT maintains traceability, e.g. from risk to mitigating action.
Focus on process	For MASS risk assessments, the Administrations focus will be the *process*, just as much as the reports. This may include checking that quality is assured through the

Topic	Key take-aways
	involvement of the right competence, and that a recognized risk assessment method has been correctly applied.
Method description	A good RBAT method description is beneficial for both the user to perform the assessment as intended, but also as a basis for the assessor (e.g. Administrations) to ask questions about how the method has been applied. The method description should be supported by a clear set of definitions and figures/examples etc. to support the users.
Level of detail	Although somewhat intimidating at first glance, the level of detail in RBAT is considered necessary. For automation to be assessed, it must be done at a level of detail where allocation of functions between agents can be described. Furthermore, the lack of data and experience requires a more in-depth qualitative analysis, e.g. to provide justifications (e.g. behind rankings) and sufficient insights for risk informed decision making (manage uncertainty). Resource demands caused by the (relatively) high level of detail intended for RBAT can be compensated by: • providing an easy-to-understand method description, being smart about what can be prepared by the analyst as a desktop study (vs. a workshop), • developing smart software solutions when it comes to graphical user interfaces (GUI) and automated processes for performing calculations, compilations, summaries and exports, • reserving plenary sessions for brainstorming and scrutinize selected topics of interest, instead of systematically reviewing the entire assessment, and • making the RBAT software easily accessible for review/QA/verification by incorporating suitable features (“clickability”, filters, navigation etc.)
Expert judgement	The lack of statistical data (e.g. failure frequencies) and experience makes the use of expert judgement for risk ranking inevitable. RBAT should include or refer to a structured process suitable for such purposes.
ConOps	Concept of Operations (ConOps) reports are the main source of input to RBAT. The RBAT terminology and structure should therefore match the contents of a typical ConOps. Potential double-work should be avoided and instead the aim should be that RBAT can support ConOps writing.
Timing	Timing of RBAT is (per now) planned to be after a mature ConOps has been developed. This will prevent spending time in workshops etc. discussing and clarifying topics which could have been solved without being subjected to questions asked as part of a risk analysis. RBAT will work as an “litmus test” of the ConOps, and produce recommendations for updates to the ConOps, input to other documents (safety/maintenance philosophies, specifications etc.), as well as recommendations about need for more detailed assessments.

Topic	Key take-aways
	• A first version of RBAT will be “frozen” after the initial update • Applicant/user may use and update RBAT throughout the process • A final version of RBAT should be frozen, demonstrating that the risk is acceptable ○ Include descriptions of how risk has been reduced ○ Reference to mitigating actions, documentation etc.
Pre-defined categories	Providing pre-defined categories combined with clear definitions can be useful for guiding the analyst, particularly those which are not experienced and trained in risk analysis. This will also make RBAT easier and more efficient to use, as well as aid the analyst in ensuring that relevant design and operational aspects have been considered. It may also promote standardization, which in turn creates predictability, e.g. so that Administrations know what to look for and what is expected.
More than the sum of its parts	RBAT has the potential to produce results which are “more than the sum of its parts”. This is enabled by a combined top-down and bottom-up approach. The Mission Model and Function Tree are reductionistic in the sense that they are used to breakdown the items to be analysed (i.e. functions) in smaller parts. The results can then be used to evaluate effects across vessels, operations and functions. Examples include the workload induced on an operator by being required to supervise and possibly intervene operations for several vessels at the same time.
Risk model	The RBAT risk model must match the intended function level description in RBAT. Risk model is here understood as both the data collection and analysis table, as well as the logic model linked to an accident type model. This includes function failures pushing the system outside the boundaries of its normal operating envelope, detection of failures and recovery to a normal or acceptable (safe) operational state.

3 HAZARD IDENTIFICATION

A hazard identification (HAZID) was prepared, executed and reported to help achieve the objectives of other RBAT activities. As stated in the Tender Specification, the aim has been to identify all possible hazards at a generic level. Furthermore, the framework shall make it possible to link the functions identified in the RBAT function tree to the failure modes[2] identified in the HAZID. This, in turn, shall form a part of the basis for performing a risk analysis using RBAT.

Currently no specific MASS cases have been developed for testing the RBAT framework (this is planned for Part 2). Consequently, there was no context for performing the HAZID. Describing a context is the first part of performing risk assessments (ISO, 2009) and forms the basis for determining the presence of hazards and their effects in terms of accident causation, likelihood, and severity. In case of a missing or poorly defined context, risk ranking will therefore likely produce results with a high degree of uncertainty. Furthermore, risk ranking is also intended to be performed by the RBAT users on a case-by-case basis and should not be pre-defined by the developers. Pinpointing detailed risks associated with specific designs or operations is also not possible. Nevertheless, because the main objective of the HAZID is to produce a generic list of hazards, accidents and causes to be incorporated as part of the RBAT framework, this is not regarded as a limitation for the study.

A complete description of the HAZID approach and results is documented in Appendix C.

The HAZID was prepared by performing a review of industry guidelines, papers, and articles to identify a set of generic accident categories and hazards. A gap analysis revealed that EMSA's accident categories (EMSA, 2020b) were the most complete and was therefore chosen to be included as part of the framework. A list of hazards was developed following the FSA guideline's definition (IMO, 2018). This includes differentiating between hazards as a *potential source of harm* and failures in the functions implemented to prevent hazards from resulting in accidents. The list is complementary too and more exhaustive than the examples of hazards described in FSA guideline's Appendix 2. It is however intentionally described at a higher and more generic level. It also has a greater emphasis on hazards external of the ship. A final preparation effort consisted of converting the functions in the RBAT Function Tree into failure descriptions. These were then compared with descriptions of failures identified as part of the literature review. This revealed that the converted function failures provided a more complete set of potential direct causes, than what was captured as part of the literature review.

The HAZID was performed by first linking each of the generic hazards to relevant accident categories. The next step consisted of identifying which (function) failures could represent direct causes of an accident, in case of a hazard being present. Results were documented using a standard HAZID log sheet and formed the basis for a matrix linking the key functions in the RBAT Function Tree to EMSA's accident categories. This makes up part of the RBAT framework and the intention is to incorporate it as part of the final software as a feature to ensure that all accident contributions have been systematically considered as part of the process.

[2] Failure mode is here interpreted as a general term for the cause of an accident, and not the observed manner of a failure, which is a more common definition of the term (DNV GL, 2019).

4 RBAT APPROACH

4.1 Purpose

The main purpose of RBAT is to:

> *risk assess whether increased or new ways of using automation and remote operation is as safe or safer than conventional shipping*.

Furthermore, it is being developed to help the user meet the objectives a *preliminary risk analysis* (DNV GL, 2018, see also Figure 1). This implies that RBAT intended to first be applied during the concept development stages as a *screening approach*[3] (IMO, 2018). The purpose is to screen out the concept's less critical aspects, so that more resources can be devoted to those areas which deserve additional attention when further maturing the operational solutions and vessel or infrastructure's design. Such attention may be provided in form of identifying the needs for more detailed risk analysis or implementation of technical and operational risk control measures.

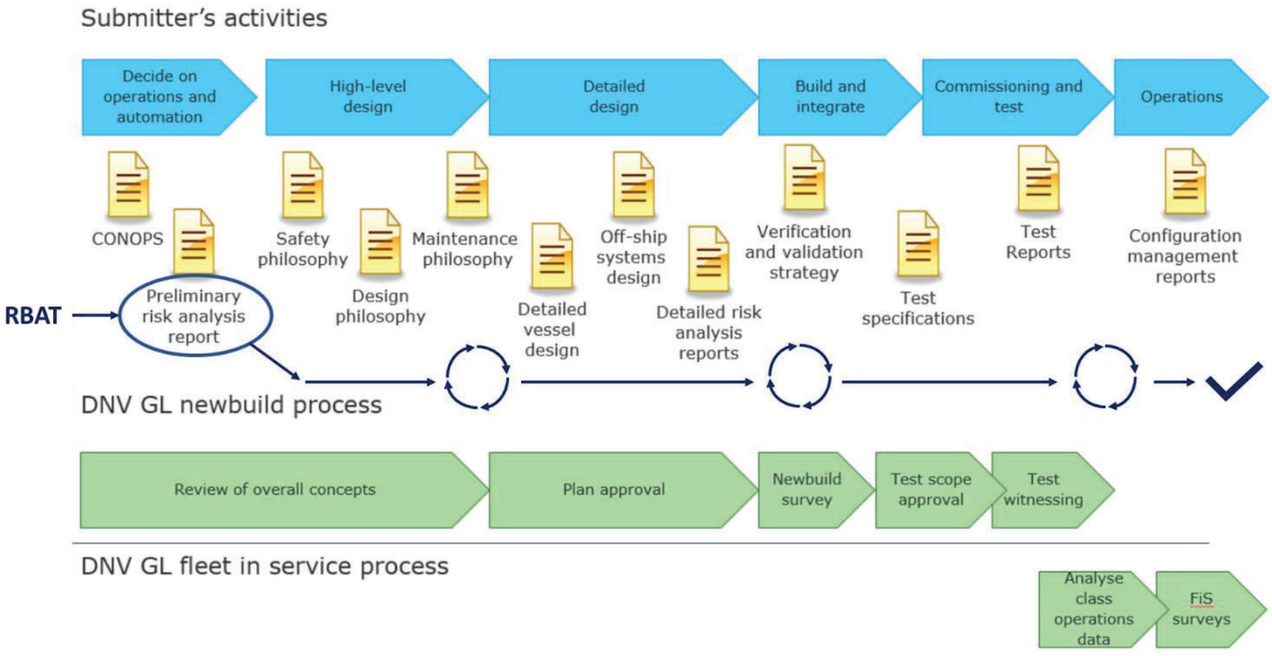


Figure 1 – Interactions between the submitter and DNV for concept qualification (DNV GL, 2018)

There is an expectation from class societies that risk assessments are performed (DNV GL, 2018; BV, 2019; ABS, 2020), and suggested functions to be addressed includes (but is not limited to):

- Navigation
- Manoeuvring
- Communication
- Integrated monitoring and control
- Cargo handling
- Passenger handling
- Ballasting
- Bilge and drainage
- Watertight integrity
- Electrical power
- Anchoring
- Mooring

[3] *Screening approach* as per in REF MSC-MEPC.2/Circ.12, para 3.1.2

4.2 Process

This sub-chapter describes how RBAT is intended to be used as part of the overall process for developing a MASS concept. A more detailed step-by-step instruction to the RBAT methodology can be found in chapter 6.

As indicated in sub-chapter 4.1, RBAT is intended to be performed in parallel with (or just after) having decided on the operational concept, use of automation, and a high-level vessel design (see Figure 1). This part of the concept development is normally documented in the *ConOps*, as promoted by several of the class societies guidelines. Although it is not a fixed rule, RBAT has been developed based on the assumption a ConOps will be the main source of input. Efforts have therefore been made to ensure that the RBAT framework matches, supports, and makes use of the contents expected to be found in a ConOps.

There is currently no standard ConOps template, however, the class society guidelines (LR, 2017; DNV GL, 2018; ABS, 2020) which promotes the use of such a document appears to be expecting similar things. Roughly speaking, a ConOps can be said to consist of three types of contents. One is the vessel's operational context, such as the operational area and environment, required infrastructure and logistics, applicable regulations, safety targets, and more. A second is the vessel and control centre's characteristics, including system capabilities and performance requirements, as well as manning and location of crew (including roles and responsibilities). The third and maybe the most key part of the ConOps is that devoted to explaining the vessel(s) mission and associated operations. This includes descriptions of the planned voyage phases, the various operational modes and envelopes, as well as the functions involved. As part of these descriptions, several of the class societies (LR, 2017; DNV GL, 2018; BV, 2019; ABS, 2020) expects to see an explanation of which functions shall be assigned to either automation or humans, and in what context (modes, situations). This is often the most detailed part of the ConOps, and although the process is iterative, this is the part which is commonly matured the latest.

Most of the ConOps is relevant for RBAT, as it makes up a significant part of the risk assessment's *context* (ISO, 2009). The part describing the mission, operations and functions is however considered a source of direct input, as these parts are included as *nodes* and items being subjected to risk analysis. RBAT provides tools which can be helpful in developing this part of the ConOps. Part 1 of the RBAT project (DNV GL, 2020c) developed a *Mission Model* which includes generic descriptions of vessel mission phases and operations, and a *Function Tree* which includes generic descriptions of vessel key functions and sub-functions. Both the Mission Model and Function Tree are supported by a complete set of coherent definitions. The purpose of these tools is to assist the RBAT user with a structured approach to defining and detailing the risk assessment scope – i.e. the functions to be automated and/or included as part of remote control. This makes up the first part of the RBAT methodology, which is to define what is referred to as *Use of Automation* (UoA, see sub-chapter 6.1 for more details). As indicated in Figure 2, it is therefore recommended to start preparing parts of the input to RBAT already as part of writing the ConOps. Not only will this provide confidence that the ConOps takes all aspects of the vessel mission and functionality into account, it also avoids the risk of having to redo work in case there is a significant mismatch between the ConOps and RBAT terminology or structure.

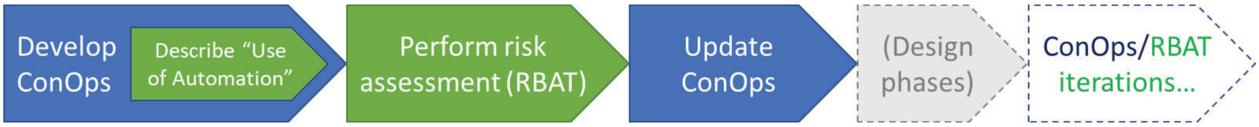

Develop ConOps
Describe "Use of Automation"
Perform risk assessment (RBAT)
Update ConOps
(Design phases)
ConOps/RBAT iterations...

Figure 2 – Relationship between ConOps and RBAT during the initial project stages

Because RBAT may trigger many ideas about how to improve or further specify the operational concept and vessel design, it may become tempting to do so during the risk assessment process. To maintain traceability of exactly what was risk assessed, it is therefore important that the ConOps is sufficiently matured and "frozen" before continuing with Part 2 to 5 of RBAT, which is the actual risk assessment. Instead of being tempted to make changes to the ConOps during the risk assessment, recommended actions should be noted down. When the risk assessment is finalized, the ConOps can be updated and used as input for further design purposes. Output from RBAT may result in changes to different parts of the ConOps; typical risk control measures including addition or removal of operations or functions, redefined minimum risk conditions (MRC), and addition of operational constraints, e.g. with regards to sea and visibility conditions.

Both the ConOps and the risk assessment should be updated at suitable milestones, e.g. when all recommendations about improvements in design have been implemented. The updates should document which actions were brought forward and to what extent they have contributed to changes in the assessed risk level. Iterations should be done until all risks have been managed as planned. A final iteration should be done after commissioning and testing. All required risk control measures should be identified, planned, executed and tracked to completion with clear traceability.

5 RBAT RISK MODEL

This chapter introduces a risk model specifically developed to accommodate the objective of RBAT, namely to risk assess whether increased or new ways of using automation and remote operation is as safe or safer than conventional shipping. Please note that purpose is here to explain the model's overall structure and main principles. The practical application of the risk model is described in chapter 6 which contains a detailed step-by-step guidance about the RBAT methodology.

Both the model and its associated risk assessment method builds on DNV's guideline for autoremote vessels (DNV GL, 2018) as well as experiences from previous work, particularly the SAFEMASS project (DNV GL, 2020a, 2020b). It is also inspired by the Functional Hazard Analysis (FHA) methodology used as part of the safety assessment process for commercial aircrafts (SAE, 1996; 2010), as well as recent methodological development in risk analysis (Ramos, et al., 2019; 2020).

To better understand the proposed risk model's underlying structure, it is useful to first revisit some of the RBAT framework's key definitions presented in the project's first report (DNV GL, 2020c). *Automation* can be defined as "the execution by a '*machine' agent* (usually a computer) of a function that was previously carried out by a human" (Parasuraman & Riley, 1997, p. 231). A key aspect of this definition is that automation is understood in terms of *functions*. This is the main reason why RBAT is a functional approach, i.e. functions are the items being subject to analysis. A function can be described as a specific purpose or objective [i.e. goal] to be accomplished, that can be specified or described without reference to the physical means of achieving it (IEC, 2020). In other words, automation is about achieving the same *goal* (as before automation was introduced), but by having a machine agent executing the function instead of a human. This transition of responsibility is commonly referred to as function (re-)allocation or assignment (IEC, 2000; ISO, 2000). Moving the control of functions from human or machine agents onboard a vessel over to a remote location can also be considered type function re-allocation, regardless of whether automation is introduced.

A key consideration is that automation of functions does not necessarily imply that humans are left with no responsibilities. Instead humans are often delegated with the responsibility for performing parts of a function which could not (easily) be automated, or to supervise the execution of (now) automated functions. Supervision often implies that the human is responsible for the *outcome* of a function and is therefore expected to intervene in case something goes wrong.

