DNV·GL

SAFEMASS

Study of the risks and regulatory issues of specific cases of MASS – Part 1

European Maritime Safety Agency (EMSA)

Report No.: 2019-1296, Rev. 0
Document No.: 11GG2XH6-2
Date: 2020-03-25

Project name:	SAFEMASS
Report title:	Study of the risks and regulatory issues of specific cases of MASS – Part 1
Customer:	European Maritime Safety Agency (EMSA), Cais do Sodré, 1249-206 LISBOA - Portugal
Customer contact:	Sifis Papageorgiou
Date of issue:	2020-03-25
Project No.:	10165993
Organisation unit:	Safety, Risk & Reliability
Report No.:	2019-1296, Rev. 0
Document No.:	11GG2XH6-2

DNV GL AS Maritime
Safety, Risk & Reliability
Veritasveien 1
1363 Høvik
Norway
Tel: +4767579900

Applicable contract(s) governing the provision of this Report: Contract Number 2019/EMSA/OP/4/2019

Abstract:

The overall objective of SAFEMASS is to identify emerging risks and regulatory gaps that are posed by the implementation of the different degrees of MASS. The intention is to provide meaningful input to the EU Member States and the European Commission, and possibly IMO.

Part 1 (out of 2) addresses emerging risks associated with low manning levels and longer periods with unmanned bridge on three different types of vessels designed to operate with a A3-B1 level of autonomy and control. The study includes a hazard identification (HAZID), fault tree analysis (FTA), review of regulatory challenges, and a set of recommended risk control options (RCO) and measures (RCM).

The information and views set out in this study are those of the author(s) and do not necessarily reflect the official opinion of EMSA. EMSA does not guarantee the accuracy of the data included in this study. Neither EMSA nor any person acting on EMSA's behalf may be held responsible for the use which may be made of the information contained therein.

Prepared by:

Øie, Sondre
Digitally signed by Øie, Sondre
Date: 2020.03.25 17:35:28 +01'00'

Sondre Øie
Principal Consultant

Norstein, Erlend
Digitally signed by Norstein, Erlend
Date: 2020.03.25 19:12:32 +01'00'

Erlend Norstein
Consultant

Johnsrud, Hans Jørgen
Digitalt signert av Johnsrud, Hans Jørgen
Dato: 2020.03.25 17:51:15 +01'00'

Hans Jørgen Johnsrud
Senior Consultant

Julie Huth Lindberg
Digitally signed by Julie Huth Lindberg
Date: 2020.03.25 22:02:35 +01'00'

Julie Lindberg Huth
Intern

Verified by:

Engelhardtsen, Øystein
Digitally signed by Engelhardtsen, Øystein
Date: 2020.03.25 19:42:51 +01'00'

Øystein Engelhardtsen
Senior Researcher

Approved by:

Hoffmann, Peter Nyegaard
Digitally signed by Hoffmann, Peter Nyegaard
Date: 2020.03.25 18:29:44 +01'00'

Peter Hoffmann
Head of Section Safety Risk & Reliability

DNV GL Distribution:

☐ OPEN. Unrestricted distribution, internal and external.

☒ INTERNAL use only. Internal DNV GL document.

☐ CONFIDENTIAL. Distribution within DNV GL according to applicable contract*

☐ SECRET. Authorized access only.

Keywords:
Maritime Autonomous Surface Ships, MASS, reduced manning, hazard, safety, risk, risk, analysis, risk control options, HAZID, fault tree analysis, human element, human/machine interface, automation, situation awareness, mode confusion

Document history

Rev. No.	Date	Reason for Issue	Prepared by	Verified by	Approved by
A	2019-12-03	First draft issued for review	SONDO	OYSTE	
B	2020-02-06	Final draft issued for review	SONDO	OYSTE	
0	2020-03-25	Final report	SONDO	OYSTE	PHOFF

Table of contents

List of figures

List of tables

EXECUTIVE SUMMARY

This report documents Part 1 of the SAFEMASS study and addresses emerging risks associated with the A3-B1 level of autonomy and control, as submitted to IMO's Maritime Safety Committee (MSC) 100/5/6. This definition of a Maritime Autonomous Surface Ship (MASS) includes the use of a high automation level combined with qualified operators onboard. MASS designed accordingly have the potential to be operated with lower manning levels compared to conventional vessels and introduces the possibility of having a periodically unmanned bridge. In this study it also excludes monitoring and control from a remote location, such as a control centre located onshore.

For Part 1 of SAFEMASS, risks emerging from "human-in-the-loop" related issues, and the potential need for increased system redundancy and reliability, were of particular interest.

As a basis for risk analysis, descriptions of three different vessel types designed and operated according to the A3-B1 MASS category were developed. This included a short route domestic passenger ship, a short-sea cargo ship, and an ocean-going cargo ship. A set of automated functions were selected from the ship concept descriptions and included as items to be studied in a hazard identification (HAZID) process. The functions included descriptions of boundaries for when the MASS transitioned from a normal operational state to an abnormal state, or further into a safe(r) state referred to as a "Minimum Risk Condition" (MRC). By combining descriptions of boundary conditions with the tasks required by the operator in response to such events, it was possible to perform a structured HAZID in accordance with the study's problem definition.

A team of industry experts participated in a two-day workshop to discuss and identify hazards associated with the three different A3-B1 MASS concepts. This resulted in a list of hazards used as a basis for constructing fault tree analysis (FTA) models suitable for further examination of the causal relationship between events in two selected accident scenarios:

- Collision between MASS and another vessel
- Capsize and sinking of MASS during voyage

The study identified several emerging risks associated with the A3-B1 MASS category's impact on the MASS operators' situational awareness (SA), as well as hazards associated with mode confusion and (dis-)trust in automation. A two-part summary of what were considered the main risks is outlined in the following sections. The first part addresses risks which could threaten successful intervention by the operator when having to respond to a critical navigation or stability related incident. The second part addresses risks related to dealing with failures which could potentially initiate such incidents if not dealt with or dealt with incorrectly.

For the operator to successfully intervene in case of a critical failure or hazardous event (e.g. vessel on collision course), he or she relies on the MASS system providing cues (in due time) about when responses are required. This phase of the response is particularly vulnerable in case the operator is located elsewhere than the bridge. Potential risks include:

- Boundary parameters and MRCs have not been pre-defined or are incorrectly defined. In such cases notifications or alarms will not be generated by the system, or they are communicated incorrectly (e.g. too late).
- Alarms on portable device are not perceived by the operator, e.g. due to noisy environments, poor alarm design.

- The portable or local alarm device fails, e.g. malfunctions or runs out of battery.
- The operator does not carry or have the portable alarm device readily available.

Next, if successfully informed, the operator must (re-)locate him-/herself to the bridge or other location where the controls and information displays are available. This can fail if:

- The operator(s) intentionally does not muster to bridge due to;
    - overreliance on the MASS system automation due to having frequently observed successful performance in similar situations, or
    - prioritizing other tasks due to high workload and/ or perceived importance and criticality of tasks.
- The operator(s) unintentionally does not muster to the bridge, or musters too late, due to;
    - being located too far away from the bridge, or in a location which is time consuming to leave from (e.g. a tank), or
    - vulnerability associated with low manning level and not being able to be a back-up resource, e.g. the operator off-duty is asleep or sick, while the operator on-duty fails to observe and/ or respond to the alarm.

If the operator is able to muster to the bridge, he or she must obtain the required situational awareness (SA) within the time available before it is too late to act on the notified or alarmed event. Threats against SA can be that the design of human-machine interfaces (HMI) and other displays does not support (rapid) acquisition and analysis. This can prevent the operator from fully entering the "automation loop" in ways which support informed decision making.

Based on his or hers SA, the operator must know how and when to respond, and have the necessary skills to do so. In this process, automation can introduce the following hazards:

- Decision-making is impaired by various stressors, e.g. due to perceived criticality and limited available time.
- Operator skillset deteriorate over time due to high level of automation/ infrequent manual control, particularly of demanding operations.
- In lack of sufficient training and experience, the operator (incorrectly) omits to take action due to placing more reliance and trust in automation over own skillset.
- Opposite to the above, mode confusion or distrust in automation causes the operator to (incorrectly) overriding successful MASS system performance.

As argued above, the A3-B1 level of autonomy and control appear to introduce some emerging risks associated with the operators' role in having to assist the MASS when it exceeds operational boundaries and enter emergency-like states. It also seems, however, that it brings with it risks associated with failures during normal operations which could contribute to such events being initiated. This became particularly evident when examining the fault tree model for loss of stability and buoyancy.

In principle, an A3-B1 MASS can be a highly reliable system, by use of advanced automation and redundant functions. The same characteristics can however potentially introduce some new, emerging risks largely driven by increased system complexity:

- In case component reliability is weakened, an increased number of sensors and instrumented functions can have the potential to produce a large amount of notifications and alarms for the MASS operator to deal with. This can cause alarm fatigue.
- Isolated each of the individual alarms may not be perceived as critical and can possibly be ignored or acknowledged without any corrective actions. This tendency can be amplified by factors such as low manning/ high workload. Another factor which could influence the MASS operators to ignore alarms is the commercial pressures to leave port or maintain voyage speed.
- Not fully investigating the cause of the alarm, the MASS operator may not have a complete understanding of the vessel's condition.
- Because the alarms can be produced (and ignored) both when being docked or during transit, and are produced from different systems, it may be difficult for the MASS operator interpret how a combination of failures can be critical.

As a result, the MASS could potentially operate with several *latent failures* in the system, such as sub-optimal selection of sailing route or a damaged cargo hatch. Although seemingly uncritical when isolated, an accident can occur when the MASS is exposed to other hazards at a later stage. Sailing with impaired watertight integrity of the cargo hold can become critical when green seas are flowing on deck during storms encountered due to poor voyage planning.

A set of risk control measures (RCMs) were developed for the models' basic events to demonstrate and suggest risk-reduction effects. The RCMs were grouped into four different RCO categories (see below). Please note that the numbering of RCOs does not reflect an order of priority. Also note that the RCM described here only are summaries and extracts. A complete list and additional details can be found in the main body of the report.

RCO #1

RCO #1 includes RCMs intended to ensure robust communication between MASS and other vessels. Although communication by itself will not solely prevent a collision, it can help to avoid that the vessels involved end up in a situation which require challenging navigational manoeuvres. It is therefore recommended that communication is made robust by providing solutions in other locations than the bridge allowing the MASS operators:

- to listen in on on-going and previous communication,
- to view basic navigational information,
- being notified about communication being initiated between MASS and other vessels, and,
- being alerted about unsuccessful communication or failures in communication system on a portable alarm device.