Based on the abovementioned explanation of automation, functions, and supervision, the RBAT risk model should provide a structure for addressing the following questions about MASS related risks:

- How can functions impacted or introduced by automation fail, and if they fail, what are the immediate effects?
- How can failures be successfully detected and responded to by the agent responsible for supervising the function?
- In case the failure cannot be recovered, what are the consequences from worst-case outcomes?

5.1 Accident model

Figure 3 illustrates an accident model which captures the abovementioned aspects and can be used as basis for the risk model. The grey lane with dotted boundaries represents the safe operating envelope of a system (e.g. MASS). As long as operations are performed within the (known) criteria which define the envelope boundaries, the system is considered to be in a safe and acceptable state.

Events, such as failure to perform functions as required, can push the system outside of the operating envelope, and put it in abnormal and potentially unsafe state. If the failures are successfully detected and responded to, the system can recover a safe state and re-enter the (safe) operating envelope. It is important to note that the term *recovery* is meant to cover a wide range of responses. The most optimal recovery is returning to a normal (pre-failure) operational state by fully regaining function. This is indicated by the first recovery path in Figure 3, which re-enters into the middle of the operating envelope. A second, but less optimal recovery, is to enter an operational state with a reduced, but acceptable, safety margin. These are recoveries where fully restoring a function is not possible, but operations can be (temporarily) continued in case the correct compensating measures are implemented. This is indicated by the second and third recovery path in Figure 3, where operations are continued closer to the envelope boundary.

So-called *minimum risk conditions* (MRCs) may be part of recoveries. These are pre-defined, as-safe-as-possible states that the ship should enter when the system experiences situations that are outside those in which it can operate normally but is still expected to deal with in one way or another. In Figure 3 the MRCs are illustrated as light blue boxes framed by dotted lines, indicating that they can be considered as acceptable operating envelopes by themselves, but only for a temporary phase until the vessel has transitioned back to a normal operational state. The concept of MRCs is well described in other publications (DNV GL, 2018) and providing a detailed explanation is therefore considered to be out of scope for this report. If a recovery fails, the abnormal situation can potentially escalate and ultimately result in an accident, unless subsequent attempts at other recovery actions are successful. As indicated in the figure, a system may enter a sequence of worsening unsafe states before an accident occurs. This will depend on the severity of the initial event, how well defended the system is, and to what degree the recoveries are successful.

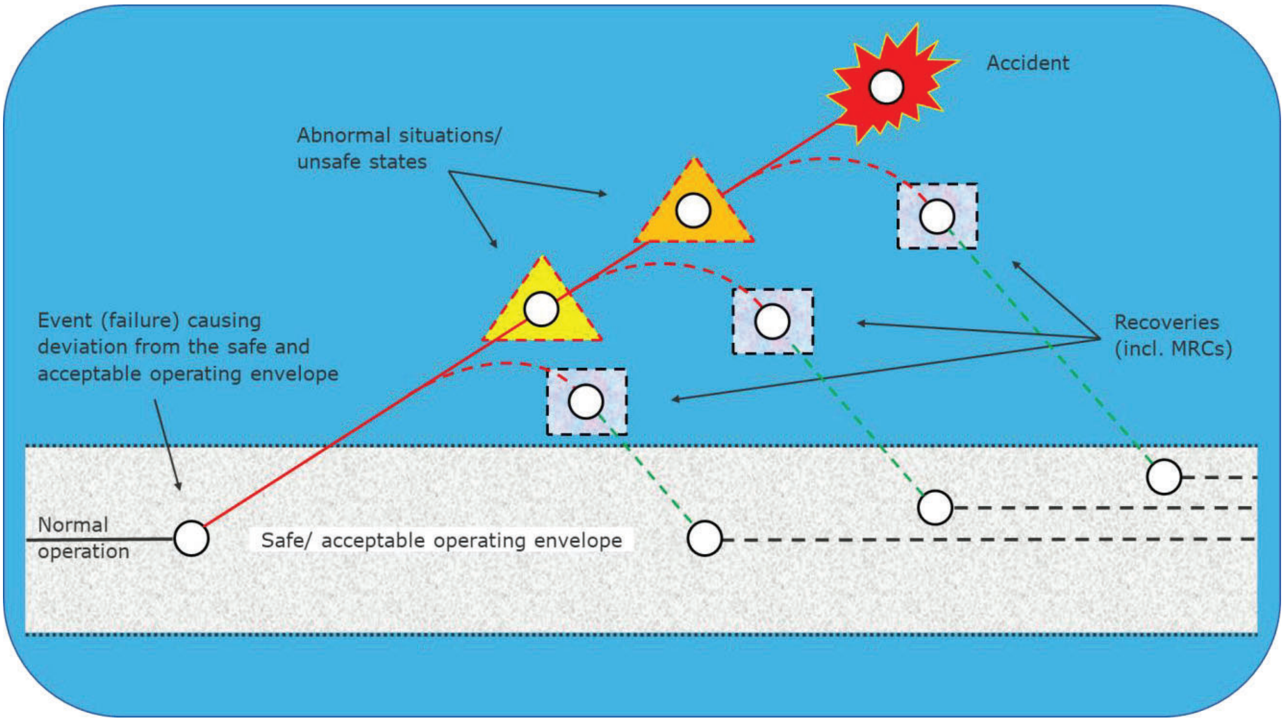

Accident
Abnormal situations/ unsafe states
Event (failure) causing deviation from the safe and acceptable operating envelope
Recoveries (incl. MRCs)
Normal operation
Safe/ acceptable operating envelope

Figure 3 – Accident model (adapted from Wang, 2007)

5.2 Event sequence diagram

Event sequence diagrams are powerful tools for modelling scenarios similar to those illustrated by Figure 3 (Wang, 2007). Such models have recently been proposed by others as a method suitable for risk assessments of MASS concepts (e.g. Ramos, 2019; 2020). They depict scenarios as starting with an initiating event followed by one or several pivotal events which, depending on their outcome, result in different end states. It was therefore decided to develop the RBAT risk model as a generic event sequence diagram, based on the accident model illustrated in Figure 3. The model is presented in Figure 4 and consist of three main parts, each including a set of sub-events. Please note that a detailed description of each part can be found in chapter 6 about the RBAT methodology, and that the following section is limited to provide an overview of the model.

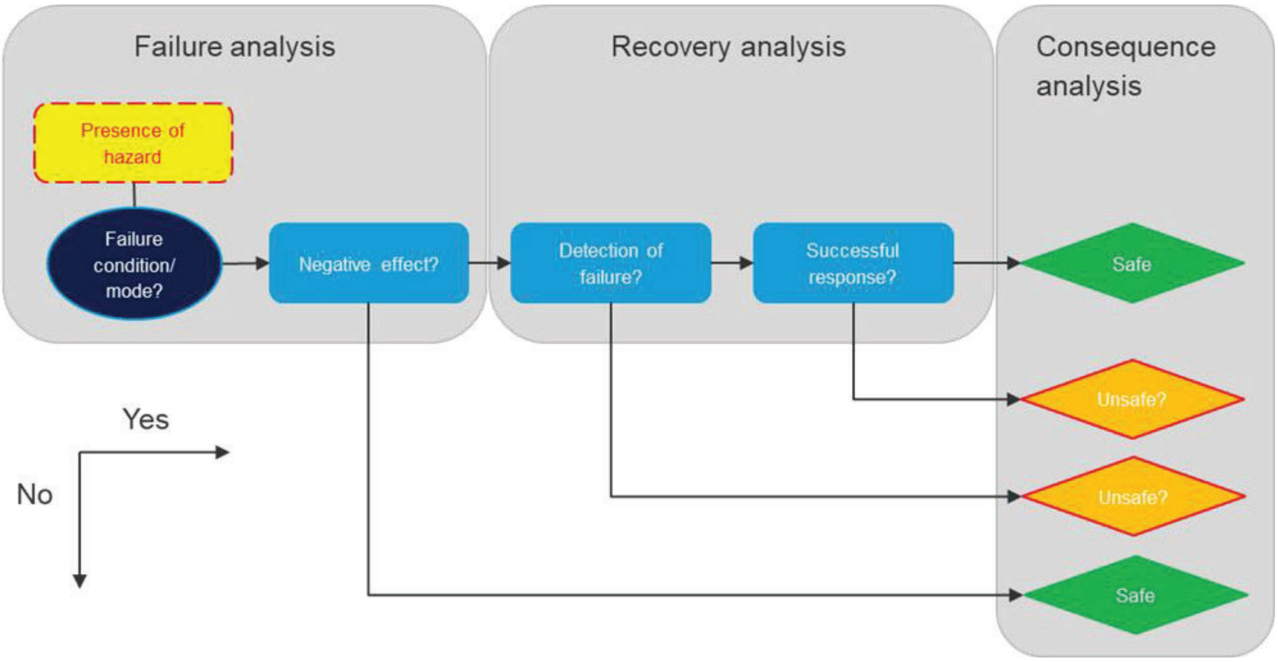


Figure 4 – RBAT event sequence diagram

The *failure analysis* consists of identifying failure conditions/modes which can have a negative effect on the system, by pushing it towards or outside the boundaries of the operating envelope, and into an abnormal situation and unsafe state. This can include failures occurring within the system (i.e. internally), or failures manifested by the system having insufficient capabilities compared to the external environment. Identification of failures and their effects must consider the presence of potential *hazards*. For example, failures in a collision avoidance system may not be as critical when sailing in open waters, as when sailing in traffic dense areas. The *recovery analysis* considers to what degree such failures can be detected (by the supervising agent) and, if so, whether they can be successfully responded to in a manner which restores the operating envelope, or maintains an acceptable safety level until the abnormal situation has been resolved. The *consequence analysis* examines what the worst-case outcomes are in case recovery fails. This can be unsafe states caused by reduced safety margins, or accidents with impact on safety.

The model serves three main purposes. One is to provide a structure for the data collection and analyses table intended to be used as part of applying RBAT. The table is presented in chapter 6 and includes columns for capturing data about each of the event in the model. The second is to form a logic structure for the quantification of risk levels. As per now, the risk associated with a function failure can be described as:

*Frequency of failure condition/mode * Probability of recovery failure * Severity of worst-case outcome*

Units of measure and scales for the various risk metrics have been proposed, and can be found in sub-chapters 6.2.2, 0 and 6.4.2. These should however be considered as preliminary and need to be carefully tested as part of Part 2 of the RBAT project, when applying the method to actual cases. Also, criteria for what is considered acceptable risk will also be developed as part of Part 2.

With respect to both abovementioned purposes, several event sequence diagrams can be linked together, forming a sequence of events. This can be relevant in cases where the outcome (consequence) of a failure condition/ mode does not involve direct losses or impacts (accidents), but instead causes the vessels safety margin to be reduced. Such outcomes can be included as additional scenarios for which event sequence diagrams are developed. This is illustrated in Appendix D.

The third purpose is to support informed decision-making about implementation of risk control measures. For example, the frequency of failures can be reduced through improved product design, inspection, testing and maintenance of components, redundancy in systems and more. In case of low probability for successful recovery risk control measures may consist of using active supervision (instead of passive), enhancing automation design so that supervision complexity is reduced and more time is made available to make decisions, as well as improving human-machine interfaces and alarm systems to create better situational awareness. Lastly, consequence reducing measures can be implemented, in case reducing failure frequency and improving probability for successful recovery does not provide the desired risk reduction.

5.3 Limitations and assumptions

RBAT is specifically developed to assess risks associated with introduction of increased automation and remote control (unmanned/ reduced manning operations). This means that risks related to hazards which are unaffected by such factors, and which are comparable to conventional concepts, are not included as part of the assessment. It is assumed that these risks are managed through standard practices. In praxis, this means that functions which are not carried out by either a machine or human agent will not be included in the assessment. Examples are functions which can be considered purely structural or mechanical. Measures required to maintain the integrity of such functions may however be affected by automation and remote control. For unmanned vessels alternative solutions may have to be developed for traditional maintenance and inspection tasks performed by the crew onboard, such as remote condition monitoring and adapting maintenance intervals according to port stays and the availability of onshore personnel.

RBAT is a *functional* assessment, i.e. functions[4] are the items being subject to analysis. The focus is to identify if and how failures of various functions can result in undesirable outcomes, e.g. accidents. This implies that if a function has not been identified and included as part of the assessment, risks associated with such a function will also not be analysed. It is therefore assumed that the hazards which justifies the need for different functions have been identified as part of previous work performed to describe the vessel's functionality, for example early in the ConOps development. This limitation can be exemplified as follows; if a vessel is carrying flammable cargo (hazard), this may require certain fire protection (function) equipment to be installed. Currently RBAT is set up to identify risks associated with how the cargo can ignite and how fire protection can fail, but not necessarily to identify flammable cargo as a hazard by itself. It is however expected that systematic use of the RBAT mission model and function tree (see sub-chapter 6.1) will to a large extent compensate this limitation of the functional approach. These models are based on a thorough review of known ship functionalities, many which exist with the purpose of controlling hazards a vessel is exposed to. A HAZID (see Appendix C) performed as part of creating the RBAT framework has provided a generic hazard register which links various hazards and accidents to the *key functions* identified when developing the function tree during Part 1 of the project. This can be reviewed as part of developing the ConOps, to ensure that functions required to control hazards present in the various mission phases have been considered and implemented. In any case, it is assumed that the more external hazards, i.e. those for which vessel functionality is required to control, have been identified prior to using RBAT.

[4] In RBAT, the functions are included in the analysis as *control actions* which are sub-functions executed by a machine or human agent to perform a parent function referred to as a *control function*. See also the report's list of definitions.

RBAT is a top-down (reductionistic) method in the sense that high level functions are broken down into the sub-functions which are included as part of the assessment. It takes however a bottom-up approach when it comes to assessing causation. As a starting point, the analysis explores whether failures of individual functions can produce worst-case outcomes which are beyond what is considered to be acceptable risks. This way the assessment follows a principle similar to what is often referred to as a *single failure criterion* (e.g. ENCO, 2015), i.e. that no single failure should cause unacceptable consequences. This is a common feature for several well-established risk analysis techniques (e.g. FMECA) and in particular those used as screening tools, where the aim is to identify critical hazards which should be targeted using more detailed risk analysis, or which require extra attention in terms of risk reduction. RBAT is not set up to *deductively* explore how various causal factors together can result in a hazardous event, such as for example fault tree analysis. This is not considered necessary when it comes to meeting the needs of a preliminary risk analysis technique. It is however recognized that the (safety) assurance of highly complex and safety critical systems, such as MASS, is better achieved by taking the risk assessment one step beyond the single failure criterion principle. RBAT therefore incorporates a method for ranking the severity of failures in terms of how many additional failures must occur for an accident to take place. A more detailed explanation is provided in sub-chapter 6.4.2.

Finally, it is important to keep in mind that RBAT is a *preliminary* risk analysis developed with the intention of screening critical hazards introduced by automation. It is limited to analyse functions at the level where allocation of responsibilities between human and machine agents can be distinguished. It is not intended to replace more detailed risk assessment techniques, such as FMECA and fault tree analysis.

6 STEP-BY-STEP GUIDEANCE TO THE RBAT METHODOLOGY

The current RBAT methodology consists of five main parts:

1. Defining the Use of Automation (UoA), and
2. Performing a failure analysis
3. Performing a recovery analysis
4. Performing a consequence analysis
5. Addressing risk control

The following sub-chapters presents these four main parts as consisting of 14 steps.

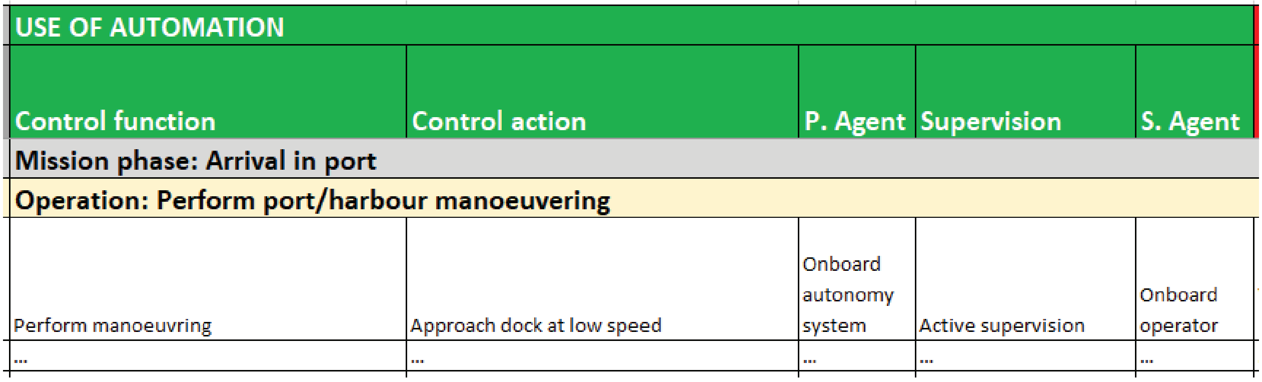
6.1 Part 1: Define Use of Automation (UoA)

The purpose of defining UoA is to describe:

- Which functions are affected by automation or remote control,
- How these functions are allocated to different *agents* (human or technology),
- Where the different agents are located (locally on vessel/site or remote),
- How the affected functions are supervised, and by which agents.

Defining the UoA 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.

As explained in sub-chapter 4.2, the UoA's context is much defined by the contents of a typical ConOps.



USE OF AUTOMATION				
Control function	**Control action**	**P. Agent**	**Supervision**	**S. Agent**
Mission phase: Arrival in port				
Operation: Perform port/harbour manoeuvering				
Perform manoeuvring	Approach dock at low speed	Onboard autonomy system	Active supervision	Onboard operator
…	…	…	…	…

Figure 5 – 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. Here the term mission refers to a set of mission phases, operations and functions performed to achieve the intended purpose of why the vessel is designed and operated.

Three levels of operational goals are used to describe the mission:

- 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. An (simplified) example is "Safe and timely transport of cargo from one Port X to Port Y".

- The mission phases, i.e. 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. An example is “Arrival in port”
- The operations, i.e. 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. An example is “Perform docking”.

Describing a mission as consisting of these three levels forms 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 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.

The generic RBAT mission model can be used as a starting point. Re-phrase and/or add descriptions if needed. Emergency responses, including relevant Minimum Risk Conditions (MRCs) should be included as separate Operations.

Figure 5 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 system) agents involved in performing the control function

Control functions and actions make up the functional goals of the hierarchical goal structure:

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 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 are required to achieve a successful outcome. Then, for each relevant key function, drill/ branch down the tree branches to a sub-function level which matches the concept's current maturity. 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. The lowest level makes up the control actions, and the parent level makes up the control functions.

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

When identifying and describing functions it is important to not only include functions which exert 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.

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

It is helpful if the ConOps includes, or is updated to include, functional block diagrams (Figure 6) illustrating the relationships and dependencies between the affected control actions (both internal and external).

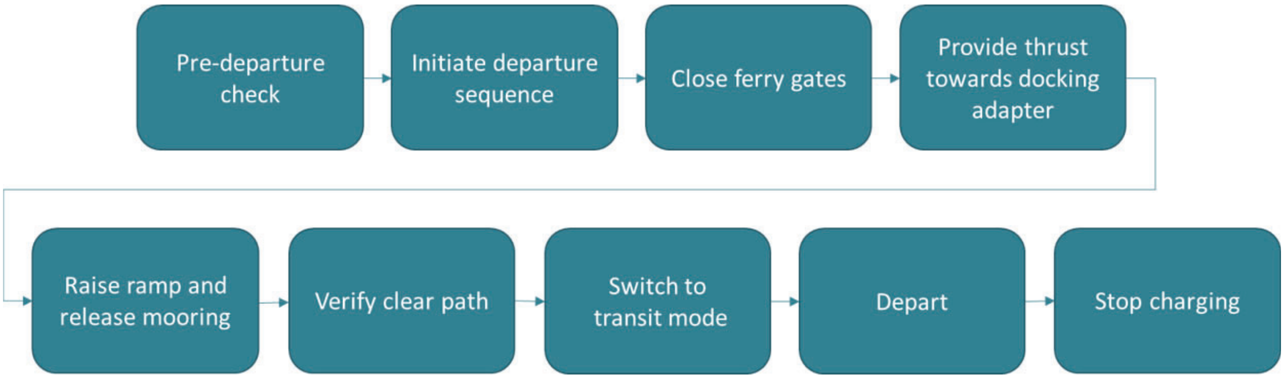

Pre-departure check
Initiate departure sequence
Close ferry gates
Provide thrust towards docking adapter
Raise ramp and release mooring
Verify clear path
Switch to transit mode
Depart
Stop charging

Figure 6 – 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 both a computerized system and a human operator. Only one agent shall be listed as responsible for performing a control action. However, depending on which level of detail control actions are described, cases may come up where more than one agent is involved. In principle, 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.

The geographical location of the agent shall also be indicated by using nomenclature pre-fixes, such as "R" for Remote and "O" for onboard (vessel). Alternatively, if "Remote" can refer to several different places, the actual location of the agent can be described.

Figure 5 shows how the control action "approach dock at low speed" is allocated to the performing agent "Onboard autonomy system".

6.1.4 Step 4: Assign responsibility for supervision of control actions

The fourth step of the process is to indicate if and how control actions are supervised, and by which agent. *Supervision* is 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. Examples of abnormalities can be system failures and malfunction, or external conditions which exceed pre-defined criteria for what are considered operational limits (e.g. weather conditions). The designated agent is the same responsible for ensuring recovery, as described in sub-chapter 6.3 (Steps 8-10). 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.

Supervision can be performed by either a machine 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 are performed manually. A machine agent will perform all actions. As such, it is the agent responsible for making decisions and performs the intervention which defines who or what is to be considered supervisor.

Three different categories of supervision are defined in RBAT:

- *Active supervision*: An agent is responsible for continuously[5] monitoring the performance of a control action with the purpose of being able to successfully intervene at any stage.
- *Passive supervision*: An agent is responsible for being available to monitor the performance and successfully intervene on demand according to pre-defined parameters (e.g. an alarm).
- *No supervision*: No agent is responsible for monitoring the performance of a control action.

It is important to emphasize that the supervision 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 supervision categories should therefore be based on the overall philosophy about monitoring and control described in the ConOps, which should also include a more detailed description of the supervision roles. Such descriptions should consider the influence from factors such as fleet size, manning level, competencies, human-machine interfaces (e.g. visual display units) when assigning supervision responsibilities to human agents. A preliminary solution for supervision should therefore be decided upon and described before commencing with the function failure and recovery analysis (Step 5).

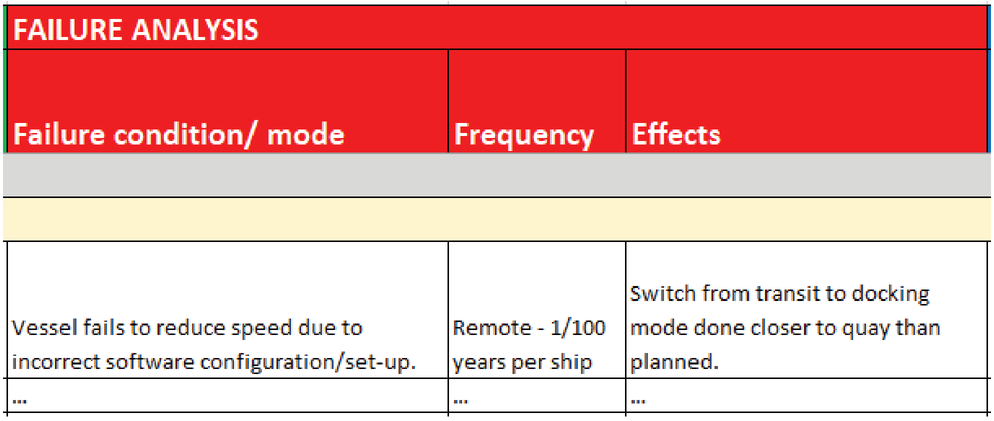
Figure 5 shows how the “Onboard operator” is responsible for actively supervising the control action “approach dock at low speed”.

6.2 Part 2: Perform failure analysis

The purpose of the failure analysis is to:

- Identify how the functions affected by automation and/or remote control can fail (Step 5)
- Indicate how often such failures are expected to occur (Step 6)
- Assess the effects from such failures in terms of the vessel’s safety margin (Step 7)

[5] ‘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.



FAILURE ANALYSIS		
Failure condition/ mode	Frequency	Effects
Vessel fails to reduce speed due to incorrect software configuration/set-up.	Remote - 1/100 years per ship	Switch from transit to docking mode done closer to quay than planned.
...	...	...

Figure 7 – Failure analysis module in RBAT

6.2.1 Step 5: Identify and describe failure conditions/ modes

The fifth step of the process is to identify and describe in what ways the various functions identified in Step 2 can fail or become degraded. In RBAT *failures* are assessed at the control action level and can be described either in terms of failure conditions and failure modes, or a combination of both. These can be internal failures in the vessel's or RCC's systems (e.g. a malfunctioning sensor), or they could result from degraded conditions 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 failure conditions representing insufficient capabilities.

Failures manifest themselves as events which occurs when functions cannot achieve their intended outcome, e.g. they fail to perform according to pre-defined requirements. As such the identified failures should address the availability (i.e. continuity) and integrity (i.e. correctness) of functions. The failure condition/mode descriptions can be user-defined at will; however, consistent use of terms and expressions will help with the RBAT compilation and review. This task can be assisted by using the guidewords provided in Table 3 as cues.

It is encouraged to explore and identified potential *undetected and unannunciated* failures.

RBAT currently does not include a separate column dedicated to describing the failure causes (often also called "failure mechanisms"). However, if the design is mature enough for causes to be specified in terms of system architecture, they can be included in the failure condition/mode description, e.g. "Partial loss of object detection due to sensors being obstructed (e.g. fog, snow)". This may also be helpful in determining the failure frequency occurrence (see Step 6).

Table 3 – Failure condition/mode guidewords

Failure conditions/modes	Alternative modes/ sub-modes
Loss of function	Needed but missing
Partial loss of function	--
Function is insufficient/incapable	--
Function provided when not required	Providing leads to hazardous event
Function provided incorrectly /malfunction	Too high/low
	Too early/late or in wrong of order
	Too short/long
	Not followed

All credible and relevant failure conditions/modes should be considered. It is important that the failure conditions/modes address failures of the control actions (and function) selected for analysis. Attempts should be made to identify the possibility of having undetected failures.

The level of detail is to some extent dictated by how the control actions are described. However, if there is a need to scrutinize a failure condition/mode further, e.g. to reduce uncertainty and/or demonstrate more specific risk contributions, the assessment can be done at lower level. Assuming that object detection is performed by redundant System A and System B, the following example can be made:

1) Loss object detection (loss of function)

i. Loss of object detection System A (partial loss of function)

ii. Loss of object detection System B (partial loss of function)

Figure 7 shows an example of a failure condition/mode description in RBAT.

6.2.2 Step 6: Assign a frequency for the failure condition/ mode occurrence

The sixth step of the process is to assign a frequency for how often a failure condition/ mode is expected to occur. Note that the frequency only reflects the occurrence of the failure condition/ mode, and not potential worst-case outcomes (see Step 11). The probability of worst-case *outcomes* also incorporates the probability that detection and response is successful (Steps 8-10).

Frequency	Per ship
Frequent	1/month per ship
Somewhat probable	1/year per ship
Probable	1/10 years per ship
Remote	1/100 years per ship
Extremely remote	1/1000 years per ship

For failure conditions/ modes known to the industry, and for which there is statistical data available concerning failure rates, this should be applied if possible. However, because many of the failure conditions/ modes will involve new technologies or novel use, it is expected that elicitation of experts' judgement will have to be utilized in the absence of historical and empirical data.

6.2.3 Step 7: Determine the effects from failure conditions/ modes

The seventh step of the process is to determine the direct effects from the failure conditions or modes. In RBAT the focus is on describing how effects from failures manifests themselves in terms of the vessel's *safety*. The effects should describe the immediate outcomes following the (single) failure condition/ mode under consideration *before* any attempts to recover or mitigate the failure (Steps 8-10) is expected to take place.

This may include:

- Degradations in vessel or system performance (reduced safety margin), i.e. events which may require recovery to maintain an acceptable level of safety
- Events which makes recovery difficult, e.g. negative effects on other control functions and actions (incl. equipment failure), or other escalating factors

Failure effects shall not include descriptions of:

- Detection and recovery (incl. MRCs). This is covered as part of the recovery analysis (Steps 8 to 10).
- What happens if recovery fails or is not available. This is done later as part of assessing the worst-case outcomes (Steps 11 and 12).

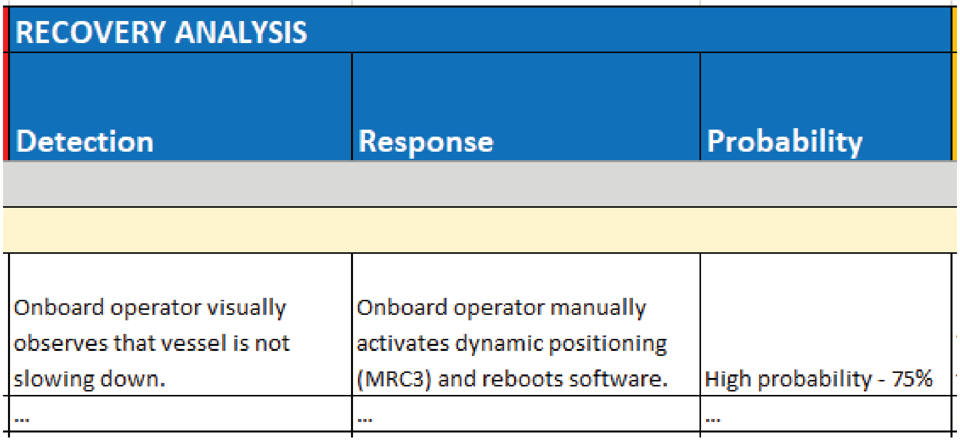
Figure 7 shows an example of a failure effect description in RBAT.

6.3 Part 3: Perform recovery analysis

The purpose of the recovery analysis is to:

- Assess how failure conditions/ modes can be detected (Step 8)
- Assess how failure conditions/ modes are responded to (Step 9)
- Estimate the probability of recovery being successful (Step 10)

Here the term *recovery* refers to being able to detect and consequently regain control in such a manner that it prevents a failure from causing adverse outcomes in terms of safety (i.e. consequences). The split of recovery into two elements (detection and response) is done intentionally so that the RBAT user is encouraged to systematically consider both aspects. This is because both may rely on (and require) different technologies and operational measures.



RECOVERY ANALYSIS		
Detection	Response	Probability
Onboard operator visually observes that vessel is not slowing down.	Onboard operator manually activates dynamic positioning (MRC3) and reboots software.	High probability - 75%
...	...	...

Figure 8 – Recovery analysis module in RBAT

6.3.1 Step 8: Assess how failure conditions/ modes can be detected

The eighth step of the process is to describe how failure conditions/ modes are detected by the *supervising agent*. As explained in Step 4, the supervising agent can both be a computerized system or a human operator. The description can include ways of detection both in terms of becoming aware of the failure *itself*, e.g. via sensors readings or messages about malfunctions (i.e. human-machine interfaces), and/ or the associated *physical effects* which can be observed, such as unexpected changes in vessel performance.

Figure 8 shows an example of how detection can be described in RBAT.

6.3.2 Step 9: Assess how failure conditions/ modes shall be responded to

The ninth step of the process is to assess which responses are available to regain control in case failure conditions/ modes are considered hazardous. A response may be carried out by the supervising agent or other (e.g. external) agents. However, it should always be initiated by the supervising agent, following successful detection. In this context recoveries can comprise of different types of measures:

- Returning to a normal pre-failure operating state by regaining function
- Entering an acceptable[6] new operating state by implementing compensating measures
- Entering a minimum risk condition which reduces the likelihood of further escalation

The recovery may include a mix of the abovementioned measures. E.g. the vessel may immediately enter and remain in an MRC until a failure has been corrected and normal operations can be resumed.

Figure 8 shows an example of how a response can be described in RBAT.

6.3.3 Step 10: Assign a probability for recovery being successful

The tenth step of the process is to estimate the probability of (detection and) recovery being successful. This is done by assigning a probability using the detection and recovery index provided in Table 4[7]. More detailed definitions of can be found in Appendix F.

Because a successful recovery depends on successful detection, assignment of probabilities should follow a “weakest link” principle, i.e. a recovery is never more probable than its detection. Furthermore, the assignment of probabilities should consider any negative effects the failure may have on recovery.

Figure 8 shows an example of how the probability for successful recovery can be described in RBAT.

[6] Acceptable in terms of being allowed, by pre-defined criteria, to continue operations.

[7] Please note that the probability index is preliminary and may be subject to updates during Part 2 of RBAT.