As an additional safeguard, MRCs should be defined for what is to be considered as failed communication.

RCO #2

RCO #2 is to ensure that MASS operator(s) are capable of mustering at the bridge when required. As indicated above, the MASS operators are for this purpose equipped with a portable alarm device which presents warnings and alarms, together with key information (alarm text). The availability and reliability of such a device should be made certain through:

- Routines and procedures implemented for how to use the device, incl. when to carry it.
- Means for securing the device to the work wear (e.g. boiler suit).
- For all expected working conditions;
  - Sufficient visual and audio signal,
  - High quality, user-friendliness and sufficient IP rating,
  - Strong signals in all areas visited by operators,
- Notifying off-duty operator in case on-duty operator's alarm is not acknowledged.
- Automatically adjust the time the notifications and alarms are issued depending on how far away from the bridge (or other control station) the operator is located.
- Provide a clear and unambiguous indication of the alarm's criticality level.

In addition to the alarm device, RCO #2 includes RCMs aimed at more operational aspects such as:

- When to muster, be in proximity of, or present at the bridge.
- Contingencies which ensure presence on bridge in case 1 out of 2 MASS operators (within a department) are indisposed.

RCO #3

RCO #3 includes RCMs aimed at ensuring that task unfamiliarity and complexity introduced with high levels of automation does not impair human performance. If not managed, such factors can cause the operators to overly trust or distrust decisions made by the system, or cause confusion regarding the MASS operational modes (so-called "mode confusion").

Recommended RCMs are:

- Providing the MASS operators with sufficient training in MASS system automation, incl.:
  - The ability to perform system diagnostics in time critical situations.
  - Build knowledge about MASS system reliability and failure prevention/ mitigation.
- Human-machine interfaces (HMI) and automation being designed according to principles of "closed loop dynamics", i.e. include operator in the loop by interaction with automation and information flows creating situational awareness.
- HMI, other control panels and communication equipment should in general be designed with a high degree of usability to allow easy information acquisition and control possibilities in time critical situations.
- Provide the MASS operator with an opportunity to demand that the vessel enters an MRC in case he or she is uncertain of/ distrusts the outcome from automated actions.

RCO #4

RCO #4 captures the RCMs identified to ensure sufficient levels of system redundancy and reliability in MASS design and operations. These include:

- The automated navigation system should be verified to fully comply with the navigational parts of COLREG, including Rule 2, 8 and 17.
- The automated navigation system should automatically be monitored for failures and sub-par performance.
- The MASS system should be able to perform crosschecks by comparing weighted input from different types of sensors in order to determine accuracy of measured data.
- The MASS system should be capable of performing self-check and diagnostics functions as means to detect failures in e.g. sensors.
- Sub-systems should report status to a master-system which keeps track of the aggregated state of the vessel (including all relevant sub-systems) and initiates transition to a minimum risk condition (MRC) when needed.
- The MASS should at all times have the possibility to enter at least one pre-defined minimum risk condition (MRC) in the case of significant equipment failures; being exposed to external hazards, or; omitted response by the MASS operator within pre-defined time criteria.
- The system responsible for taking the MASS into an MRC should be independent and segregated from the MASS primary navigational system.

For Part 1 of SAFEMAS, a review of relevant regulations was also performed to identify and discuss challenges associated with the A3-B1 MASS category's possibility to comply with existing rules. The main identified challenges that will pose compliance issues to the A3-B1 MASS are found in the replacement of continuous monitoring by introducing high levels of automation. Both COLREG, STCW and SOLAS cover regulations that require a constant physical presence on the navigation bridge. The following four regulations are therefore identified as to prevent A3-B1 operation:

- COLREG 72, Pt. A, Rule 2, Responsibility
- COLREG 72, Pt B, Sec. I, Rule 5, Look-out
- STCW Convention VIII/2 Watchkeeping arrangements and principles to be observed
- SOLAS Ch. V/14 Ship's manning

In conclusion, the study suggest that potential "ironies of automation"- pitfalls should be avoided and that existing Levels of Automation (LoA) models should be revised to be better suited for use in system engineering. Future efforts made to increase automation should adopt principles of human-centred design and apply established Human Factors Engineering techniques and standards. Due to the inherent complexity of MASS design and operations, system designers should avoid addressing automation at a ship level using overly simplistic LoA models. Instead automation should be considered at a task and system function level, supported by definitions and models which allow more nuanced evaluations of joint human-system interactions. Such an approach is arguably better suited for determining the MASS system’s and operators’ roles and responsibilities in execution of functions across various operational modes.

ACRONYMS

AIS	Automatic identification system
CPA	Closest point of approach
COLREG	The International Regulations for Preventing Collisions at Sea
ECDIS	Electronic chart display and information system
EMSA	European Maritime Safety Agency
ENC	Electronic Navigational Charts
FSA	Formal Safety Assessment
FTA	Fault tree analysis
HAZID	Hazard identification
HMI	Human-machine interface
IALA	International Association of Marine Aids to Navigation and Lighthouse Authorities
IHO	International Hydrographic Organization
IMO	International Maritime Organization
LNG	Liquified natural gas
MARPOL	The International Convention for the Prevention of Pollution from Ships
MASS	Maritime Autonomous Surface Ships
MRC	Minimum Risk Condition
MSC	IMO’s Maritime Safety Committee
RCM	Risk control measure
RCO	Risk control option
RPM	Revolutions per minute
SOLAS	The International Convention for the Safety of Life at Sea
SOPEP	The Shipboard Oil Pollution Emergency Plan
STCW	International Convention on Standards of Training, Certification and Watchkeeping for Seafarers
TCPA	Time to closest point of approach

DEFINITIONS

Anticipated failure

Failure expected to occur (e.g. >once a year) that should not prevent normal operation of the vessel.

A3-B1

Vessel with an A3 level of autonomy (autonomous) and qualified operators onboard.

Bridge/deck operator

See Operator.

Common Cause Failure

Two or more items fail within a specified time such that the success of the system mission would be uncertain.

(In) control

Carrying out actions which have a direct impact on the performance of system functions.

Emerging risks

New risks or an increase in existing risks due to the introduction of (here) A3-B1 level of autonomy and control.

Engine operator

See Operator.

Maritime autonomous surface ship (MASS)

In this report MASS always refers to a vessel designed according to the A3-B1 level of autonomy and control.

Master operator

The operator on board that has the overall responsibility for the ship.

Minimum risk condition

A minimum risk condition (MRC) is a state that the ship should enter when the auto remote infrastructure experiences situations that are outside those in which it can operate normally, but is still expected to handle with an acceptable level of risk /6/.

Mode confusion

Mode confusion occurs when the crew believes they are in a mode different than the one they are actually in and consequently make inappropriate requests or responses to the automation /16/.

Operator

Human operator who is onboard the MASS, responsible for the supervision, monitoring and control of either bridge/deck functions (Bridge Operator) or engine functions (Engine Operator). Also referred to as MASS Operator. Bridge Operator can fulfil the role as Master Operator (see Master Operator).

Situational awareness

The perception of environmental elements and events with respect to time or space, the comprehension of their meaning, and the projection of their future status /9/.

Supervision

Periodically or continuously, overseeing the operation of a system and standing by to intervene in case the operation is deemed not to be safe or not according to operational goals or limitations.

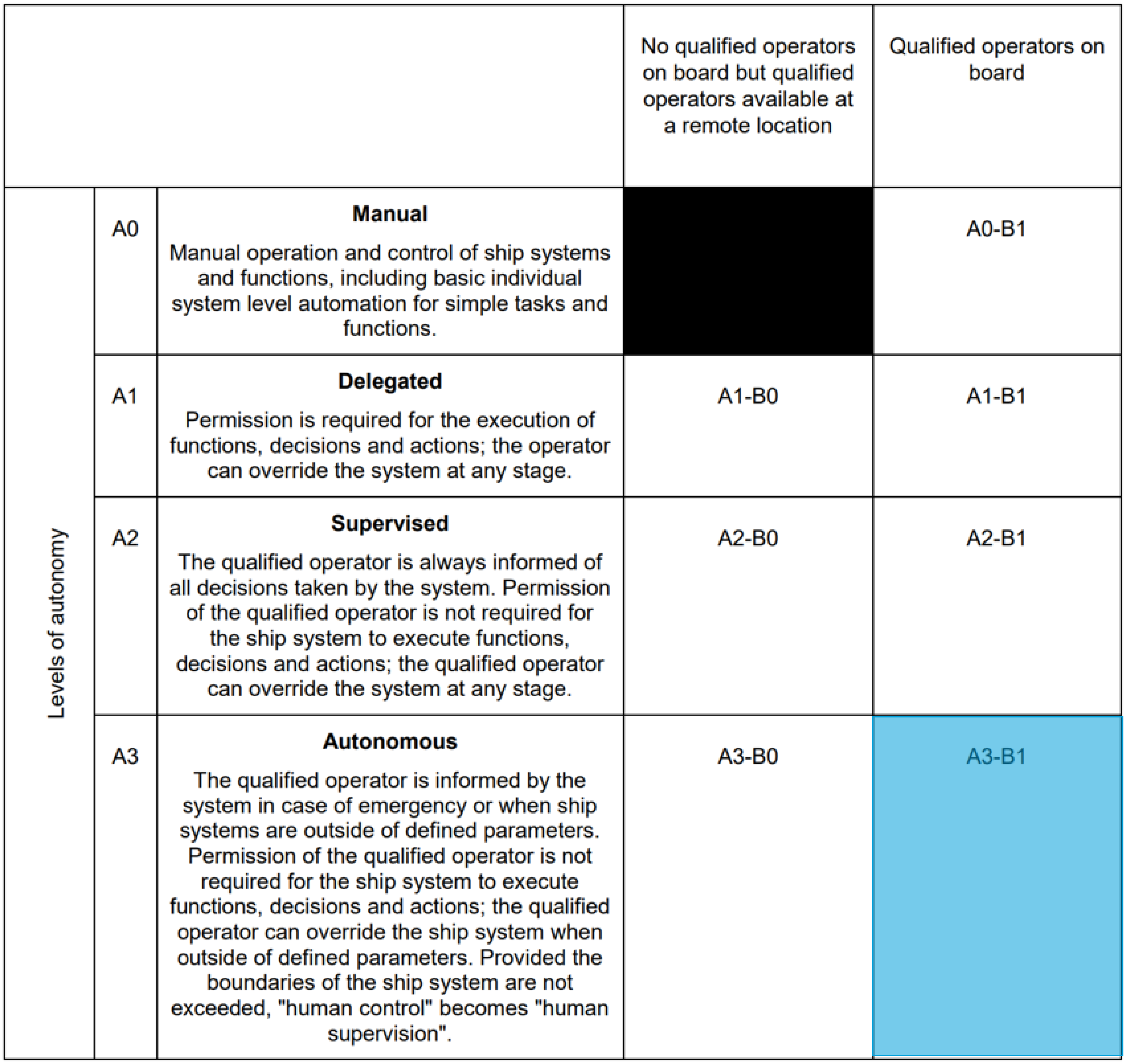
Trust (in automation)

The attitude that an agent will help achieve an individual’s goals in a situation characterized by uncertainty and vulnerability /11/.