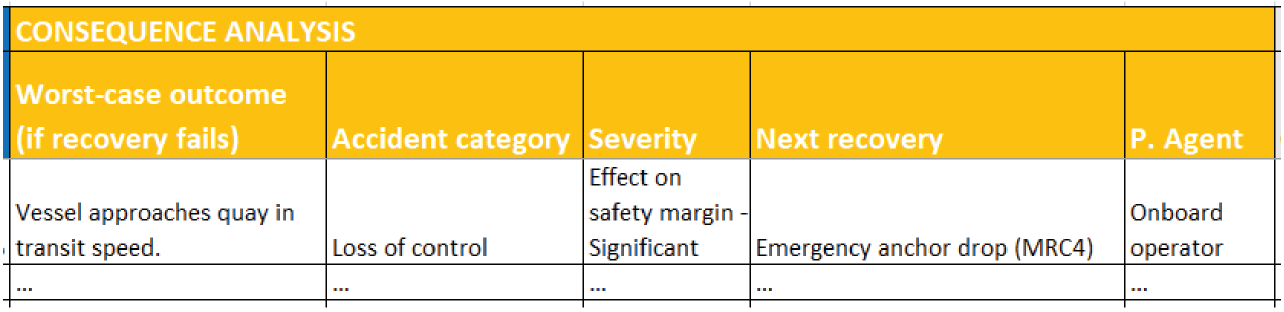
Table 4 – Probability index for successful detection and response

Probability	Success	Human agent	Machine agent
Very high probability	99%	Successful detection and response are expected.	
High probability	75%	Successful detection and response should be expected.	
Moderate probability	50%	Successful detection relies on extraordinary operator vigilance. Successful response relies on above average operator performance.	Detection and response systems are available and functional, but performance capabilities are marginally below required limits.
Low probability	25%	Successful detection and response only happen by chance (random, coincidence).	Detection and response systems are degraded, and/or performance capabilities significantly below required limits.
Very low probability	1%	Successful detection and response cannot be expected.	Detection and response systems are severely impaired or unavailable/ not implemented.

6.4 Part 4: Perform consequence analysis

The purpose of the consequence analysis is to:

- describe what the worst-case outcomes of an *unrecovered* failure
- assess the outcome's severity, and
- identify what the next recovery is (if any) who or what the performing agent is



CONSEQUENCE ANALYSIS				
Worst-case outcome (if recovery fails)	Accident category	Severity	Next recovery	P. Agent
Vessel approaches quay in transit speed.	Loss of control	Effect on safety margin - Significant	Emergency anchor drop (MRC4)	Onboard operator
…	…	…	…	…

Figure 9 – Consequence analysis module in RBAT

6.4.1 Step 11: Describe the worst-case outcome

The eleventh step of the process is to describe the *worst-case outcome* in case a failure condition/mode occurs and fails to be recovered by the initial response (i.e. first "layer of defense"). Worst-case outcomes therefore differ from the failure *effects*, which are the immediate outcomes from the failure condition/ mode which may require (and trigger) a recovery. Worst-case outcomes are the answer to the following question:

What happens in case the failure condition/mode occurs and initial attempts at recovery fails?

If additional/other layers of defense are available, the worst-case outcome shall be described as the situation the vessel is in *after* the initial response has failed, and *before* any other responses can expected.

Worst-case outcomes are described in terms of either:

- degraded system performance
- accidents (if relevant)

Remaining recovery opportunities shall not be described as worst-case outcomes. These (if any) are described as part of Step 13. Instead, worst-case outcomes are the events or conditions which trigger the need for other recovery actions.

The degree of losses (i.e. consequences) also does not have to be described - this is indicated by the severity ranking performed as part Step 12.

A separate “Accident category” column is dedicated for identifying which accidents the failures may contribute to, such as collision, grounding and flooding. This is populated using EMSA’s accident categories (see Table 7 in Appendix C). To keep track of which (function) failures contribute to which accidents, this column shall be used even if the failure only causes degraded system performance, and not directly and accident. For incidents involving degraded system performance, the *Loss of control* category shall be used.

Figure 9 shows an example of a worst-case outcome and accident category described in RBAT.

6.4.2 Step 12: Rank the worst-case outcome severity

The eleventh step of the process is to rank the worst outcome severity. This is done by assigning a degree of severity using the index in Table 5.

If the worst-case outcome is an accident severity is ranked according to the *effects on human safety*. If the outcome manifest itself as degraded system performance, the *effects on safety margin* are determined.

The effects on human safety index, including the equivalent fatalities, is adopted from the FSA guideline (IMO, 2018). The “Negligible” level has been added by the authors of this report as an option to be used for failure conditions/modes with no or insignificant consequences in terms of safety.

The effects on safety margin has been developed for RBAT to capture the criticality of failure conditions/modes which alone does not have an immediate effect on human safety (i.e. an accident), but together with one or several other failures may cause injuries or fatalities. This feature is included to enable screening out the less important failures and make it easier to examine how combinations of the most critical failures can result in accidents.

Figure 9 shows an example of a worst-case outcome ranking in RBAT.

Table 5 – Severity index for worst-case outcomes

Severity	Effects on human safety	Equivalent fatalities	Effects on safety margin
Negligible	No injuries, only inconvenience/ discomfort (if any)	0,001	Multiple other failures must occur to cause an accident*
Minor	Single injury or multiple minor injures	0,01	Two additional failures must occur to cause an accident*
Significant	Single serious or multiple injuries	0,1	One additional failure must occur to cause an accident*
Severe	Single fatality or multiple serious injuries	1	Failure alone can cause an accident*
Catastrophic	Multiple fatalities	10	Failure alone can cause an accident with significant escalation potential**

* Refers to events with a severity rating of "severe" or worse. **Refers to events with a severity rating of "catastrophic".

6.4.3 Step 13: Identify the next recovery

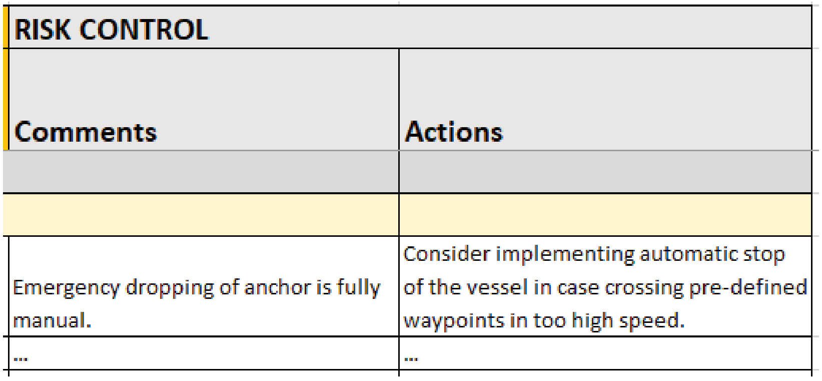
The thirteenth step of the process if to identify any next recovery (if any) required in case the first line of recovery fails. This can be additional MRCs or other safeguards planned to be used in case the worst-case outcomes should occur. When finished analysing the mission's normal operations these recoveries shall be included as control functions and control actions under a mission phase devoted for capturing abnormal operations and emergencies. Because the recoveries will be decomposed and analysed separately, they only have to be mentioned in brief as part of this step.

The agent responsible for performing recovery must also be identified. If several agents are involved, the agent responsible for initiating the recovery should be identified.

Figure 9 shows an example of how a next recovery and responsible performing agent can be described in RBAT.

6.5 Part 5: Address risk control

The purpose of addressing risk control is to ensure that RBAT is used to specify ways for how to reduce risks associated with the identified failure conditions/modes.



RISK CONTROL	
Comments	**Actions**
Emergency dropping of anchor is fully manual.	Consider implementing automatic stop of the vessel in case crossing pre-defined waypoints in too high speed.
...	...

Figure 10 – Risk control module in RBAT

6.5.1 Step 14: Identify and document risk control measures

The fourteenth and final step of the process is to identify risk control measures (RCM). This is done by recording actions and any necessary comments in a column dedicated for this purpose (see Figure 10). In the case of RBAT, risk can be reduced by:

- Removing the hazard associated with the function, e.g. the fewer or less flammable hazards onboard, the need for fire prevention and protection functions (which can fail) is reduced or eliminated (inherent safety).
- Reducing the function's failure frequency, e.g. by improving component reliability through design or maintenance or introduce system redundancy.
- Improving supervision of control functions, i.e. increase probability of failure being detected and recovered.
- Introduce measures which mitigate the consequences in case a worst-case outcome should occur.

An elaborate description of generic RCM attributes (categories) can be found in the FSA guideline's Appendix 6 and is therefore not described in any more detail here.

7 OPPORTUNITIES FOR PERFORMING AGGREGATED ANALYSES

The current version of RBAT is limited to addressing risks and control measures per function. It is however set up to create opportunities for using the data to perform aggregated analyses, particularly if supported by suitable software features. This chapter provides a summary of the opportunities which are known at present and should be explored as part of developing RBAT further.

7.1 Human involvement

While RBAT is performed per vessel, the operators may be performing and supervising agents for multiple ships. This creates challenges when it comes to human factors related topics such as task complexity, several vessels requiring attention at the same time, and excessive workload, among other things[8].

RBAT collects the following data which can be used in combination to control for such factors:

- Via the Mission Model and Function Tree and the use of unique operator identification labels[9], RBAT captures *when* different operators are involved. This makes it possible to check the amount, type and sequence of control actions each operator is required to either supervise or perform, both internally for each vessel, but also across several vessels.
- Involvement is described either as being a performing or (active/passive) supervising agent. This provides an indication of workload and the availability/capacity for each operator. For example, if an operator is expected to actively supervise the operation on Vessel A while simultaneously performing control actions on Vessel B, this may reduce human reliability for one or both tasks. A likely scenario would be that active supervision is turned into passive supervision, to be able to perform the required control action. If an incident occurs on Vessel A the operator does not have the benefit of situational awareness which comes with active supervision, and human errors are more likely to occur. RBAT should be used to check for such weaknesses and update the ConOps accordingly.

7.2 Event sequences

As explained in sub-chapters 6.4.1 (Step 11) and 6.4.2 (Step 12) the consequences from function failures are not only considered in terms of accidents, but also in terms of effects on safety margin. In cases where failures do not directly result in an accident, the RBAT user can rank the severity according to how many additional failures must occur for this to happen. By also identifying which accident category the failure can potentially contribute to, the RBAT user can filter and check how combinations of failures or sequences of events pose a threat towards accident prevention. This makes it possible to screen for vulnerabilities inherent in the system design and operational concept.

7.3 Accident contribution

By keeping track of which accident categories various functions contribute to, also across the vessel's mission phases and operations, it is possible to consider whether certain functions should be devoted additional attention, for example in terms of equipment reliability/availability, supervision, as well as inspection and maintenance.

[8] See SAFEMASS reports for more detailed explanations (DNV GL, 2020a; 2020b).

[9] E.g. LO1= local operator 1, RO1= remote operator 1 etc.

8 RECOMMENDATIONS FOR PART 2 OF RBAT

The following recommendations have been noted for Part 2 of the RBAT study:

- Preliminary testing of RBAT performed as part of the method development has brought forward some indications that a separate definition for supervision by a machine agent may be needed. A machine agent (i.e. computerized) may be continuously monitoring a control function and actions, yet only detect and respond to failures (on demand) in cases where pre-defined parameters have been breached. As such, a machine agent represents a mix of active and passive supervision, as it is currently defined.
- A significant part of the failure conditions/modes will result from software failures or limitations. Software failures are difficult to predict both in terms of modes as well as frequencies, and the experience with software developed for MASS applications is limited. The current version of RBAT includes failure frequencies as part the risk metrics. Challenges and limitations when it comes to software failure frequencies should be explored and understood to establish a best possible approach for performing risk ranking. Alternatives include (but is not limited to) use of elicitation techniques, conservatism, or assume occurrence of failures and limit the estimation of probability to that of recovery.
- It was opted not to include a separate column in the RBAT table for describing failure causes/mechanisms. The guidance state that failure causes can be (optionally) included as part of the failure description. The rationale was that because RBAT is intended to be used at an early stage in the concept development, the system architecture, and therefore causes, will not always be apparent. Another argument is related to a general ambition about keeping the number of columns down as a way of preventing the method from becoming over complex and time consuming. There are however counterarguments; by having to identify failure causes it will be easier to estimate the failure frequency. Another pro-argument is that both the detection and response may be different depending on what has caused the failure to occur. If there is limited information available about the actual design, this can be compensated by using generic terms.
- How to best approach global and continuous functions, i.e. functions which span across several mission phases and/or interact with several other functions, have not been thoroughly explored. One example is integrated monitoring and control. Potential challenges may arise related to repeating the same functions across multiple operations, but with diminishing returns from efforts put into performing the analysis. How to best test a suitable approach should be planned when starting Part 2 of the study.
- Table 4 in sub-chapter 6.3.3 includes a probability index for recovery, including definitions for degrees of what can be considered successful detection and response performed by human or technological supervising agents. The suggested definitions for machine agents are considered immature and should be targeted for improvement based on new knowledge and insights gained from the upcoming test cases in Part 2 of the study.
- Since issuing report 1/2 “Handle payload” has been identified as a key function. In case opportunities arise as part of the scope of work for Part 2, this function should be decomposed into a set of sub-functions.
- The definition of Minimum Risk Condition should be re-visited and aligned with a definition of safe operating envelope, as well as definitions used to describe safety and reliability (e.g. definitions of failure).

9 REFERENCES

American Bureau of Shipping, ABS (2020). *ABS Advisory on Autonomous Functionality*. https://ww2.eagle.org/en/innovation-and-technology/digital/autonomy.html

Bureau Veritas, BV (2019). *Guidelines for Autonomous Shipping*. Guidance Note: NI 641 DT R01 E.

DNV GL (2018a). *Autonomous and Remotely Operated Ships*. Class Guideline: DNVGL-CG-0264. Edition September 2018.

DNV GL (2018b). Report from HazId workshop on remote machinery operations: ROMAS project. Report No.: 2018-0084, Rev. 1.1

DNV GL (2019). *Technology Qualification*. Recommended Practice: DNVGL-RP-A203. Edition September 2019.

DNV GL (2020a). Study of the risks and regulatory issues of specific cases of MASS (SAFEMASS) – Part 1. Report No.: 2019-1296, Rev. 0.

DNV GL (2020b). Study of the risks and regulatory issues of specific cases of MASS (SAFEMASS) – Part 2. Report No.: 2019-0805, Rev. 0.

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

DNV GL (2020d). 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.

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

European Maritime Safety Agency, EMSA (2020b). Annual overview of marine casualties and incidents 2020. Downloaded from: http://www.emsa.europa.eu/we-do/safety/accident-investigation/item/4266-annual-overview-of-marine-casualties-and-incidents-2020.html

ENCO (2015). Assessing regulatory requirements and guidelines for the single failure criterion. Final Report ENCO FR-(15)-12.

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

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 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.

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.

Kritzinger, D. (2016). *Aircraft System Safety: Assessments for Initial Airworthiness Certification.* Woodhead Publishing.

Lloyd’s Register, LR (2017). *ShipRight Design and Construction: LR Code for Unmanned Marine Systems.* February 2017

Parasuraman, R., Riley, V. (1997) *Humans and automation: use, misuse, disuse, abuse*. Human Factors: The Journal of the Human Factors and Ergonomics Society 39, 230–253. https://doi.org/10.1518/001872097778543886

Ramos, M.A., Utne, I.B., & Mosleh, Ali. (2019). Collision avoidance on maritime autonomous surface ships: Operators’ tasks and human failure events. *Safety Science*, 116, pp. 33-44.

Ramos, M.A., Thieme, C.A., Utne, I.B., & Mosleh, A. (2020). A generic approach to analysing failures in human-system interaction in autonomy. *Safety Science*, 129, 104808.

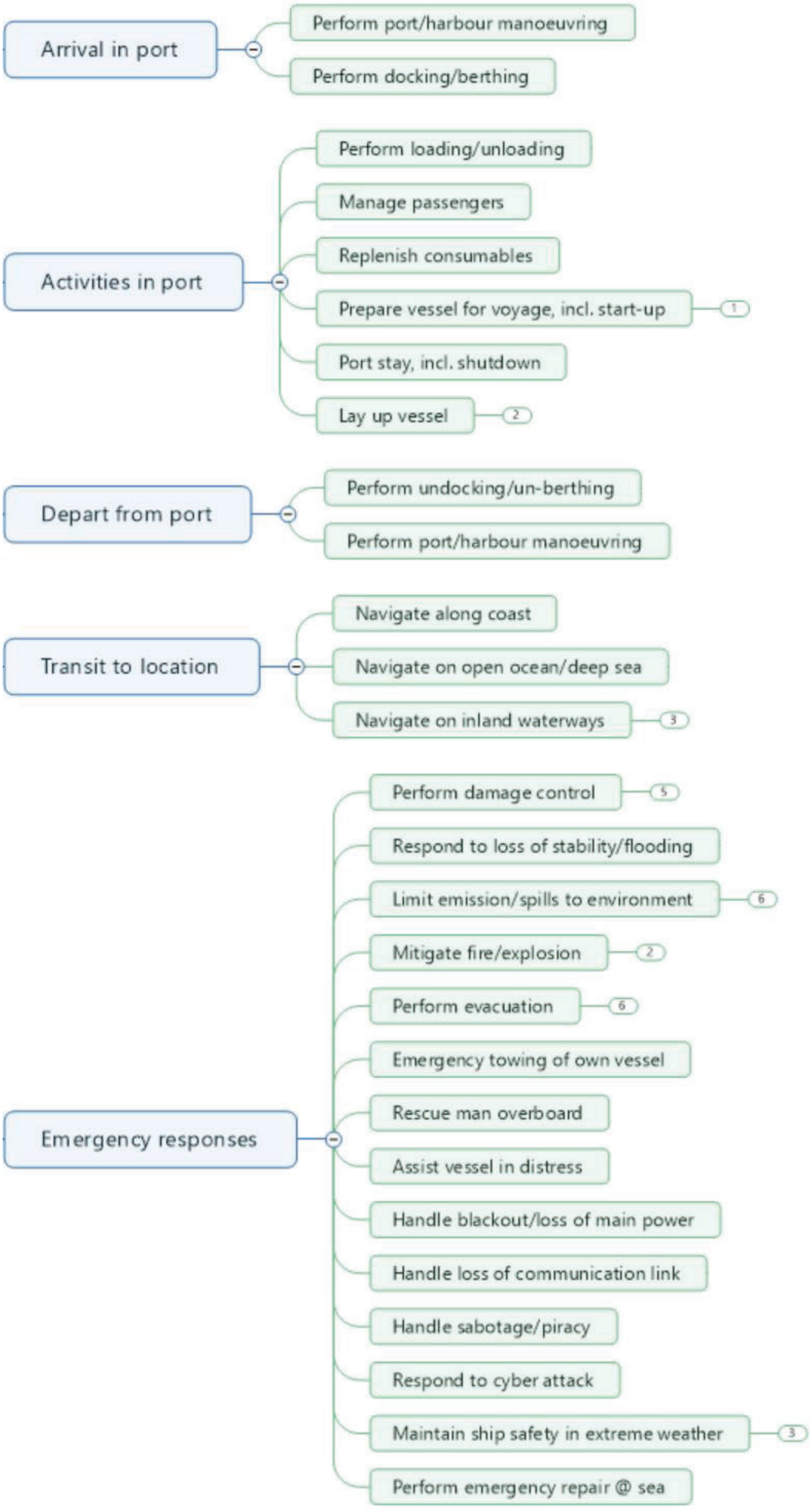
SAE Aerospace (1996). *Guidelines and methods for conduction the safety assessment process on civil airborne systems and equipment. Aerospace Recommended Practice ARP4761*. First edition.

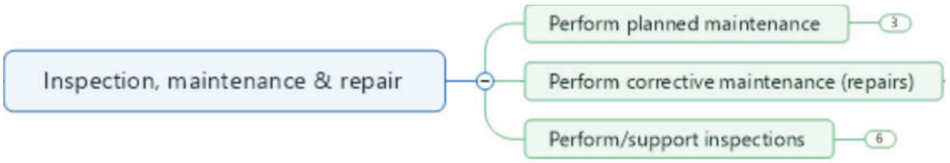
SAE Aerospace (2010). *(R) Guidelines for Development of Civil Aircraft and Systems*. Aerospace Recommended Practice ARP4754. Rev. A.

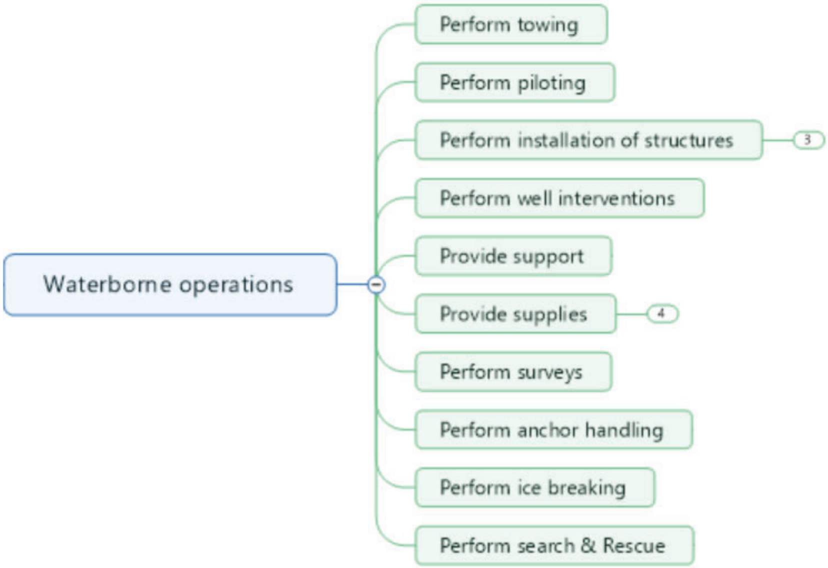
Sheridan, T. B., Parasuraman, R. (2006). *Human-automation interaction*. Reviews of Human Factors and Ergonomics, 1, 89–129.

Wang, C. (2007). *Hybrid causal logic methodology for risk assessment.* Dissertation submitted to the Faculty of the Graduate School of the University of Maryland (Ph.d.).

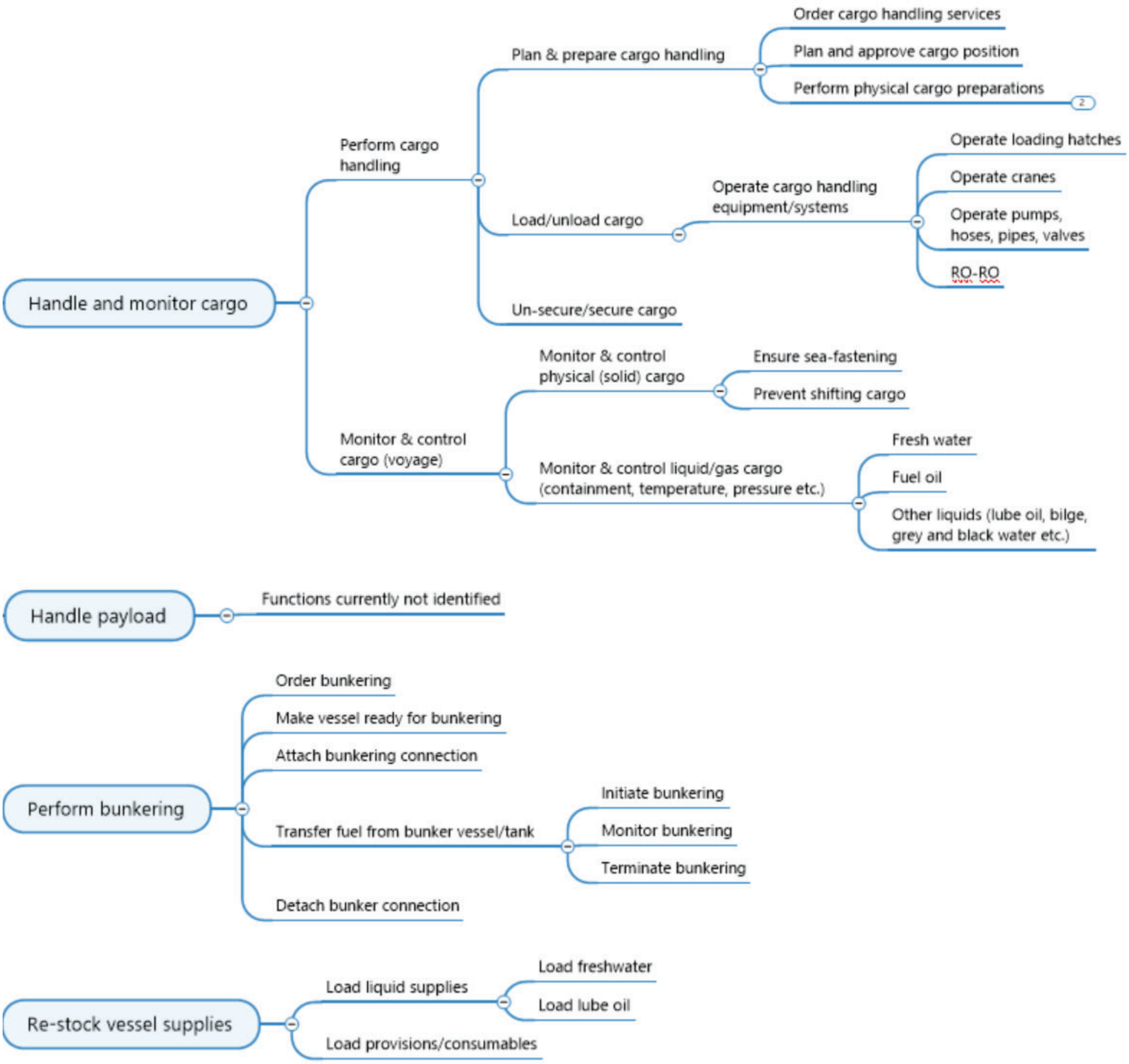
APPENDIX A
Mission Model

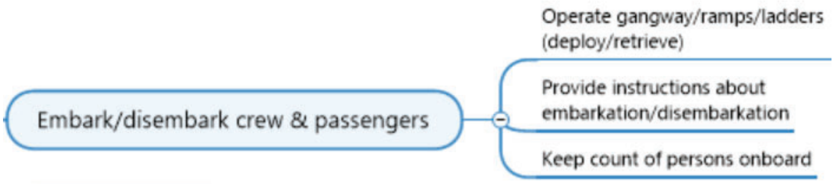

Arrival in port
Perform port/harbour manoeuvring
Perform docking/berthing
Activities in port
Perform loading/unloading
Manage passengers
Replenish consumables
Prepare vessel for voyage, incl. start-up
1
Port stay, incl. shutdown
Lay up vessel
2
Depart from port
Perform undocking/un-berthing
Perform port/harbour manoeuvring
Transit to location
Navigate along coast
Navigate on open ocean/deep sea
Navigate on inland waterways
3
Emergency responses
Perform damage control
5
Respond to loss of stability/flooding
Limit emission/spills to environment
6
Mitigate fire/explosion
2
Perform evacuation
6
Emergency towing of own vessel
Rescue man overboard
Assist vessel in distress
Handle blackout/loss of main power
Handle loss of communication link
Handle sabotage/piracy
Respond to cyber attack
Maintain ship safety in extreme weather
3
Perform emergency repair @ sea

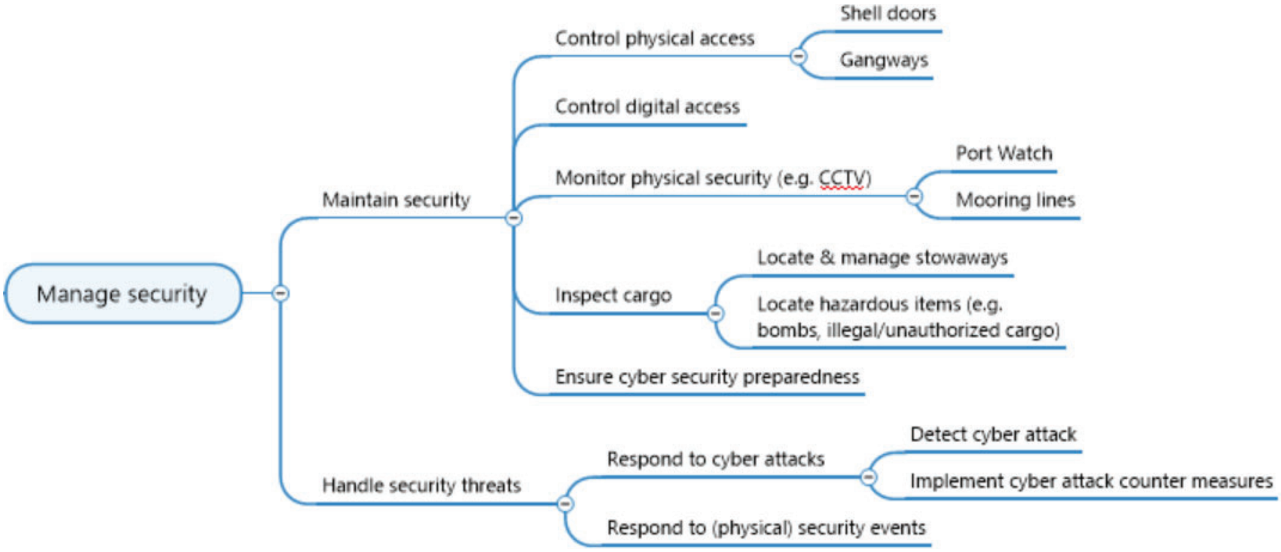

Inspection, maintenance & repair
Perform planned maintenance
3
Perform corrective maintenance (repairs)
Perform/support inspections
6

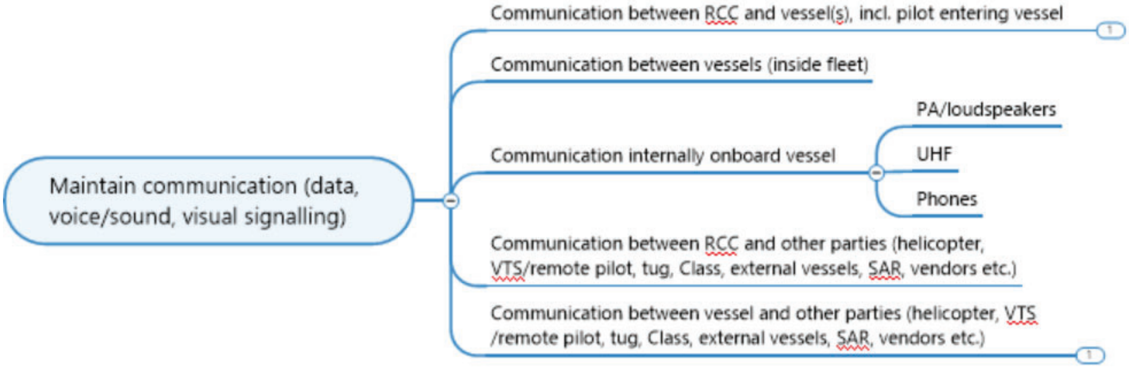

Waterborne operations
Perform towing
Perform piloting
Perform installation of structures
3
Perform well interventions
Provide support
Provide supplies
4
Perform surveys
Perform anchor handling
Perform ice breaking
Perform search & Rescue