1 PROBLEM DEFINITION

Part 1 of the SAFEMASS study addresses emerging risks associated with low manning levels and longer periods with an unmanned bridge on three different types of vessels designed to operate with an A3-B1 level of autonomy and control (see Table 1). This definition of autonomy levels was submitted to IMO's Maritime Safety Committee (MSC) 100/5/6 by Australia, Denmark, Finland, France and Turkey.

Table 1 - MSC 100/5/6 proposal for level of autonomy and control



			No qualified operators on board but qualified operators available at a remote location	Qualified operators on board
Levels of autonomy	A0	**Manual** Manual operation and control of ship systems and functions, including basic individual system level automation for simple tasks and functions.	■	A0-B1
	A1	**Delegated** Permission is required for the execution of functions, decisions and actions; the operator can override the system at any stage.	A1-B0	A1-B1
	A2	**Supervised** The qualified operator is always informed of all decisions taken by the system. Permission of the qualified operator is not required for the ship system to execute functions, decisions and actions; the qualified operator can override the system at any stage.	A2-B0	A2-B1
	A3	**Autonomous** The qualified operator is informed by the system in case of emergency or when ship systems are outside of defined parameters. Permission of the qualified operator is not required for the ship system to execute functions, decisions and actions; the qualified operator can override the ship system when outside of defined parameters. Provided the boundaries of the ship system are not exceeded, "human control" becomes "human supervision".	A3-B0	A3-B1

As an extension of this problem definition, the need for human intervention and system redundancy is investigated for cases where the automation system exceeds its pre-defined parameters for what constitutes its operational boundaries. This includes examining human element related issues related to the transitions of the human role in and out of the automation loop. One of the tasks in Part 1 is also to summarize issues regarding compliance with SOLAS /1/, STCW /2/, MARPOL /3/ and COLREG /4/ based on the findings from investigating emerging risks associated with the A3-B1 category of MASS. The study proposes a set of *risk control options* (RCOs) and measures (RCMs) and solutions for how to address risks emerging from applying the A3-B1 MASS category to ship concepts.

2 BACKGROUND INFORMATION

Recent investigations on Maritime Autonomous Surface Ships (MASS) has demonstrated a broad impact on all aspects of shipping. It affects not only pure technical issues like reliability, but it also influences aspects associated with social (working conditions and potential passengers' comfort) and legal dimensions. There are currently several ongoing IMO activities with the aim to identify the need for amending IMO provisions, which allow for the operation of ships with a higher degree of automation. It is essential to identify changes in risks of ship operation, either increase of existing risks or additional risks emerging from increased automation.

On this background, EMSA has initiated the SAFEMASS study, as an effort to fill in recognised knowledge gaps and develop recommendations for amending IMO regulatory frameworks in order to meet the safety expectations.

When studying MASS at a conceptual stage, it is DNV GL opinion that it is important not to limit the capability to what is seen feasible today, but at the same time not be too futuristic. Reference is made to the discussions in *DNV GL Position Paper: Remote-Controlled and Autonomous Ships* /5/*.* Being too futuristic can invalidate the results and create a sense of unrealism. A balance between feasibility and future opportunities has therefore been strived when developing the study basis. The focus in this study is, therefore, on the feasibility of automation, but without being restricted by accounting for current regulatory restrictions.

The applied approach is partly based on a guideline issued by DNV GL in September 2018, titled *DNVGL-CG-0264 Autonomous and remotely operated ships* /6/. The guideline's overall objective is to provide a framework which ensures that the application of novel concepts and technologies result in a safety level equivalent to- or better than conventional vessel operations.

This guideline recommends a risk-based approach, with an operational and functional focus. It includes processes applicable to develop sample ship descriptions for the A3-B1 category, as well as recommendations for risk analysis.

3 METHOD OF WORK

The study on the A3-B1 combination, i.e. MASS with qualified seafarers onboard and a high level of automation, included the following activities:

- Task 1. a) Provide a description of generic ships and their enablers
- Task 1. b) Perform HAZID of the A3-B1 category of MASS
- Task 1. c) Develop analytical fault tree models
- Task 1. d) Summarize issues regarding compliance with SOLAS, STCW, MARPOL and COLREG
- Task 1.e) Provide risk control options (RCOs) and propose regulatory solutions

More detailed method descriptions are provided in the chapters presenting the results from each activity.

3.1 Meetings and work sessions

The following meetings and work sessions were held:

- **Kick-off meeting**: A kick-off meeting was held at DNV GLs main office at Høvik on the 27th of June, 2019. Participants from DNV GL included a project manager and sponsor, together with experts on autonomous and remote shipping. EMSA was represented by their project officer responsible for following up SAFEMASS. The purpose of the meeting was to clarify objectives and scope and to agree on a schedule for the planned work sessions, meetings and deliverables.
- **Status meetings**: Status meetings have been held bi-weekly or adjusted according to needs and progress. Participants have been DNV GLs project manager and EMSAs project officer. The purpose has been discussing the status and progress of the project. DNV GL has also had (internal) bi-weekly or weekly status meetings with the same purpose.
- **Other internal meetings**: Internal meetings in DNV GL were held to discuss ship descriptions, various analysis (HAZID, fault tree, RCO, etc.) and reporting.
- **HAZID work session**: A HAZID dedicated to collect data for Part 1 of SAFEMASS was held at DNV GLs main office at Høvik on the 11th and 12th of September, 2019. The purpose was to identify and discuss emerging risks as a result of applying A3-B1 level of autonomy and control to the three ship concepts developed in Part 1.
- **EMSA meeting**: DNV GL was invited to present SAFEMASS at EMSAs main office in Lisbon on the 25th of November, 2019. The purpose is to share and discuss the main preliminary results with the administrations from EMSAs member countries and other key stakeholders.

3.2 Expertise involved

DNV GL has established a team of leading experts on topics important for ship automation/autonomy. This team has been supported by experts from industry and maritime administrations. Efforts were made to secure involvement from internal and external people with the following areas of expertise:

- MASS/ remote operations
- Human element/ human factors engineering
- Control systems/ software
- Navigation/ maritime operations
- FSA/ risk analysis methodology
- Maritime safety and risk management
- Rules and regulations

An overview of the SAFEMASS participants' roles and area of expertise, together with which SAFEMASS activities they have been involved in, is provided in Appendix A.

3.3 Limitations

The following limitations apply for this study:

- Efforts have been focused towards identifying issues (i.e. emerging risks) which are significantly different than what is the case for conventional vessels and shipping. This includes addressing the functions and operational modes considered to be the most impacted by automation. One of the implications from this limitation is reflected in how a selected set of hazards identified in the HAZID was subject to further risk analysis.
- The main goal is to identify hazards and analyse the risk associated with the role of the human element in MASS operations. Risks associated with technical aspects are addressed, but primarily to highlight issues related to human performance.
- Due to the lack of data and a high level of uncertainty inherent in the concepts described, no quantification of risk has been performed. Instead, the analysis has been explorative and tried to highlight emerging risks associated with the A3-B1 MASS category qualitatively.
- Future developments in external facilities such as the navigational infrastructure surrounding the MASS may have a significant impact on both operations and presence of risks. Examples can be fairways dedicated for MASS traffic, or support from vessel traffic services. While it is acknowledged that such enablers may exhibit strong influence on the course of future concept developments, elaborating on such details was however considered out of scope for this study. As such, the operational context to a large degree reflect todays current situation.

4 A3-B1 SHIP CONCEPT DESCRIPTIONS (TASK 1. A)

This chapter provides descriptions of three different ship types used as a basis for further hazard identification and risk analysis of the A3-B1 MASS examined in Part 1 of the SAFEMASS study;

- a short route domestic passenger ship,
- a short-sea cargo ship and (no hazardous cargo onboard, no LNG carrier or tanker),
- an ocean-going cargo ship (no hazardous cargo onboard, no LNG carrier or tanker).

The first sub-chapter 4.1 explain what the commonalities are between the A3-B1 vessels, followed by sub-chapters 4.3 to 4.5 which outlines what the specific features are for each of the three different ship types with regards to vessel characteristics operational profile and context.