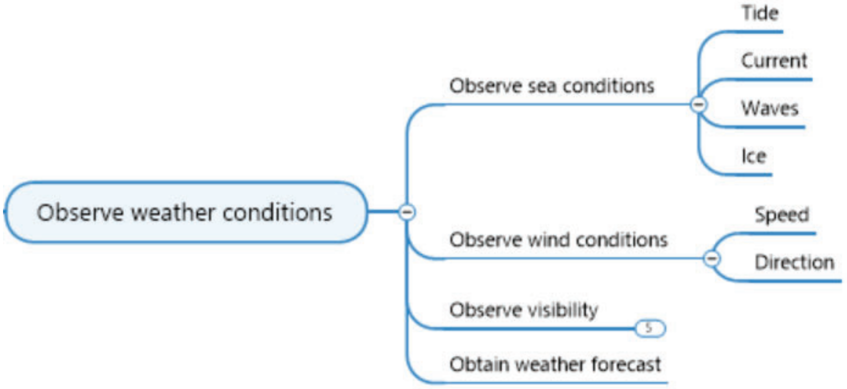
APPENDIX B
Function Tree

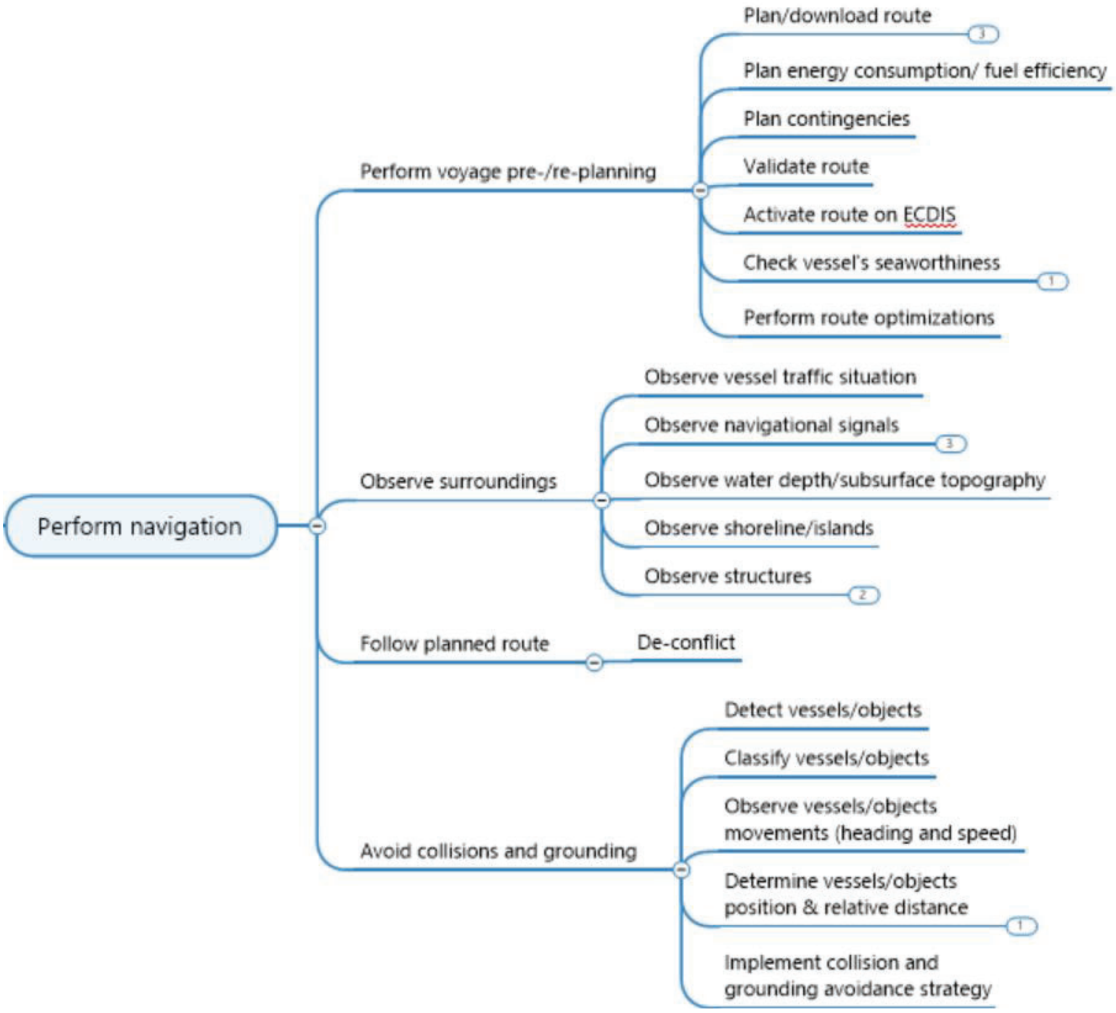

Handle and monitor cargo
Perform cargo handling
Plan & prepare cargo handling
Order cargo handling services
Plan and approve cargo position
Perform physical cargo preparations
2
Load/unload cargo
Operate cargo handling equipment/systems
Operate loading hatches
Operate cranes
Operate pumps, hoses, pipes, valves
RO-RO
Un-secure/secure cargo
Monitor & control cargo (voyage)
Monitor & control physical (solid) cargo
Ensure sea-fastening
Prevent shifting cargo
Monitor & control liquid/gas cargo (containment, temperature, pressure etc.)
Fresh water
Fuel oil
Other liquids (lube oil, bilge, grey and black water etc.)
Handle payload
Functions currently not identified
Perform bunkering
Order bunkering
Make vessel ready for bunkering
Attach bunkering connection
Transfer fuel from bunker vessel/tank
Initiate bunkering
Monitor bunkering
Terminate bunkering
Detach bunker connection
Re-stock vessel supplies
Load liquid supplies
Load freshwater
Load lube oil
Load provisions/consumables

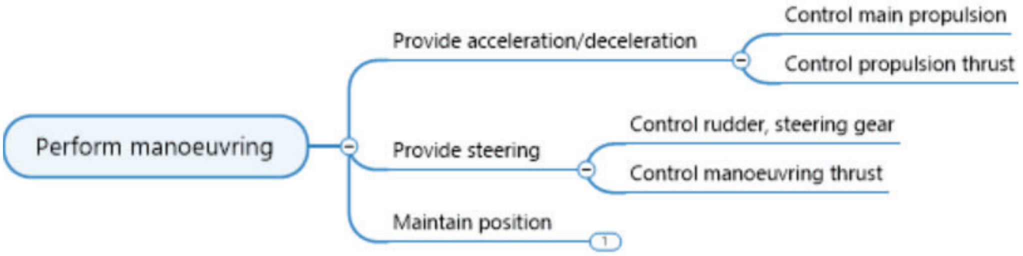

Embark/disembark crew & passengers
Operate gangway/ramps/ladders (deploy/retrieve)
Provide instructions about embarkation/disembarkation
Keep count of persons onboard

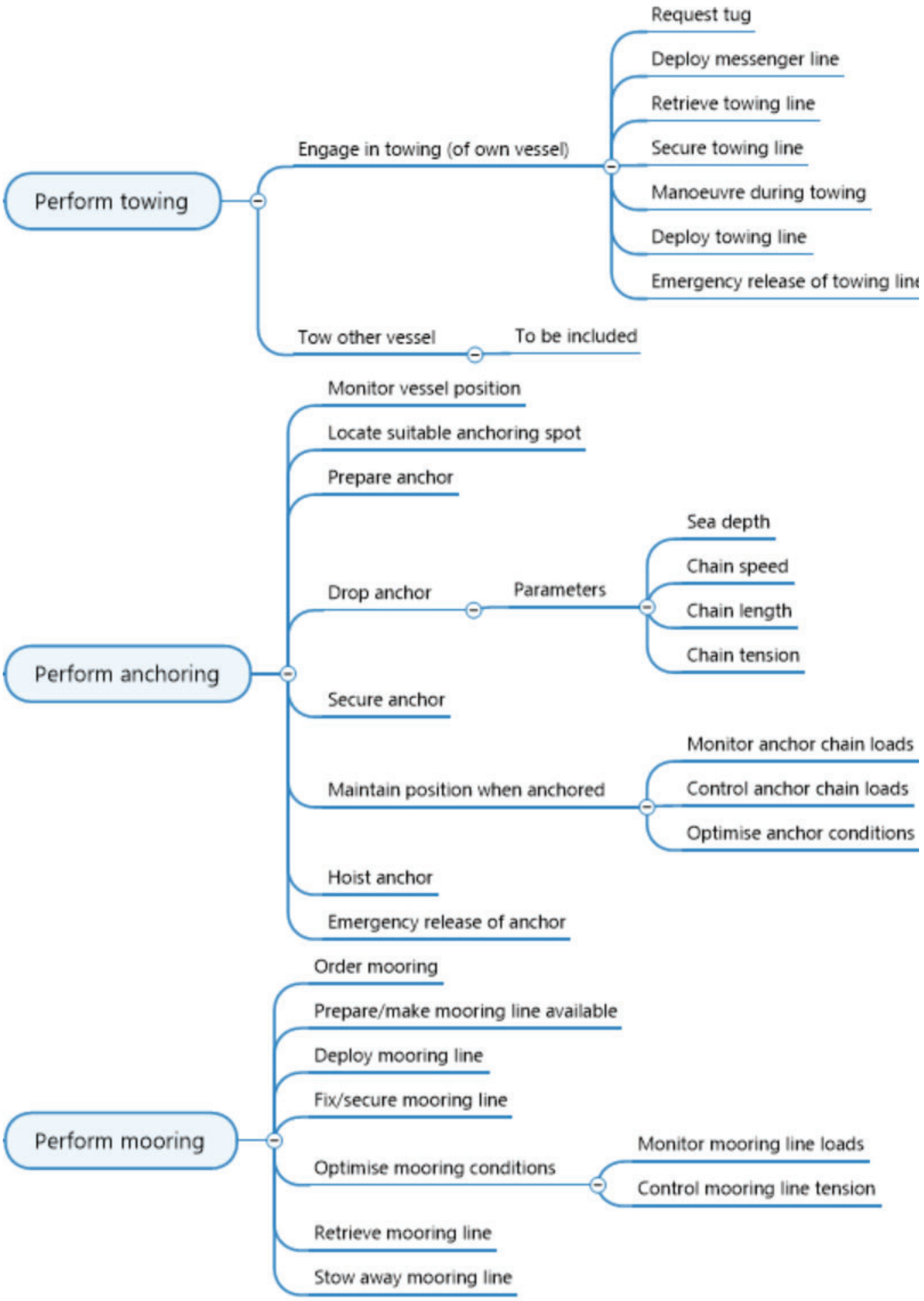

Manage security
Maintain security
Control physical access
Shell doors
Gangways
Control digital access
Monitor physical security (e.g. CCTV)
Port Watch
Mooring lines
Inspect cargo
Locate & manage stowaways
Locate hazardous items (e.g. bombs, illegal/unauthorized cargo)
Ensure cyber security preparedness
Handle security threats
Respond to cyber attacks
Detect cyber attack
Implement cyber attack counter measures
Respond to (physical) security events

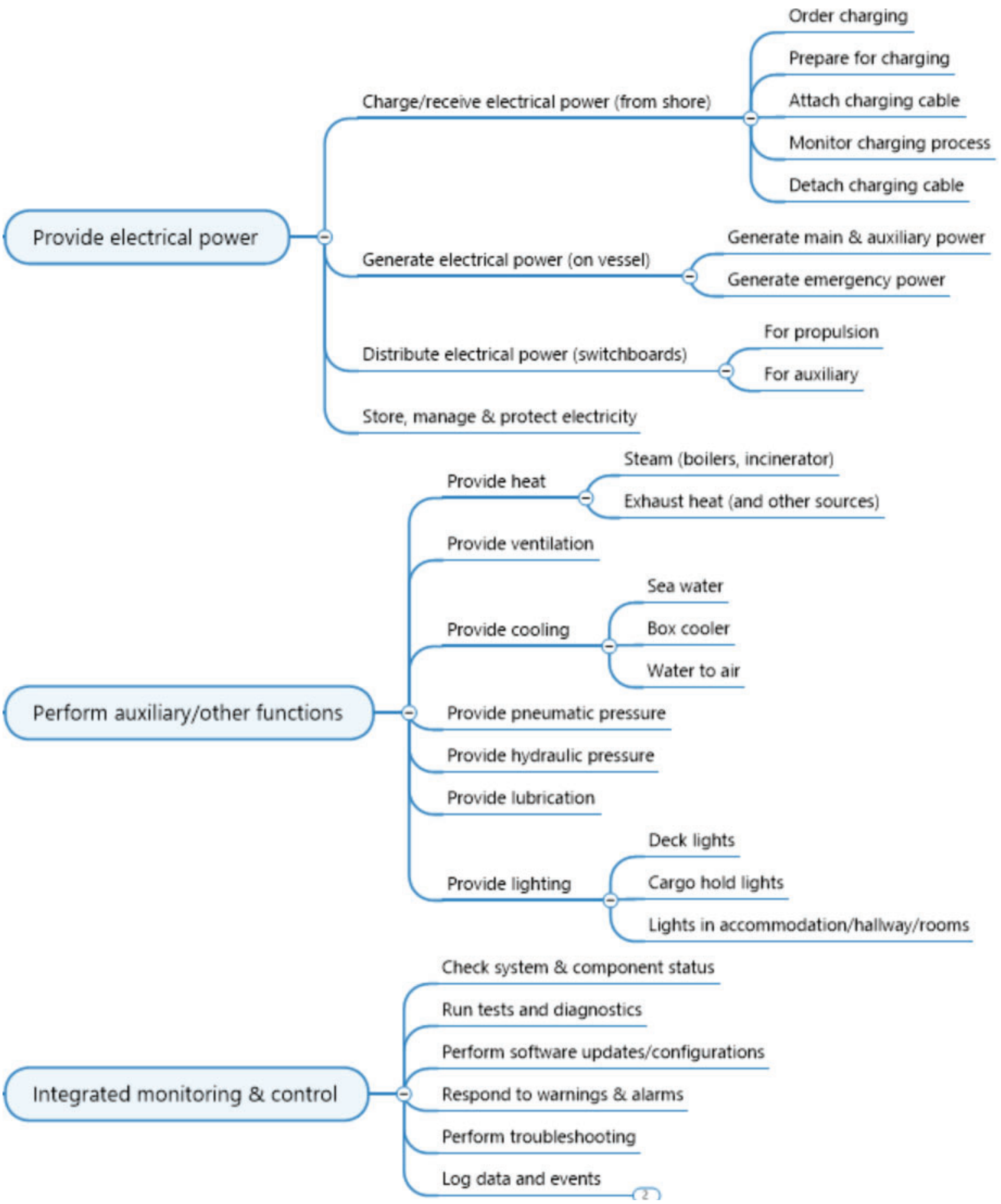

Maintain communication (data, voice/sound, visual signalling)
Communication between RCC and vessel(s), incl. pilot entering vessel
1
Communication between vessels (inside fleet)
Communication internally onboard vessel
PA/loudspeakers
UHF
Phones
Communication between RCC and other parties (helicopter, VTS/remote pilot, tug, Class, external vessels, SAR, vendors etc.)
Communication between vessel and other parties (helicopter, VTS /remote pilot, tug, Class, external vessels, SAR, vendors etc.)
1

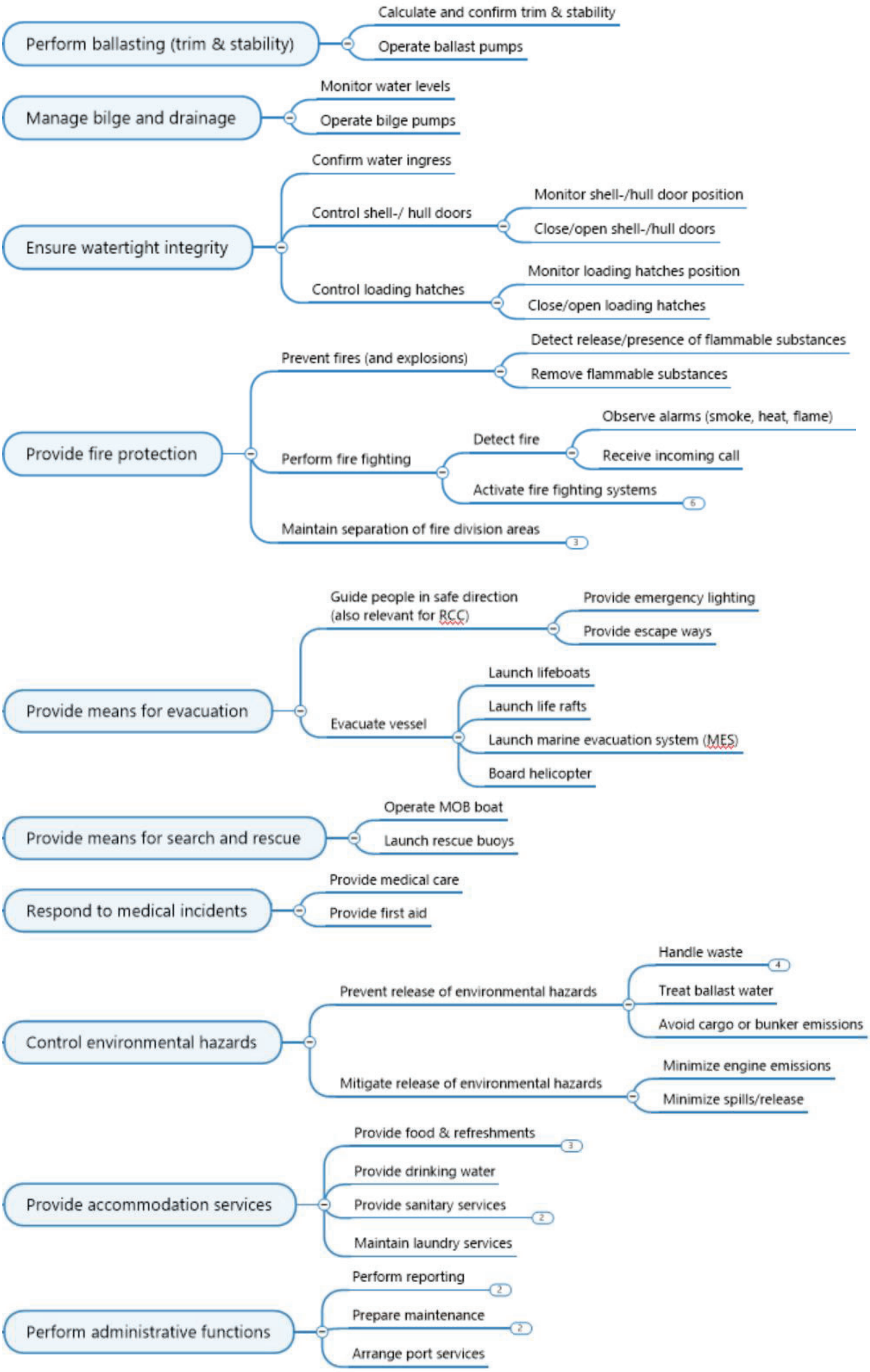

Observe weather conditions
Observe sea conditions
Tide
Current
Waves
Ice
Observe wind conditions
Speed
Direction
Observe visibility
5
Obtain weather forecast


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
Monitor charging process
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
Perform auxiliary/other functions
Provide heat
Steam (boilers, incinerator)
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
Check system & component status
Run tests and diagnostics
Perform software updates/configurations
Respond to warnings & alarms
Perform troubleshooting
Log data and events
2


Perform ballasting (trim & stability)
Calculate and confirm trim & stability
Operate ballast pumps
Manage bilge and drainage
Monitor water levels
Operate bilge pumps
Ensure watertight integrity
Confirm water ingress
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
6
Maintain separation of fire division areas
3
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 C
Hazard identification

Problem definition

Appendix C documents the HAZID performed as part of activity c) for Part 1 of RBAT, namely, to develop a list of hazardous conditions and events which can be linked to functions being targeted for various levels of automation.

Limitations

As with the RBAT framework in general, the focus is on safety-related aspects, and not concerns related to cybersecurity, unless they have implications for safety.

Terms and definitions

The HAZID aims to, as far as reasonable, build on the definitions, terminology and methodological principles as outlined in the FSA guideline (IMO, 2018). In cases additional definitions or alternative interpretations are found necessary, this is explained and accounted for.

Accident scenario

The FSA guideline defined an accident scenario as “a sequence of events from the initiating event to one of the final stages”, i.e. it is the qualitative description of the causes and final outcomes of an accident, usually communicated by use of various risk models such as event- and/or fault trees.

Accident

An accident is defined by the FSA guideline as “an unintended event involving fatality, injury, ship loss or damage, other property loss or damage, or environmental damage”. As can be read from the definition; what characterizes an accident, and distinguishes it from a hazard or failure, is that it involves observable consequences (i.e. losses). If an event only has negligible consequences, it is not considered an accident, but can instead represent a failure or cause.

Prospectively, an accident is therefore to be considered at, or near, the end of an accident scenario sequence, i.e. when the maximum amount of expected consequences has been achieved. Still, accidents can be considered to occur sequentially or in parallel, e.g. a ship may sink following a capsizing.

Accident category

The term accident category is used by the FSA guideline about “a designation of accidents reported in statistical tables according to their nature, e.g. fire, collision, grounding, etc.”. I.e. an accident category is a generic umbrella term for labelling different types of accidents. In addition, the term “accident sub-category” is used, but without being defined specifically. In the FSA guideline it is used about more detailed descriptions of accidents, typically including the location of the accident e.g. “fire in accommodation”.

Direct cause

The term “direct cause” is not defined by the FSA but is illustrated as the events closest to the accidents (see figure 6 on page 19 in the guideline). In the context of the RBAT HAZID, direct causes are the events which singly, or in few numbers, can cause an accident (and severe losses) if they occur in the presence of a hazard. I.e. a direct cause does not necessarily by itself (isolated) involve any serious, accident-like consequences. A loss of the communication link between a control centre and a MASS does not have to cause an accident in the middle of the ocean, but when sailing close to navigational hazards (e.g. ship traffic) such failures can be the direct cause of an accident.

A direct cause, the way it is illustrated in the FSA guideline, can also correspond to what is referred to as the TOP event in a fault tree analysis, i.e. a critical event (e.g. system failure) for which causes are deductively explored. Another closely related term is hazardous event which refers to incidents which occurs when a hazard (potential source of harm) is realized.

For a HAZID, direct causes are normally described using binary/absolute terms, such as “failure to…” or “loss of…”.

When used to assess risk associated with automation, a direct cause reflect failure to perform a function or set of sub-functions as intended (or required).

Initiating event

In accident causation, the FSA guideline uses the term “initiating event” about the first of a sequence of events leading to a hazardous situation or accident. Because accidents, and especially major ones, have multiple rather than single (root) causes, multiple initiating events often need to be considered in combination. The most detailed level of events in a fault tree, so called “basic events”, can be considered a type of initiating events.

In cases where event trees are used without being combined with fault trees, the initiating event may be a single event. If so, the initiating event is often an incident involving a loss of control over a hazard. The objective of the analysis is to examine the probability of certain outcomes as a product of performance of safety barriers and presence of escalating factors.

In the FSA guideline the terms “initiating event” and “causes” are often used interchangeably or in combination.

Hazard

The FSA guideline defines the term hazard as “a potential to threaten human life, health, property or the environment”. For the purpose of this study, 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 is present (movements, pressures, gravity, electricity, temperature etc., see Figure 11).

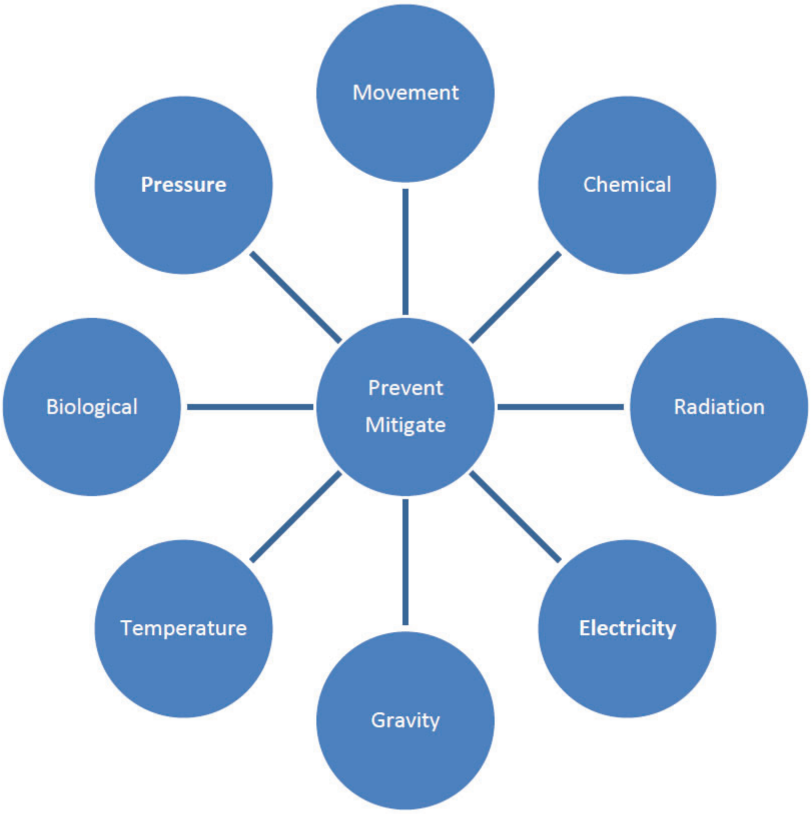


Figure 11 – Potential safety hazards

In maritime, examples of hazards include:

- Weather conditions influencing the vessels stability and manoeuvrability
- Other vessels (and objects) which needs to be navigated around
- Surface (e.g. a pier) or sub-surface (e.g. a reef) structure which needs to be avoided

HAZIDs are often based on brainstorming sessions (e.g. workshops) and does not necessarily make a clear distinction between the sources of harm and the causes which allow hazards to result in accidents (i.e. losses). Such causes refer to failures in functions which have been implemented specifically to prevent, control or mitigate the effects from hazards. An example can be loss of propulsion which, by itself, does not necessarily cause any harm, but may do so in the presence of a shallow reef;

Shallow reef (hazard) + Loss of propulsion (failure) = grounding (accident) = damage to ship (consequence).

The need to make this distinction stems from how the risk of an undesired event (e.g. accident) is determined by the context in which they occur (ISO, 2009). Losing the communication link between a MASS may not cause many problems while docked, however, when arriving a port with dense vessel traffic, this may be critical. As such, a function failure should not be considered a source of harm by itself, but in combination with whatever hazards may be present.

<u>HAZID methodology</u>

HAZID preparations

The first step of preparing the HAZID was to identify a set of generic accident categories. This was done by reviewing various known sources, including publications made available by EMSA, DNV, Bureau Veritas, and IHS Markit (IHS Fairplay). The various accident categories, including available definitions, were systematically compared to check for overlaps, inconsistencies, and potential gaps. Table 6 provides a summary of the comparison.

Table 6 – Comparison of accident categories

EMSA	DNV	Bureau Veritas	IHS Fairplay
Collision	Collision	Collision	Collision
	Striking		
Contact	Impact	--	Contact
	Aircraft strike	--	--
Grounding/stranding	Grounding	Grounding	Wrecked/stranded
Fire/explosion	Fire/explosion	--	Fire & explosion
Loss of control	Cargo transfer failure	--	--
Capsize/listing	Foundering/capsize	Sinking	Foundered
Flooding/foundering			
Damage to ship equipment	---	Hull or machinery damage	Hull/Machinery damage
Hull failure	Structural failure		
Non-accidental event	Sabotage	Illegal actions	War loss/Damage during hostilities
Missing	--	Loss of localisation	Missing vessel
--	--	--	Miscellaneous

It was concluded that EMSAs accident categories (see Table 7) were the most complete and covered all the categories found in other sources. It was also considered the accident taxonomy best supported by definitions and explanations, which is made available in their Annual Overview of Marine Casualties and Incidents (EMSA, 2020).

It is noteworthy that *damage to/loss of ship equipment* and *hull failure* refer to independent events which occur in the absence of the other accident categories. For example, hull failure caused by loss of or degraded structural integrity, and not because of a collision or grounding, or damage to ship equipment caused by equipment breakdown or malfunction, and not by a fire or explosion. It could also be mentioned that *loss of control* can be precursor events to other several other accident categories. The *casualty of persons* category was not found in EMSAs annual review but was communicated by EMSA via email to be valid. It represents illness and injuries (incl. fatalities) to people which are not caused by any of the other accidents. Examples include infections due to virus or bacteria, slips, trips and falls, or being hit by falling objects.

Table 7 – EMSAs accident categories

Collision

- With other ship
- With multiple ships

Contact

- Floating object
    - Cargo
    - Ice
    - Other
- Flying object
- Shore object

Grounding/stranding

- Grounding
- Stranding

Fire/explosion

- Fire
- Explosion

Capsize/listing

- Capsize
- Listing

Flooding/foundering

- Flooding
- Massive flooding
- Progressive flooding
- Foundering

Damage to/ loss of ship equipment

Hull failure

Non-accidental event

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

Missing

Loss of control

- Loss of containment
- Loss of directional control
- Loss of electrical power
- Loss of propulsion power

Casualty of persons

A literature review of approximately 40 publications was then performed with the purpose of identifying as many hazards and causes as possible, which could contribute to the various accident types. The documents included academic articles, conference papers, technical risk assessments reports, industry standards, and guidelines. Because the HAZID is being used to establish a high-level and generic accident model, risk analysis of both conventional vessels as well as MASS were reviewed.

Out of the approximately 40 reviewed documents, the following provided input to the HAZID:

- Antão, P. & Soares, G. (2006). Fault-tree Models of Accident Scenarios of RoPax Vessels. International Journal of Automation and Computing, 2, pp. 107-116.
- Banda, O.A.V. & Kannos, S. (2017). Hazard analysis process for autonomous vessels. Report part of the “Smart City Ferries” (ÄLYVESI) project.
- Bureau Veritas (2019). Guidelines for Autonomous Shipping. Guidance Note NI 641 DT R01 E.
- Chen, P., Mou, J., & Li, Y. (2015). Risk analysis of maritime accidents in an estuary: A case study of Shenzhen Waters. Scientific Journals of the Maritime University of Szczecin, 42 (114), pp. 54–62.
- DNV GL (2017). Concept hazard identification (HAZID) of “Yara Birkeland” - autonomous operation. DNV GL Report No.: 2017-0926.
- DNV GL (2018). Autonomous and remotely operated ships. Class guideline DNVGL-CG-0264.
- DNV GL (2018). Report from HazId Workshop on Remote Machinery Operations. Report No.: 2018-0084, Rev. 1.1
- Fan, C., Wróbel, K., Montewka, J., Gil., M., Wan, C., & Zhang, D. (2020). A framework to identify factors influencing navigational risk for Maritime Autonomous Surface Ships. Ocean Engineering, 202, pp. 107-188.
- Kum, S. & Sahin, B. (2015). A root cause analysis for Artic Marine accidents from 1993 to 2011. Safety Science, 74, pp. 206–220.
- Thieme, C.A., Utne, I.B., & Haugen, S. (2018). Assessing ship model applicability to marine autonomous surface ships. Ocean Engineering, 165, pp. 140-154.
- Uğurlu, Ö., Köse, E., Yıldırım, U. & Yüksekyıldız, E. (2015). Marine accident analysis for collision and grounding in oil tanker using FTA method, Maritime Policy & Management, 42:2, 163-185, DOI: 10.1080/03088839.2013.856524
- Ung, S-T. (2019). Evaluation of human error contribution to oil tanker collision using fault tree analysis and modified fuzzy Bayesian Network based CREAM. Ocean Engineering, 179, pp. 159–172.
- Wróbel, K., Montewka, J., & Kujala, P. (2017). Towards the assessment of potential impact of unmanned vessels on maritime transportation safety. Reliability Engineering and System Safety, 165, pp. 155-169.
- Zhang, M., Zhang, D., Goerlandt, F., Yan, X., & Kujala, P. (2019). Use of HFACS and fault tree model for collision risk factors analysis of icebreaker assistance in ice-covered waters. Safety Science, 111, pp. 128–143.
- Quraishi, E.A. (2019). Risk Analysis of Marine Accident Inland Waterways of Bangladesh Using Fault Tree Analysis Method. Master Thesis submitted to Department of Naval Architecture and Marine Engineering.

A list of generic hazards was identified. This included applying the distinction between hazards and (system) failures as explained under the heading title “Direct cause”.

Table 8 – List of generic hazards

Navigational hazards

- Onshore structures (bridges, dock, pier, jetty)
- Offshore structures (windmills, rigs, platforms)
- Seabed structures/obstructions (subsea installations, pipelines, shipwrecks)
- Shallow waters (reefs/ rocks, sandbanks, shore, beach)
- Narrow waters/ shoreline
- Ship traffic (large vessels)
- Pleasure crafts (sailboats, motorboats, rowboats, canoes)
- Floating foreign objects (logs, barrels, containers, fishing equip., buoys, ice)
- Unclear/ missing navigational marks

Natural hazards

- Strong currents
- Strong winds
- Reduced visibility
- Large waves/ heave/ swell (w/o green sea on deck)
- Green seas on deck
- Heavy icing
- Tsunami
- Lightning*
- Floods (onshore)
- Landslides (onshore)
- Earthquake (onshore)

Hazards onboard vessel

- High voltage/ electricity/ sparks
- Flammable materials and liquids
- High pressure (e.g. liquid/gas storage)
- Chemically harmful/toxic substances (incl. exhaust/ emissions)
- Biological hazards (virus, bacteria)
- Passengers & crew conditions (heights, confined spaces etc.)
- Cargo loads
- Extreme temperature (incl. hot surfaces) *
- Radiation*
- Naked flames*
- Movement (e.g. rotating machinery) *

Sabotage/piracy – physical

- Unauthorized persons boarding vessel
- Unauthorized persons accessing the RCC
- Intentional blocking of vessel fairway
- Stowaways

Sabotage/piracy – digital, cyber

- Malware entering the systems
- Unauthorized persons gaining access to the communication link
- Unauthorized persons interfering with onboard systems
- Interception of data traffic by 3rd party
- Cyber-attacks/hacking

*Added after HAZID

Finally, a set of generic direct causes were developed by converting the key functions in the RBAT function tree into failures, e.g. “maintain communication” was converted to “communication failure”. These were then linked to, and checked against, various causes (i.e. failures) identified during the literature review.

RBAT key function failures	Failures identified as part of the literature review
Cargo handling failure	Crane failure Pump failure Loading hose failure (loss of containment)
Payload handling failure	None identified.
Bunkering failure	Bunkering hose failure (loss of containment)
Vessel supply loading failure	See *Cargo handling failure*.
Embark/disembarkation failure	None identified.
Security failure	None identified.
Weather observation failure	None identified.
Navigational failure	Object detection failure (sensor failure or degradation) Lookout/ watchkeeping failure Failure in detection of navigational marks Failure in detection of ship lights, sounds or shapes Failure in detection of semi-submerged towed or floating devices (e.g. seismic gauges, fishing trawls) Failure in detection of discrepancy between charted and sounded water depth (e.g. wreckage) Depth gauge/ Echo sounder failure Incorrect voyage plan (intentional, unintentional) Failure to maintain planned (correct) route Incorrect navigational data/parameters (nautical, weather forecast) Navigation instrument failure (radar, GPS., ECDIS etc.) Anti-collision system failure Deck computer failure (network, software) Navigational infrastructure incompatible with vessel Incorrect navigational mode switch
Manoeuvring failure	Shaft line failure Bow thruster failure

RBAT key function failures	Failures identified as part of the literature review
	Steering gear box failure Rudder failure Coupling failure Unexpected manoeuvres (control system failure, incorrect signal)
Towing failure	Towing arrangement failure – MASS Towing arrangement failure – Tug
Anchoring failure	Anchor line failure Anchor winch failure
Mooring failure	Mooring system failure (excessive tension, incorrect location, incorrect sequence) Foreign/ new dock not equipped for mooring MASS Object caught between vessel and quay/dock, blocking mooring
Watertight integrity failure	Watertight doors, hatches not fully closed Structural failure (fatigue, wave loads, vibration or adverse cargo load distribution)
Ballasting failure	Failure to calculate pre-departure stability Cargo overload Cargo shifting during voyage (incl. liquification, losses of cargo overboard)
Bilge and drainage failure	None identified.
Electrical power failure	Emergency power supply failure Ship power loss/blackout RCC power loss/ blackout (incl. power grid blackout) Charging failure Battery failure
Auxiliary failure	Main engine failure Auxiliary machinery failure Accumulator failure Hydraulic systems failure Overheating

RBAT key function failures	Failures identified as part of the literature review
Integrated monitoring and control failure	Failure to detect slamming or high vibrations in vessel IAS unavailable
Communication failure	Loss of communication links Communication systems failure (e.g. VHF) CCTV (camera) failure Visual signalling/navigational lights failure Vessel Traffic Service failure Network storms Jamming or spoofing of GPS or AIS signals Increase of latency Reduced/ insufficient bandwidth Insufficient radio-coverage for wireless links Unstable data links over time Failure in data integrity (e.g. error in data transmission, bit faults, bugs) Lack of unified data sharing standard Failure of electronic components in the communication links Damage to vessels IT infrastructure Damage to RCCs IT infrastructure Faulty software upgrades Failure to issue mayday
Evacuation failure	Failure to launch lifeboat Escape chute failure
Search and rescue failure	Failure to launch MOB boat
Medical incident response failure	None identified.
Fire protection failure	Failure to detect fire Failure to activate firefighting systems Failure to perform emergency shutdown
Environmental hazard control failure	None identified.
Accommodation services failure	None identified.