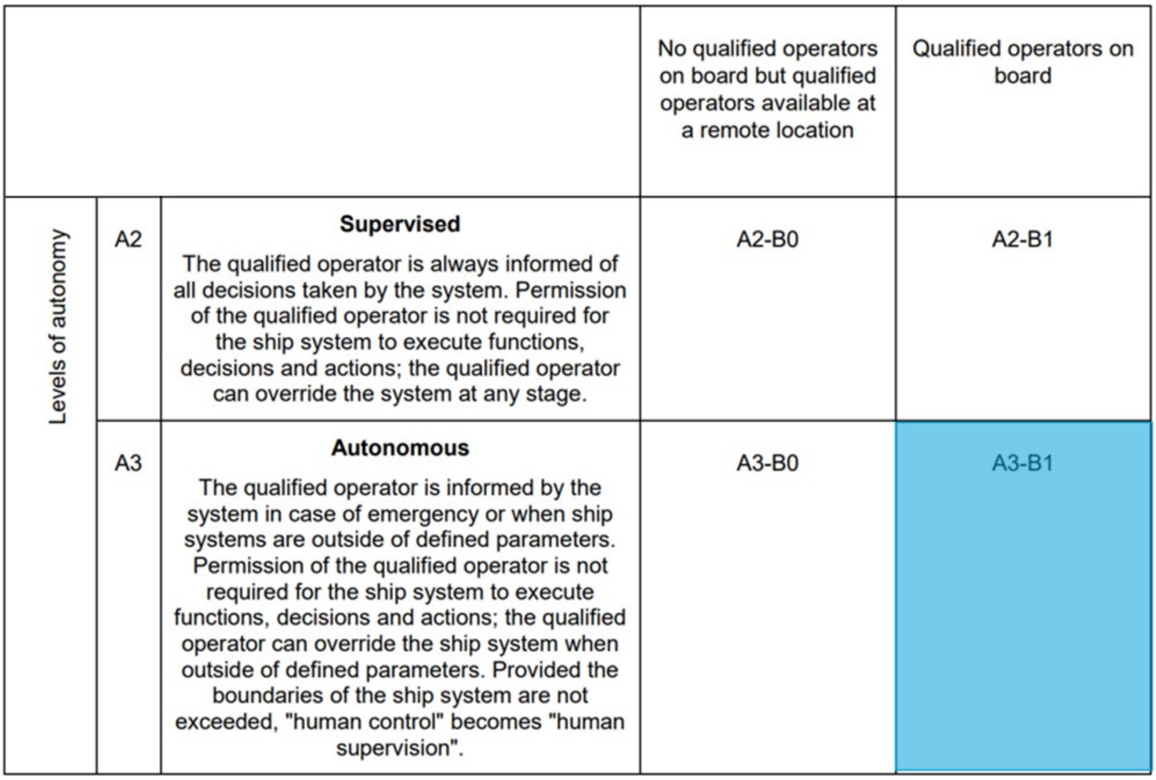
4.1 A3-B1 level of autonomy and control

While the three different ship types included in the A3-B1 study all have specific features, they also have several commonalities which are described in this chapter. First, the principles of "minimum risk conditions" (MRC) and how they are relevant for A3-B1 MASS is explained in chapter 4.1.1. This is further elaborated upon in an interpretation of the A3-B1 level of autonomy and control provided in chapter 4.1.2.

4.1.1 "Minimum risk conditions" applied to the A3-B1 MASS category

The A3-B1 MASS category is defined in Table 2. As can be read, a key aspect of the A3 level is that the operator is informed in case of emergency or when the ship system is outside of defined parameters. This is also when the operator can take control by overriding the ship systems.

Table 2 – A3 and A2 level of autonomy and control as proposed in MSC 100/5/6



			No qualified operators on board but qualified operators available at a remote location	Qualified operators on board
Levels of autonomy	A2	**Supervised** The qualified operator is always informed of all decisions taken by the system. Permission of the qualified operator is not required for the ship system to execute functions, decisions and actions; the qualified operator can override the system at any stage.	A2-B0	A2-B1
	A3	**Autonomous** The qualified operator is informed by the system in case of emergency or when ship systems are outside of defined parameters. Permission of the qualified operator is not required for the ship system to execute functions, decisions and actions; the qualified operator can override the ship system when outside of defined parameters. Provided the boundaries of the ship system are not exceeded, "human control" becomes "human supervision".	A3-B0	A3-B1

To fully grasp the concept behind the A3 level of autonomy, it is in the context of this study considered useful to also have an idea of what is meant by emergencies and defined parameters. One way to do this is by applying the concept of *Minimum Risk Conditions* (MRC) /6/.

MRC provide a framework and set of definitions for how to design and operate a MASS in case of potentially critical disruptions. Events may force the ship or other parts of the autonomous infrastructure out of its normal operational state and push it through an abnormal state and further to MRC-states (see Figure 1). Disruptions can either be caused by changes in the environment (e.g. deteriorating weather) or by failures / incidents (e.g. loss of a propulsion system). In such an event, it is essential that the relevant response is pre-defined, and that the ship is put in a state that poses the least risk to life, environment and property.

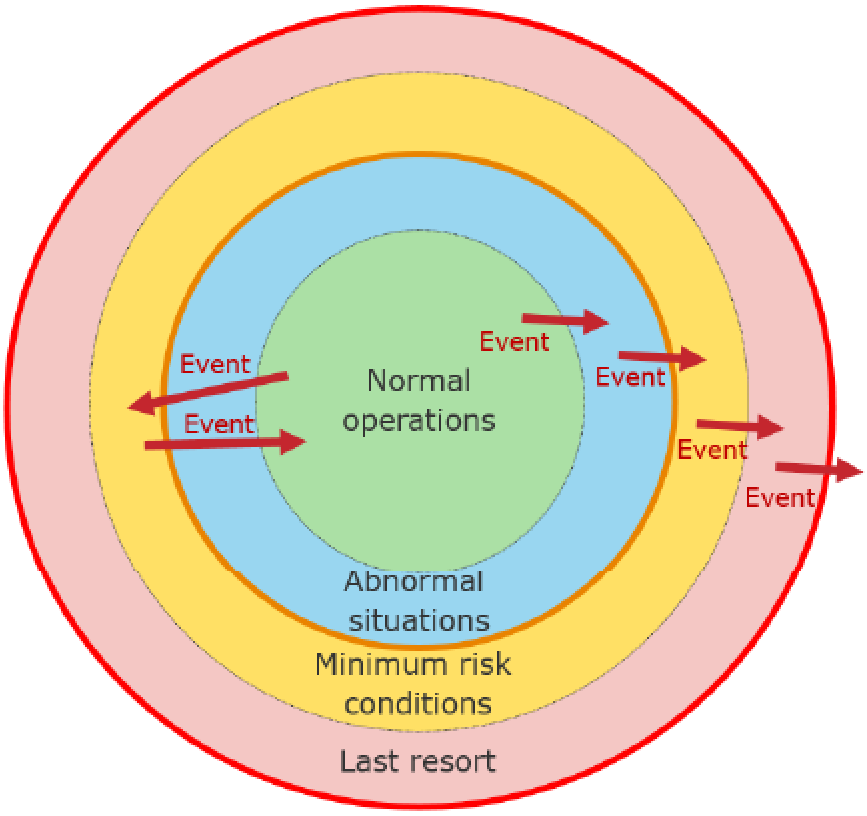


Figure 1 – The concept of normal operations, abnormal situations and MRCs /6/

Most MRCs are considered active states, where the vessel and its important systems remain functional, albeit with (some) reduced capabilities. It is also possible that an event enables the ship to regain normal operation after it has been in an MRC state (e.g. improving weather or restoration of propulsion).

There may be several viable MRCs for a specific event depending on e.g. the vessel's operational status, location, and external conditions. These MRCs should be organised in a hierarchy with clear decision paths between them; i.e. if MRC 1.0 fails or cannot be entered, go to MRC 1.1 etc. The MRCs for which there are no other viable MRCs in case of further disruptions, are referred to as last resort MRCs. If a specific MRC cannot be sustained for an indefinite period of time, it is normally not accepted as a last resort MRC.

Examples of MRCs are:

1) Stay moored at quay
2) Move away from quay and other vessels
3) "Limp home" (sail to a safe location with reduced capabilities)
4) Move as slowly as possible/ necessary
5) Navigate to next waypoint and stop there
6) Call for assistance (e.g. tug)
7) Drop emergency anchor

8) Controlled beaching

9) Keep position (two variants);

    a. If moving, stop and keep position

    b. If stationary, stay at current position

10) Abort ongoing operation (e.g. hoisting, fuelling, loading, charging)

Which MRC to enter in case of a disrupting event may be decided in real-time during the operation/ voyage. When navigating waters that are congested or have high traffic, it is expected that the vessel has at least two MRCs available at any time during normal operations.

External hazards, failures or incidents considered potential should not force the vessel outside of last resort MRC. Anticipated events, such as equipment failures expected to occur more than once every year, should not force the vessel into an MRC. Instead the design should allow the vessel to maintain normal operation or to handle abnormal situations.

Based on the concept of MRC, the following design principles have been suggested /6/:

1) *Maintain safe state*. It should be possible to enter and maintain an MRC in all operations and scenarios defined in the Concept of Operation (ConOps) /6/.

2) *Maintain normal operation*. As mentioned above, *anticipated failures* should not prevent what is considered normal operation of the vessel. The capability to maintain safe state (within MRC) should not be based only on fail-to-safe properties of a single system or component. Instead, any single failure or incident should be mitigated by applying redundancy principles (e.g. two steering systems) or alternative control capabilities (e.g. loss of collision avoidance is mitigated by position keeping).

How MRC applies to the A3-B1 MASS category is further elaborated in the sub-chapter below.

Additional information about how to apply the concept of MRCs can be found in DNV GL's *Class Guideline DNVGL-CG-0264 Autonomous and remotely operated ships* /6/.

4.1.2 Interpretation of the A3-B1 level of autonomy and control

To better understand the practical implications of applying the A3-B1 MASS category to the concepts in this study, the definition was broken down and interpreted as described in the following sections.

It is assumed that the various levels can be interpreted based on what distinguishes them from the next level up, or for the case of A3-B1, the next level down. As such, the interpretation is to a large degree driven by how it compares to the A2 level.

Having the principles of MRCs in mind, the following interpretations and assumptions were made about the A3-B1 level of autonomy and control:

"***The qualified operator is informed by the system in case of emergency or when ship systems are outside of defined parameters […]***"; Compared to the A2 level where the operator is always informed about the decisions taken by the system, the A3 level informs the operator in case of emergencies or when the system is outside defined parameters. Based on this comparison, the following assumptions have been made regarding the A3-B1 category:

- Emergencies and boundaries for operational parameters are pre-defined as part of the design and concept of operations (to the extent possible). This includes ensuring that functions, either fully automated or performed jointly by MASS and operator(s), is capable of either restoring normal operations or enter an MRC in case abnormal situations should occur. It also assumes that the MASS system is aware of its own limitations, i.e. can recognize a situation that is outside its *defined parameters* and that the safest alternative is to involve the operator(s) and/or enter an MRC.
- MASS performance is reliable to the extent where the operators are not expected to actively monitor the external surroundings or the status of any functions while the vessel is operating inside its *normal operational state* as illustrated in Figure 1. I.e. operators do not monitor leading indicators (e.g. trends, patterns) related to system performance or traffic unless notified to do so.
- Alarms or other ways of notification are only provided to the operator in case the MASS detects that one or more of its autonomous functions are degraded, or if it is recognizing that it is in a situation where its safety or security is threatened by external factors beyond what it is capable of handling (i.e. capability of maintaining normal operations).

"***Permission of the qualified operator is not required for the ship system to execute functions, decisions and actions***"; This part of the definition is identical to what is stated for the A2 level. For the A3 level the following assumptions have been made:

- While the operator is informed in case of emergencies or operating outside its normal operational window, the MASS will still make decisions and attempt to take actions in cases where the operator does not intervene.
- Operator intervention is primarily intended to support the vessel in either;
    - safely regaining normal operations in cases where limitations in MASS capabilities by design forces it to enter an MRC, or
    - safely enter an MRC in cases where MASS capabilities are limited by design or autonomous functions have failed or been degraded.

"***The operator can override the ship system when outside defined parameters***"; In the A2 level, the qualified operator can override the system at any stage, i.e. also when operating inside its normal operational state. For the A3 level, it is therefore assumed that the operator does not have the opportunity to override the system when operating inside its normal operational state. Attempting to do so will represent a violation and not intended by design.

"***Provided the boundaries of the ship system are not exceeded, "human control" becomes "human supervision"***"; There is no similar phrase in the A2 level definition. The sentence is interpreted to summarize the assumptions made above. It again indicates that operator involvement is not required for normal operations and that the role of the operator is limited to *supervision*. Because of the assumption that the operator is primarily informed when the ship is about to or has entered an abnormal state, supervision is interpreted to mean that the operator shall be available to respond to notifications and alarms. One example could be presence on or close to the bridge in areas with high traffic density or if passing through areas considered challenging for safe navigation.

"Qualified operators on board"; The operators onboard are qualified according to the STCW requirements which provides a uniform standard for all maritime competence. Hence, they have certified maritime competence equal to crew on vessels of similar size and power generation in the same sea area. Furthermore, the additional competence needed for the specific ship type is provided by the management company as required by the ISM Code.

4.2 Identification and breakdown of generic A3-B1 functions

Being able to identify risks emerging as a result of adopting the A3-B1 level of autonomy and control requires that the functions expected to be performed by the MASS are identified. The following sub-chapters provides a description of *generic* functions expected to be affected by automation, together with a set of assumptions considered to be applicable for all three ship types.

The first step in this process is to perform a function analysis by breaking down (decomposing) the MASS main functions into a hierarchy of sub-functions. This function hierarchy (or "tree") helps to define further how the A3-B1 operational concepts are enabled, but without having to provide comprehensive and detailed descriptions of the required technology.

Logically, the function breakdown is done by asking "how" the main functions will be achieved, as illustrated in Figure 2. Oppositely, the justification for the identified sub-functions or tasks can be found by asking "why" they are required.

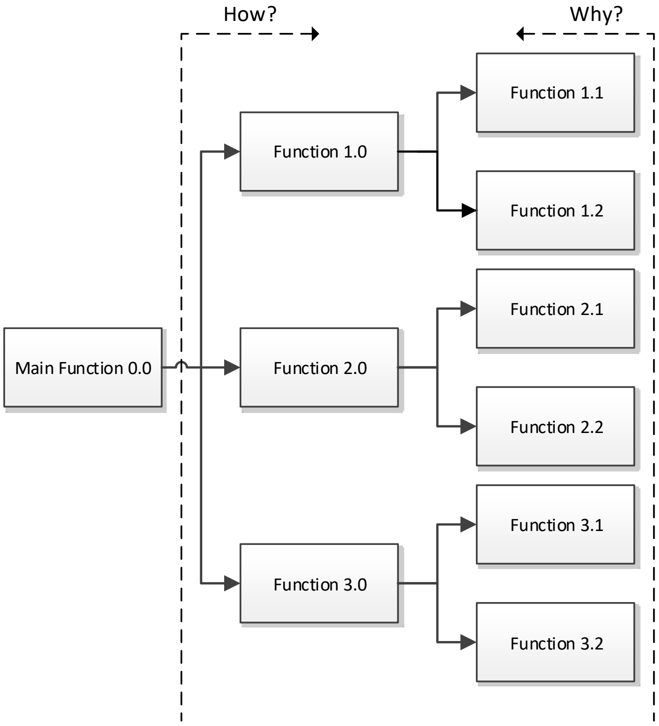


Figure 2 – The "how" and "why" logic behind function hierarchies

A generic function tree was developed which included a complete list of functions expected to be performed by the study's three different types of A3-B1 MASS. The main functions are listed in Figure 3, while the next level of sub-functions is described in the following subsequent chapters. As requested by EMSA, for Part 1, the functions associated with the following operational goals should be examined:

- Navigation;
- Mooring;
- Loading/ unloading;
- Engine room/ equipment monitoring;
- Maintenance.

The complete function tree was distributed to the HAZID workshop participants prior to the meeting, as a tool for them to better understand the MASS capabilities. Please note, however, that due to constraints in the reporting format (i.e. space) only figures showing the first level of sub-functions are included.

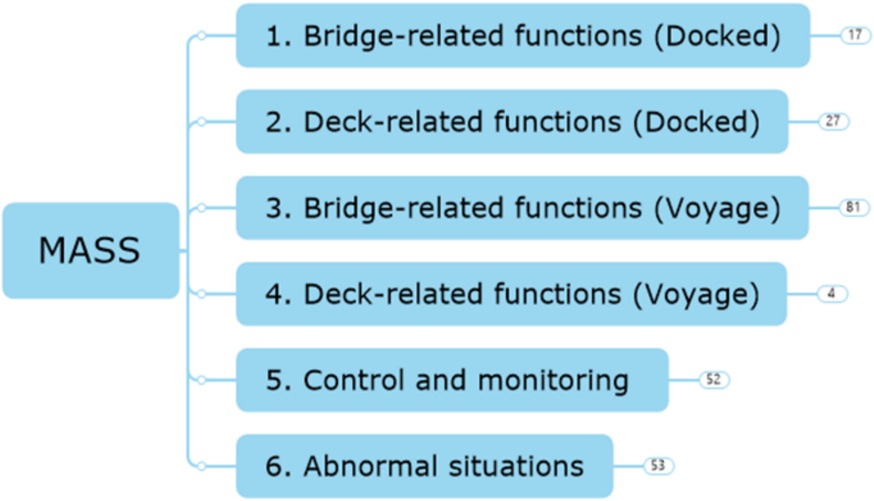

MASS
1. Bridge-related functions (Docked)
17
2. Deck-related functions (Docked)
27
3. Bridge-related functions (Voyage)
81
4. Deck-related functions (Voyage)
4
5. Control and monitoring
52
6. Abnormal situations
53

Figure 3 – Main functions performed by MASS

At the main function level, various sub-functions were categorized as being part of the Bridge, Deck or Engine department's operational goals. While the functions for Bridge and Deck varies highly depending on when the vessel is in voyage or docked, the engine department on a MASS was more similar. For this reason, the Bridge/Deck functions were divided into Docked and Voyage mode, while all engine-related functions were grouped under the main function "Control and monitoring". Furthermore, functions related to contingency and emergency response was grouped under the function "Abnormal situation".

When the function tree was considered to include a near complete list of functions, the next step was to select which functions were considered the most relevant to be included in further risk analyses. These are marked with blue in the figures below showing extracts from the function tree. This selection was based on a combination of two criteria, *criticality* and their potential to introduce *emerging risks* of ship operation. Emerging risks were defined as either as an increase of existing risks, or new risks stemming from increased use of automation. Criticality was defined as cases where loss, degradation or incorrect execution of a function could contribute to either initiate or fail to prevent an accident defined as *an unintended event involving fatality, injury, ship loss or damage, other property loss or damage, or environmental damage* /7/.

Please note that the HAZID discussions were not limited to only concern the sub-functions initially included as study nodes. In case discussions about other related sub-functions emerged, these were recorded in the HAZID log (see Appendix B).

4.2.1 Bridge-related functions

Figure 4 illustrates the highest level of Bridge sub-functions. A total of 9 sub-functions were identified in the function tree. Of these, 4 were related to docked operation while 5 concerned the vessel in voyage. Due to practical limitations of the study it was only possible to address a selected set of functions found to be the most affected by implications from introducing the A3-B1 MASS category. On this basis, the following subfunctions were discussed in the HAZID workshop: Voyage planning, Trim, Stability & Stress, Harbour manoeuvring and Navigation & Manoeuvring during transit.

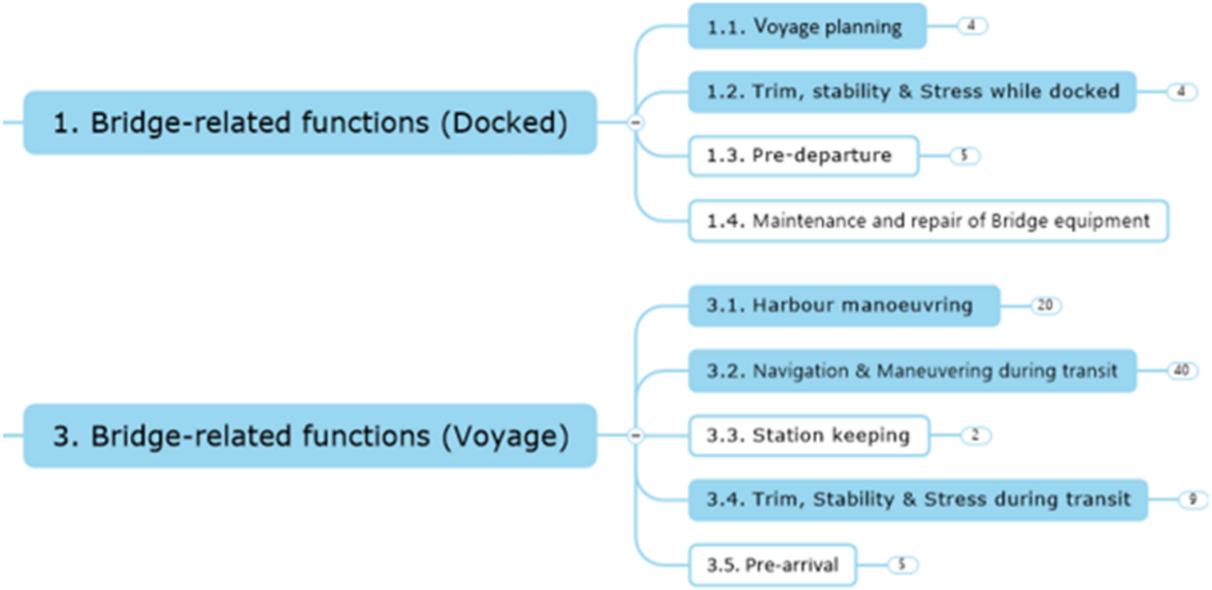

1. Bridge-related functions (Docked)
1.1. Voyage planning
4
1.2. Trim, stability & Stress while docked
4
1.3. Pre-departure
5
1.4. Maintenance and repair of Bridge equipment
3. Bridge-related functions (Voyage)
3.1. Harbour manoeuvring
20
3.2. Navigation & Maneuvering during transit
40
3.3. Station keeping
2
3.4. Trim, Stability & Stress during transit
9
3.5. Pre-arrival
5

Figure 4 – Breakdown of Bridge-related functions.