RBAT key function failures	Failures identified as part of the literature review
Administration failure	None identified.

HAZID procedure

The HAZID procedure consisted of the following steps:

1. Select a hazard guideword
2. Link hazard to relevant accident category
3. Identify the direct causes (i.e. function failures) of the accident
4. Repeat Step 1 to 3 until all hazard guidewords have been considered

The direct causes (pt. 3) were identified by checking whether one or several failures to perform sub-functions found in the RBAT function tree potentially could contribute to the accident. If this was the case, the highest function level in the RBAT function tree, i.e. the *key functions*, where included to represent a direct cause.

HAZID results

The HAZID log (Table 10) was used to develop a matrix (Table 9) which indicate the relationship between functions in the RBAT Function Tree and EMSAs accident categories, which is also the main deliverable of the HAZID activity.

A couple of noteworthy observations include:

Some of the accident sub-categories to *Loss of control* are precuring events to several of the other accident categories. For example, loss of directional control, loss of electrical power and loss of propulsion power can, depending on the scenario, precede Contact, Collision, Grounding and Capsize. They also represent a degraded and unsafe state, more than an accident with significant losses. This makes it difficult to associate them with specific sources of harm (i.e. hazards). Loss of control was therefore not applied as an accident category when creating the HAZID log. However, because Loss of control is likely to be the worst-case outcome of several failure conditions/modes identified using RBAT, it is included as an accident category in the function failure/accident matrix (Table 9).

Due to how *Integrated monitoring and control* is a function which interfaces with most of the other key functions it is considered a potential direct cause to all accident categories. It has therefore not been included as part of the HAZID log, as it would just be replicated for all the hazard-accident combinations, and not provide any additional insights.

Loss of RCC due to onshore natural hazards, such as floods and earthquakes, is likely to represent a wide variety of direct causes and contribute to several different accident categories. The link towards direct causes and accidents are therefore simply denoted as “Multiple”. The contribution to accident causation is argued to be similar as for *Communication failure* (loss of communication link).

Perform administration was the only key function which was not identified as a potential direct cause to any accidents.

Table 9 – Matrix indicating the relationship between the EMSA accident categories and key functions in the RBAT Function Tree

	Cargo handling and monitoring failure	Payload handling failure[10]	Bunkering failure	Vessel supply re-stock failure	Embark/disembarkation failure	Security failure	Weather observation failure	Navigational failure	Manoeuvring failure	Towing failure	Communication failure	Anchoring failure	Mooring failure	Watertight integrity failure	Ballasting failure	Bilge and drainage failure	Electrical power failure	Auxiliary function failure	Integrated monitoring and control failure[11]	Evacuation failure	Search and rescue failure	Medical incident response failure	Fire protection failure	Failure to control environmental hazards	Accommodation services failure	Administration failure
Collision		--					X	X	X	X	X	X	X				X		(X)							
Contact		--					X	X	X	X	X	X	X				X		(X)							
Grounding/stranding		--					X	X	X	X	X	X	X		X		X		(X)							
Fire/explosion	X	--	X	X													X		(X)				X			
Capsize/listing	X	--					X	X	X					X	X			X	(X)							
Flooding/foundering		--												X					(X)							
Damage to ship equipment	X	--					X	X	X									X	(X)				X			
Hull failure	X	--					X	X	X						X				(X)							
Non-accidental event		--				X													(X)							
Missing		--				X													(X)							
Loss of control[12]	*X*	--	*X*						*X*	*X*		*X*	*X*				*X*	*X*	*(X)*					*X*		
Illness/injury/loss of life[13]	*X*	--		*X*	*X*	*X*				*X*	*X*						*X*		*(X)*	*X*	*X*	*X*			*X*	

[10] The *Payload* key function has recently been added to the Function Tree and was therefore not included as part of the HAZID.

[11] Due to how *Integrated monitoring and control* can be considered a meta-function with interfaces across most of the other functions, it is expected to potentially contribute to all accident categories.

[12] Refers to loss of containment, directional control, electrical power, propulsion power and therefore resemble function failures (degraded system performance) more than accidents with losses.

[13] Refers to incidents involving illness/injuries/loss of life which can occur independently from the other accident categories. Some links have been made after completing the HAZID log, because of clarifications made with EMSA.

Table 10 – HAZID log

ID	Hazard	Direct causes	Accidents
	Navigational hazard		
H-1	Onshore structures (bridges, dock, pier, jetty)	Weather observation failure Navigational failure Manoeuvring failure Towing failure Anchoring failure Mooring failure Electrical power failure	Contact
H-2	Offshore structures (windmills, rigs, platforms)	Weather observation failure Navigational failure Manoeuvring failure Electrical power failure	Contact
H-3	Seabed structures/obstructions (subsea installations, pipelines, shipwrecks)	HOLD until functions for "Waterborne operations" have been identified.	HOLD until functions for "Waterborne operations" have been identified.
H-4	Shallow waters (reefs/ rocks, sandbanks, shore, beach)	Weather observation failure Navigational failure Manoeuvring failure Towing failure Anchoring failure Electrical power failure Ballasting failure	Grounding/stranding
H-5	Narrow waters/ shoreline	Weather observation failure Navigational failure Manoeuvring failure Towing failure Anchoring failure Electrical power failure	Grounding/stranding

ID	Hazard	Direct causes	Accidents
H-6	Ship traffic (large vessels)	Weather observation failure Navigational failure Manoeuvring failure Towing failure Anchoring failure Electrical power failure Communication failure	Collision
H-7	Pleasure crafts (sailboats, motorboats, rowboats, canoes)	Weather observation failure Navigational failure Manoeuvring failure Towing failure Anchoring failure Electrical power failure Communication failure	Collision
H-8	Floating foreign objects (logs, barrels, containers, fishing equip., buoys, ice)	Weather observation failure Navigational failure Manoeuvring failure	Contact
H-9	Unclear/ missing navigational marks	Navigational failure Manoeuvring failure	Grounding/stranding
	Natural hazards		
H-10	Strong currents	Weather observation failure Navigational failure Manoeuvring failure Towing failure Anchoring failure Mooring failure Electrical power failure	Collision

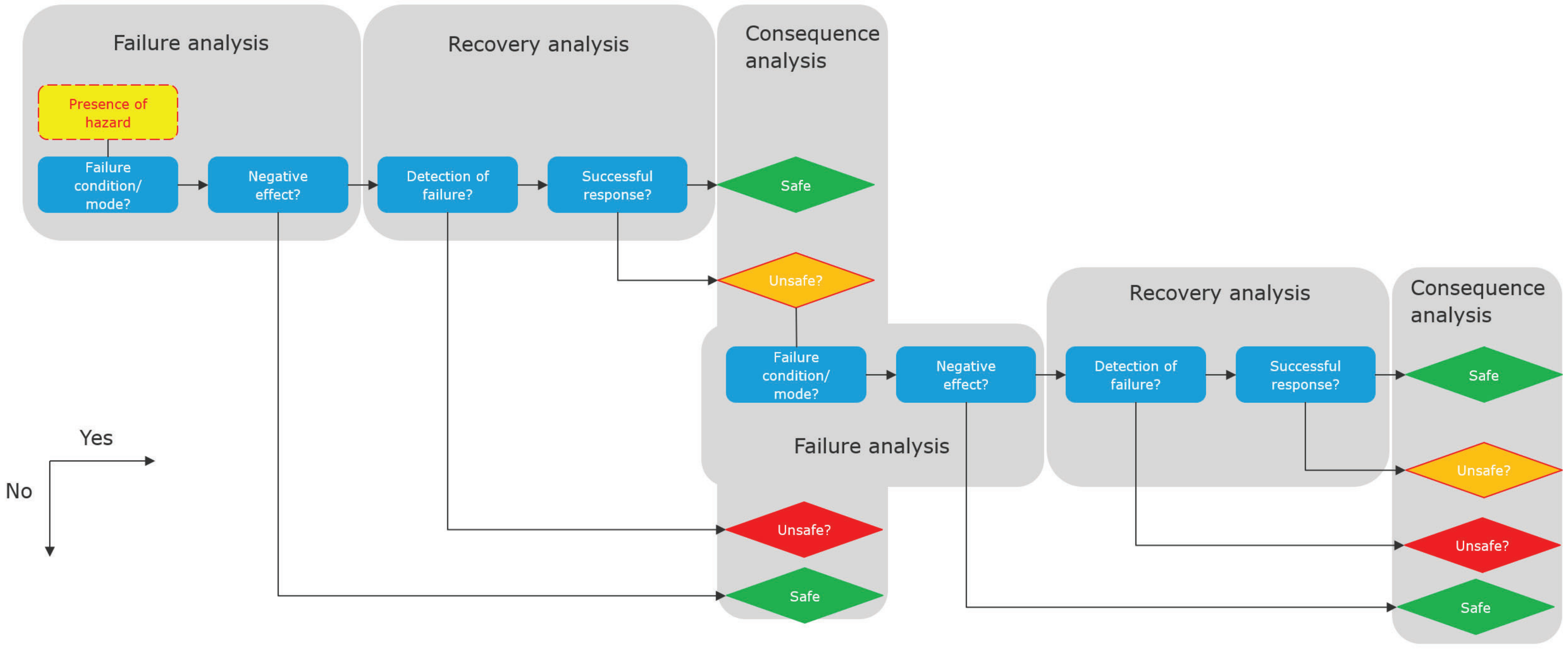
ID	Hazard	Direct causes	Accidents
H-11	Strong currents	Weather observation failure Navigational failure Manoeuvring failure Towing failure Anchoring failure Mooring failure Electrical power failure	Contact
H-12	Strong currents	Weather observation failure Navigational failure Manoeuvring failure Towing failure Anchoring failure Mooring failure Electrical power failure	Grounding/stranding
H-13	Strong winds	Weather observation failure Navigational failure Manoeuvring failure Towing failure Anchoring failure Mooring failure Electrical power failure	Collision
H-14	Strong winds	Weather observation failure Navigational failure Manoeuvring failure Towing failure Anchoring failure Mooring failure Electrical power failure	Contact

ID	Hazard	Direct causes	Accidents
H-15	Strong winds	Weather observation failure Navigational failure Manoeuvring failure Towing failure Anchoring failure Mooring failure Electrical power failure	Grounding/stranding
H-16	Strong winds	Weather observation failure Cargo handling failure	Damage to/loss of ship equipment
H-17	Reduced visibility	Weather observation failure Navigational failure Communication failure	Collision
H-18	Reduced visibility	Weather observation failure Navigational failure Communication failure	Contact
H-19	Reduced visibility	Weather observation failure Navigational failure Communication failure	Grounding/stranding
H-20	Large waves/ heave/ swell (w/o green sea on deck)	Cargo handling failure Weather observation failure Navigational failure Manoeuvring failure Ballasting failure	Capsize/listing
H-21	Large waves/ heave/ swell (w/o green sea on deck)	Cargo handling failure Weather observation failure Navigational failure Manoeuvring failure Ballasting failure	Hull failure

ID	Hazard	Direct causes	Accidents
H-22	Green seas on deck	Weather observation failure Navigational failure Manoeuvring failure Watertight integrity failure	Capsize/listing
H-23	Green seas on deck	Watertight integrity failure	Flooding/foundering
H-24	Green seas on deck	Weather observation failure Navigational failure Manoeuvring failure	Damage to/loss of ship equipment
H-25	Heavy icing	Weather observation failure Navigational failure Auxiliary function failure	Capsize/listing
H-26	Heavy icing	Weather observation failure Navigational failure Auxiliary function failure	Damage to/loss of ship equipment
H-27	Floods (onshore)	Multiple- Loss of RCC due to natural hazards	Multiple
H-28	Tsunami (onshore)	Multiple- Loss of RCC due to natural hazards	Multiple
H-29	Landsides (onshore)	Multiple- Loss of RCC due to natural hazards	Multiple
H-30	Earthquake (onshore)	Multiple- Loss of RCC due to natural hazards	Multiple
	Hazards onboard vessel		
H-31	High voltage/ electricity	Electrical power failure	Fire/ explosion
H-32	Flammable materials and liquids	Cargo handling failure Bunkering failure Vessel supply re-stock failure Fire protection failure	Fire/ explosion
H33	Liquid/gas stored under high pressure	Cargo handling failure Auxiliary function failure	Damage to/loss of ship equipment

ID	Hazard	Direct causes	Accidents
H-34	Chemically harmful/toxic substances	Cargo handling failure Vessel supply re-stock failure Failure to control environmental hazards	Loss of control (containment)
H-35	Biological hazards (virus, bacteria)	Accommodation services failure Medical incident response failure	Illness/ injury
H-36	Passengers & crew embarkation conditions	Embark/disembarkation failure	Illness/ injury
H-37	Cargo loads	Cargo handling failure	Hull failure
H-38	Cargo loads	Cargo handling failure	Capsize/listing
H-39	Cargo loads	Cargo handling failure	Damage to/loss of ship equipment
	Sabotage/piracy – physical		
H-40	Unauthorized persons boarding vessel	Security failure	Non-accidental event
H-41	Unauthorized persons accessing the RCC	Security failure	Non-accidental event
H-42	Intentional blocking of vessel fairway	Security failure	Non-accidental event
H-43	Stowaways	Security failure	Illness/ injury
	Sabotage/piracy – digital, cyber		
H-44	Malware entering the systems	Security failure	Non-accidental event
H-45	Unauthorized persons gaining access to the communication link	Security failure	Non-accidental event
H-46	Unauthorized persons interfering with onboard systems	Security failure	Non-accidental event
H-47	Interception of data traffic by 3rd party	Security failure	Non-accidental event
H-48	Cyber-attacks/hacking	Security failure	Non-accidental event

APPENDIX D
Linked event sequence diagrams



APPENDIX E
Verb list

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 F

Detection and response definitions

Probability	Success	Detection (human agents)	Definition
Very high probability	99 %	Successful detection is expected.	The failure condition/mode is detected by presenting the operator(s) with clear, unambiguous, and timely available cues (i.e. they are annunciated).
High probability	75 %	Successful detection should be expected.	As for "Very high probability", but lower probability can be argued for.
Moderate probability	50 %	Successful detection relies on operator vigilance.	Cues about the failure condition/mode are available, but detection relies on operators being vigilant.
Low probability	25 %	Successful detection only happens by chance (random, coincidence)	As for "Moderate probability", but lower probability can be argued for.
Very low probability	1 %	Successful detection cannot be expected.	No cues about the failure condition/mode are made available (e.g. they are unannunciated), or the cues are very vague, making detection random or impossible.

Probability	Success	Recovery (human agents)	Definition
Very high probability	99 %	Successful response is expected.	Opportunities for recovering from failures conditions/modes are systematically build into the system by use of solutions for monitoring and control, training and organisation (e.g. teamwork, manning level).
High probability	75 %	Successful response should be expected.	As for "Very high probability", but lower probability can be argued for.
Moderate probability	50 %	Successful response relies on above average operator performance.	Opportunities for recovering from failures condition/modes are available, but successful outcome relies on operator(s) having a higher than average skillset and trouble-shooting capabilities.
Low probability	25 %	Successful response only happens by chance (random, coincidence)	As for "Moderate probability", but lower probability can be argued for.
Very low probability	1 %	Successful response cannot be expected.	Opportunities for recovering from failures condition/modes are not available or depends extensively on external factors (circumstances) beyond the operator(s) control.

DNV

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.