A feature common for all ship types is the station keeping ability (function 3.3) for which the following assumptions were made:

- While the passenger ferry is equipped with azimuth thrusters, both the short and ocean-going cargo ship is utilizing conventional screw propeller with rudder, assisted by a bow thruster. Still, it is assumed that all three ships are capable of docking autonomously to some degree.
- Likewise, it is assumed that the autonomous system can provide the same manoeuvrability as if manoeuvred by humans. Consequently, the vessels can maintain station-keeping by adjusting the heading towards the wind or current and adjust the revolutions per minute (RPM) of the main propeller and bow thruster. This type of station keeping must not be confused with a higher degree of Dynamic Position (DP) system, which often is used in the offshore industry.

All three ship types share the same functionality regarding navigation and manoeuvring during transit (function 3.2). For this function the following assumptions were made:

- All ships are equipped with an autonomous navigation system capable of adhering to COLREG within its normal operational state.
- The navigation system is able to autonomously manage most navigational challenges such as high traffic density scenarios.
- During more critical phases the operators are present at the bridge to quickly intervene in case the vessel is approaching or operates outside pre-defined parameters. In these situations, the system will notify the watchkeeping personnel and request assistance. See also section 4.1.2.
- The MASS operator is informed via a portable alarm device about failures in ongoing communication between MASS and other vessels, or in case of failures in the communication equipment.
- Portable communication devices are available at strategic locations on the vessel. The device will provide some basic information regarding the event. However, more detailed information related to the event is only available on the bridge.

4.2.2 Deck-related functions

The highest level of Deck sub-functions is illustrated in Figure 5. In total, 11 sub-functions were identified. Of these, 8 was related to harbour activities and only 3 related to voyage.

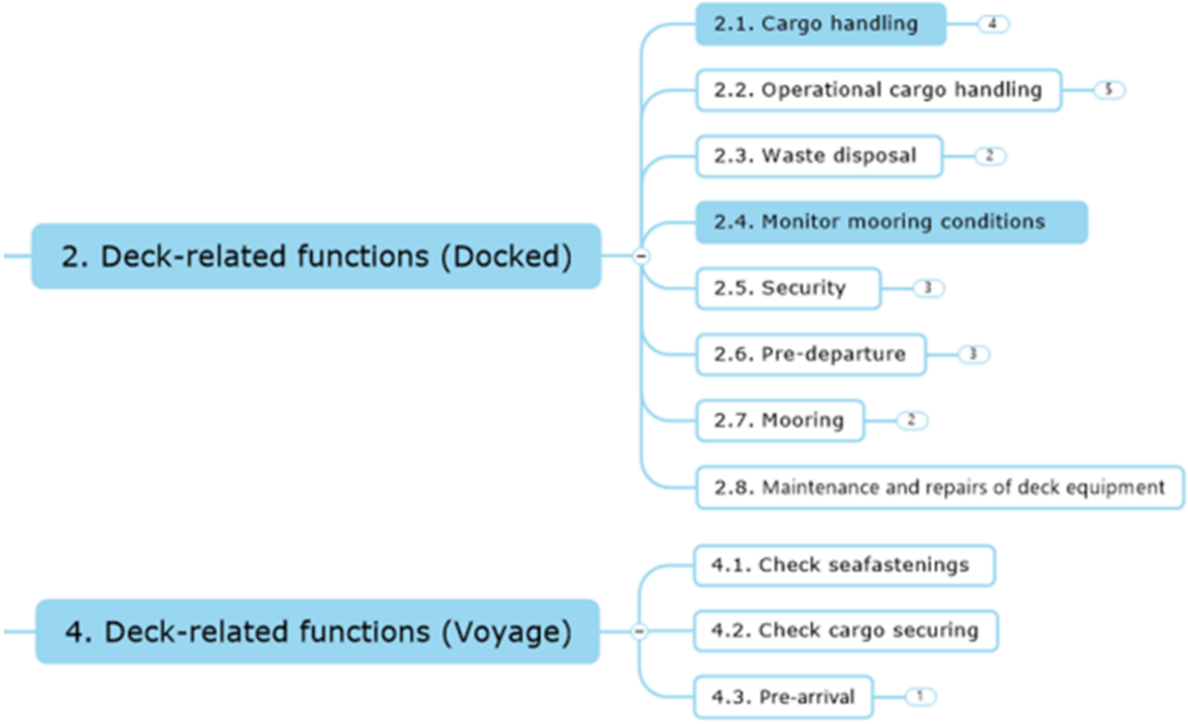

2. Deck-related functions (Docked)
2.1. Cargo handling
4
2.2. Operational cargo handling
5
2.3. Waste disposal
2
2.4. Monitor mooring conditions
2.5. Security
3
2.6. Pre-departure
3
2.7. Mooring
2
2.8. Maintenance and repairs of deck equipment
4. Deck-related functions (Voyage)
4.1. Check seafastenings
4.2. Check cargo securing
4.3. Pre-arrival
1

Figure 5 – Breakdown of Deck-related functions

While all the vessels differ with regards to the type of cargo, the cargo handling (functions 2.1, 2.2, 4.1 and 4.2) share the similarities of being fully autonomous in accordance with the A3-B1 MASS category. As such, the following common assumptions were made:

- The MASS system can interact with the shore side cargo system to load or unload the vessel.

- Likewise, it is assumed that the system will be able to secure the cargo and detect loose objects prior to departure.
- The personnel on board do not need to be actively involved. However, they can be expected to supervise the operation.

4.2.3 MASS control and monitoring

Figure 6 illustrates the main sub-functions related to Control and Monitoring. A total of 8 functions were identified, with only the Maintenance and repairs of engine equipment (function 5.7) being included as a separate node in the HAZID workshop.

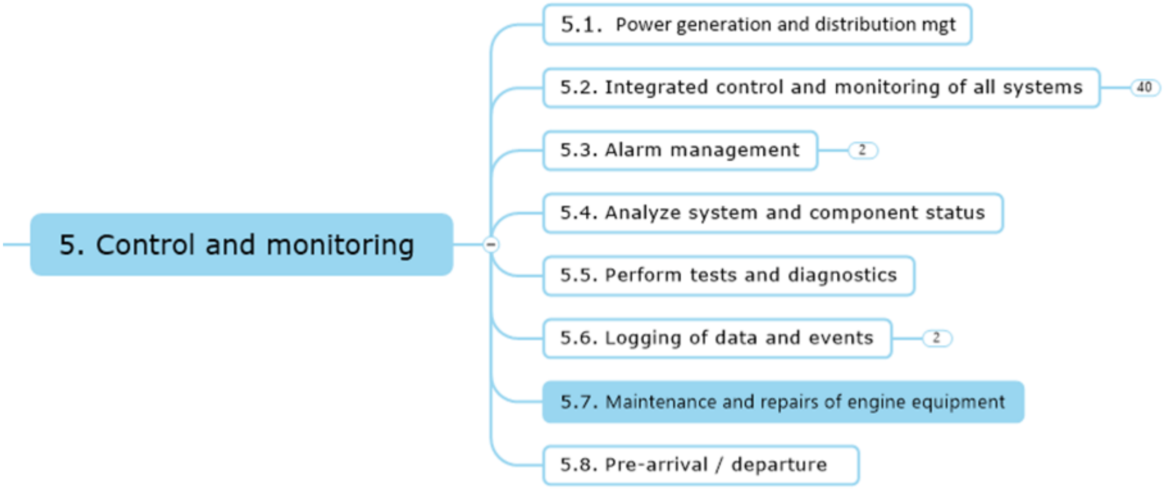

5. Control and monitoring
5.1. Power generation and distribution mgt
5.2. Integrated control and monitoring of all systems
40
5.3. Alarm management
2
5.4. Analyze system and component status
5.5. Perform tests and diagnostics
5.6. Logging of data and events
2
5.7. Maintenance and repairs of engine equipment
5.8. Pre-arrival / departure

Figure 6 – Breakdown of MASS control and monitoring functions

The following assumptions were made about the maintenance function:

- The machinery and instruments are designed for minimum maintenance during voyage.
- All planned maintenance shall be conducted by service personnel in port.
- Personnel onboard are only expected to manage unaccepted repairs or critical maintenance tasks during the voyage.

Because the control and monitor functions are an embedded part of most of the other functions, they were however addressed in the HAZID workshop discussions. Especially, the sub-function of *Integrated control and monitoring of all systems* (function 5.4) and *Alarm management* (function 5.3) was found to be central topics during the discussion. A common feature relevant to all the three ship types is a similar alerting system concept for which the following assumptions were made:

- A vessel designed according to the A3-B1 autonomy does not require personnel to be present at the Bridge or ECR (Engine Control Room) at all time for alarm response.
- It is, however, assumed that the person(s) responsible for watchkeeping has a remote alarm system available at all time in the form of a portable device.
- The portable alarm device will alert the watchkeeper if the system requires assistance but only provide basic information about the situation.

4.2.4 Manage abnormal situations

Figure 7 illustrates the Abnormal Situation function, where a total of 7 subfunctions was identified.

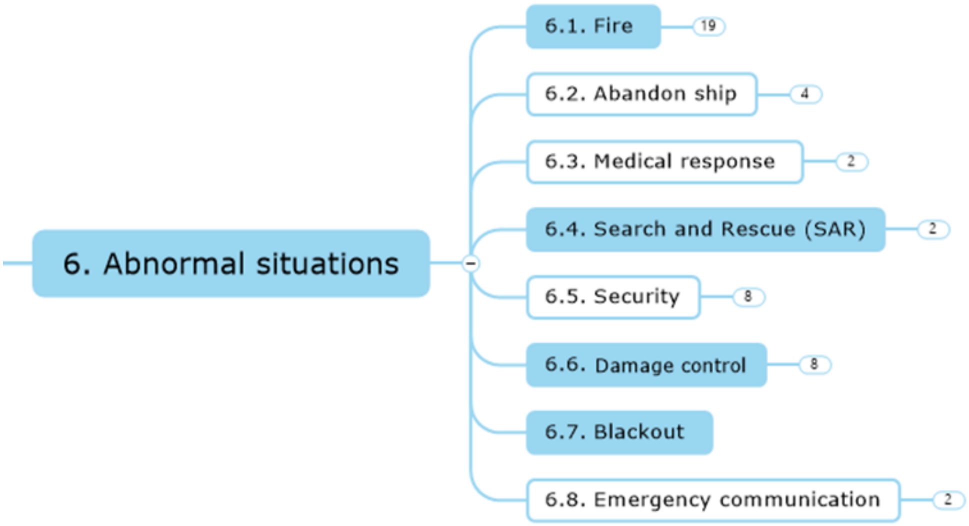


Figure 7 – Breakdown of functions related to managing abnormal situations

Functions related to managing abnormal situations refer to those involved with the last resort-MRCs (see Figure 1). The ideal approach would be to include all functions involved in abnormal / emergency situations as part of further analyses. However, as with the abovementioned functions, due to practical limitations of the study, only the functions affected most by the implications of introducing the A3-B1 MASS category were addressed.

4.3 Short route domestic passenger ship

The following sub-chapters describe the operational profile and context of the short route domestic passenger ship. For this case a combined car and passenger ferry was chosen. The ship is designed to operate autonomously with qualified operators onboard according to for A3-B1 MASS category.

4.3.1 Ship characteristics

The characteristics, including ship dimensions for the domestic passenger ship, is described in Table 3.

Table 3 – Ship characteristics for passenger ship

Route:	Halhjem – Sandvikvåg
Type:	Passenger Ferry (Ro-Ro)
LOA:	130.00m
Beam:	17.00m
Draught:	5.00m
Tonnage:	7500GT
	1000DWT
Capacity:	500 Passengers / 200Cars

4.3.2 Ship power generation and propulsion

The passenger ship is equipped with 3 x 2500 kW main generators and 2 x aux generators of 600KW. Furthermore, 2 x thruster of 2800 kW is installed for propulsion.

4.3.3 Area characteristics.

The following sub-chapters describes the navigational characteristics, weather and sea-state limitations for the route between Haljem - Sandvikvåg illustrated in Figure 8.

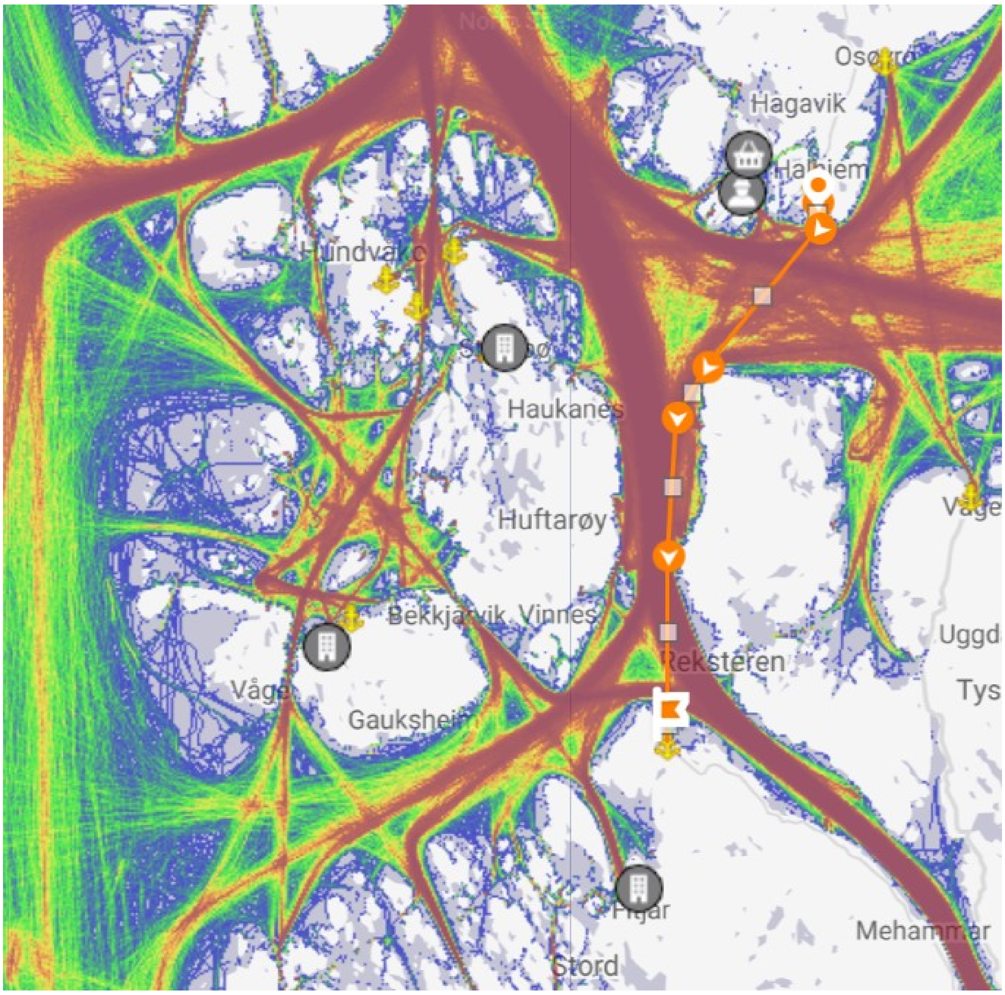


Figure 8 – The passenger ship route between Haljem – Sandvikvåg. AIS extract from Marin Traffic.

4.3.3.1 Navigational characteristics

The passenger ship is operating a route of approximately 12nm between Haljem and Sandvikvåg which crosses the main Norwegian sheltered route for vessels sailing north or south. Consequently, there is a high traffic density as illustrated in Figure 8. In addition, the vessel is exposed to increased navigational risk during departure and arrival as the quay is positioned in a narrow area. There is also a high density of pleasure crafts in these areas during the summer season which causes an additional navigational risk during the final approach to the port of Haljem.

4.3.3.2 Weather and sea-state limitations

As most of the transit between Haljem to Sandvikvåg is protected by islands, it is not expected that wave height will represent any major hazards to navigation. However, the area is located on the west Norwegian coast, which is exposed to high wind, potentially impacting safe navigation of the vessel.

4.3.4 Ship manning and responsibilities

The passenger ship is designed according to level A3-B1 autonomy which includes having qualified operators onboard. Consequently, the safe manning onboard can be reduced to the minimum of personnel required to manage the evacuation of passengers, as well as manage the vessel when the defined parameters are exceeded.

Table 4 describes what is assumed to be a safe minimum manning and required competencies for the passenger ship, based on the increased level of automation introduced by the A3-B1 MASS category.

Table 4 – Proposed safe manning on the passenger ship

Department	Title	No.	STCW	Responsibility
Bridge/Deck	Bridge/Deck Operators	1	II/2 II/5	Navigational supervision Cargo and deck operation Daily maintenance and operation of Deck machinery Daily maintenance and operation of Bridge equipment
	Able Seaman	2	II/4, II/5	MOB Team, operating the maritime evacuation system and assistance during an evacuation Daily preparation of food, general cleaning Assist cargo and deck operation
Engine	Engine Operators)	1	III/2 III/5, III/6	Daily maintenance and operation of machinery Daily maintenance and operation electrical systems
Total		4		

All Bridge/deck responsibility is designated to a Bridge/Deck operator, and all Engine responsibility is designated to an Engine operator. In addition, it is expected that two Able Seamen are required onboard fulfil other functions as; preparation of food to the crew, general cleaning, evacuation of passengers, maintain MOB contingencies and maintenance.

Due to the trade pattern it is not necessary to keep the off-signing shift onboard, thus reducing the required manning to four persons on board at all time.

4.3.5 Bridge manning philosophy

The passenger ship can in principle complete the entire voyage without human involvement. However, due to the close vicinity to shallow waters and a (at times) high density of recreational crafts and fishing boats, the bridge operator is periodically required to be present on the bridge during port manoeuvring and transit.

Figure 9 illustrates the operational profile of the domestic passenger ship. The bridge will be manned during the 50 minutes voyage from Halhjem to Sandvikvåg, including port manoeuvring. Once the vessel is moored, the bridge does not require manning, and the bridge operator can conduct other tasks.

Time in port	10 minutes (17%)
Port manoeuvring time	10 minutes (17%)
Transit time	40 minutes (66%)
Total turnaround time	1 hour
Manning characteristic	Bridge manned during Transit and Port manoeuvring

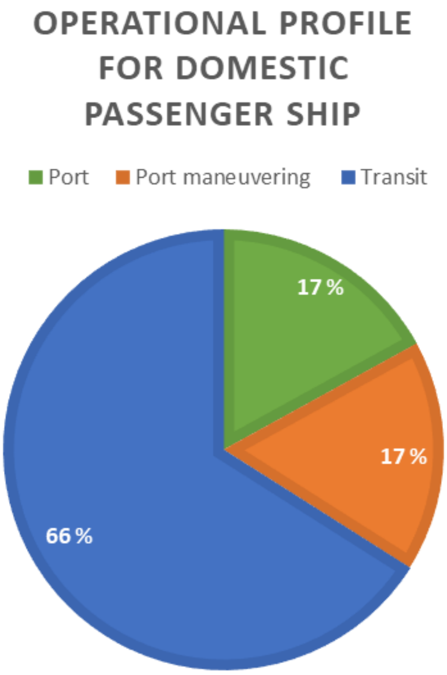


Figure 9 – Estimated operational profile for domestic passenger ship.

4.4 Short-sea cargo ship

The following sub-chapters describe the operational profile and context for a container feeder vessel used to represent a short-sea cargo ship designed and operated according to the A3-B1 MASS category.

4.4.1 Ship characteristics

The characteristics, including ship dimensions, is described in Table 5. The characteristics are based on a container feeder vessel designed for short-sea trade but certified for worldwide operation.

Table 5 – Ship characteristics for Container feeder vessel

Route:	Bremerhaven – Kristiansand
Type:	Container feeder
LOA:	130.00m
Beam:	20.00m
Draught:	8.00m
Tonnage:	8000GT
	10 000DWT
Speed:	18kn
Capacity	800 TEU

4.4.2 Ship power generation and propulsion

The container ship is equipped with a diesel engine producing 7200 kW MCR at 500 rpm, a shaft generator of 1000kW and 2 x auxiliary diesel sets of 350 kW. In addition, a 750kW bow thruster is used for port manoeuvring.

4.4.3 Area characteristics

The following sub-chapters describe the navigational characteristics, weather and sea-state, tidal and ice limitations for the route between Bremerhaven and Kristiansand illustrated in Figure 10.

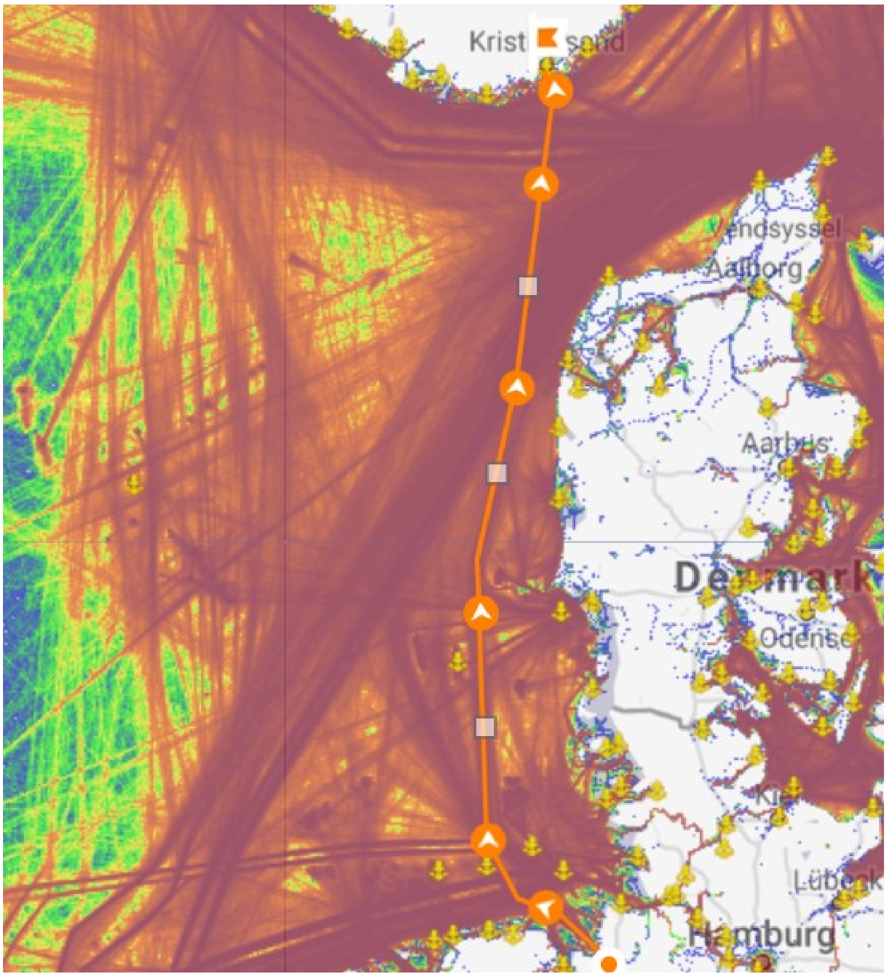


Figure 10 – Route between Bremerhaven – Kristiansand. Traffic density extract from Marin Traffic.

4.4.3.1 Navigational characteristics

The container ship is operating a shipping route of approximately 300nm between Bremerhaven and Kristiansand, which is crossing several major shipping routes. After departing Bremerhaven, the vessel is exposed to the main shipping route from traffic sailing to and from the Baltic sea, via the Kiel canal. In addition, there is traffic sailing to and from the Elbe and Weser rivers.

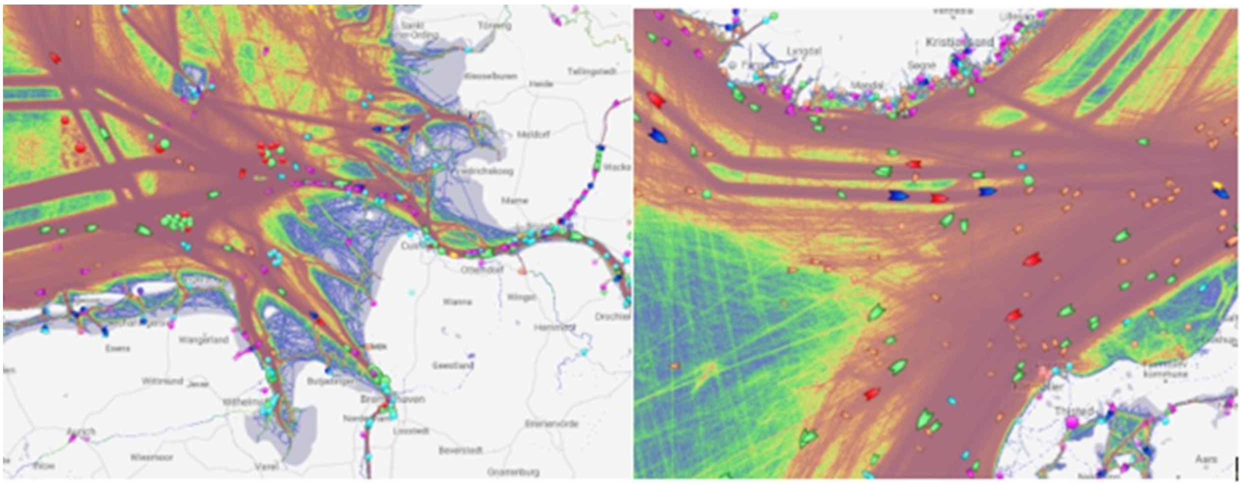


Figure 11 – Traffic density around Bremerhaven and Skagerrak. Source: Marin Traffic.

Figure 11 illustrates the average traffic situation around Bremerhaven and western part of Skagerrak. The main navigational hazards around Bremerhaven with regards to traffic in this area can be divided in two major parts; departure/arrival Bremerhaven and crossing the traffic lane going to and from the Elbe river. Furthermore, the vessel crosses an open sea area between Denmark and Norway west of Skagerrak. This area is known to have a high density of traffic as it is the main open sea shipping route to and from the Baltic sea.

4.4.3.2 Weather and sea-state limitations

The shipping route from Bremerhaven to Kristiansand is located on the East side of the North Sea including the German Bight, Danish West coast and West part of Skagerrak. All these areas are exposed to the open North Sea which often encounters strong wind systems and generates waves which are considered a risk during transit.

4.4.3.3 Tidal limitation

The tidal range in Bremerhaven is approx. 3.8m with tidal currents from 2.5 to 3.5 knot. This does not restrict the vessel with regards to draft limitations on the quay-side. However, the tidal current can impact the safe manoeuvring of the vessel. The tide in the Port of Kristiansand is marginal and will not be considered in this case.

4.4.3.4 Ice limitation

Bremerhaven Port is exposed to ice only in case of extreme weather conditions and is therefore not considered as a navigational hazard. Likewise, Kristiansand is not normally exposed to ice, but it occasionally occurs during the winter period.

4.4.4 Ship manning and responsibilities

Table 6 describes the minimum manning proposed for a container ship designed and operated according to level A3-B1 autonomy. All bridge/deck responsibility is divided into two bridge/deck operators, and all Engine responsibility is designated to two engine operators. This allows the personnel to work 12-hour shifts and maintain continuous supervision of their respective departments. Reducing the manning further would be difficult due to the trade pattern, as the voyage exceeds 12 hours. Furthermore, the Galley department is assumed to be completely removed, which require all crew members to be responsible for preparing their own food.

Table 6 – Proposed safe manning on short sea container ship

Department	Title	No.	STCW	Responsibility
Bridge/Deck	Bridge/deck operators	2	II/2 II/5	Navigational supervision Cargo and deck operation Daily maintenance and operation of Deck machinery Daily maintenance and operation of Bridge equipment Daily preparation of food, general cleaning
Engine	Engine operators	2	III/2 III/5 III/6	Daily maintenance and operation of machinery Daily maintenance and operation electrical systems Daily preparation of food, general cleaning
Total		4		

4.4.5 Bridge manning philosophy

The task of port manoeuvring is considered a high-risk operation due to the proximity to shore and other vessels. During this operation the Bridge will therefore be manned and actively monitored by the Bridge/Deck Operators.

The docking/undocking phase will commence when departing the harbour and prior to arriving at the destination port. Hence, in this scenario the Bridge will be manned during departure Bremerhaven and prior to arriving Kristiansand. The Operator will remain on "standby" during the remaining voyage and conduct other operational tasks.

Figure 12 illustrates the operational profile of the container ship which indicates the time spent on port manoeuvring to be 2%. Hence, the bridge is only required to be manned for 2% of the whole operation. For the remaining time the ship is either under transit or conducting cargo operation in port, which does not require any active human involvement.

Time in Port	24 hours (57%)
Port manoeuvring time	1 hour (2%)
Transit time	17 hours (41%)
Total Turnaround time	42 hours
Manning characteristic	Bridge manned during Port manoeuvring

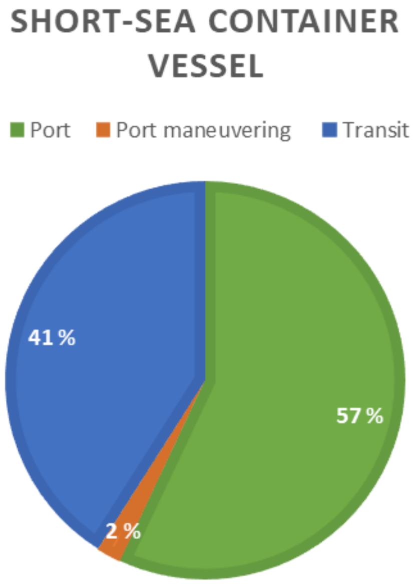


Figure 12 – Operational profile for a Container feeder ship

4.5 Ocean going cargo ship

The following sub-chapters describe the operational profile and context for a Bulk carrier used to represent an ocean-going cargo ship designed and operated according to the A3-B1 MASS category. As for the previous vessels, qualified operators will be present on board to supervise the operation.

4.5.1 Ship characteristics

Table 7 illustrates the ship dimensions for the ocean-going bulk carrier.

Table 7 – Ship characteristics for ocean-going bulk carrier.

Route:	Milne Inlet Port (CA) – Rotterdam (NL)
Type:	Bulk carrier (Panamax)
LOA:	220.00m
Beam:	32.00m
Draught:	14.00m
Tonnage:	40 000GT
	75 000DWT
Speed:	15knot

4.5.2 Ship power generation and propulsion

The bulk carrier is equipped with a single screw diesel propulsion unit with one 6-cylinder 2 stroke engine producing MCR 10 000 kW at 120 rpm. In addition, three 4cycle diesel generators, producing 800Kw at 900 rpm. Furthermore, a 1000Kw bow thruster is utilized for manoeuvring in port.

4.5.3 Area characteristics

The vessel is transporting Iron Ore from Milne Port (CA) to Rotterdam (NL) over the North Atlantic Ocean. Route distance is approximately 3600nm (see Figure 13).

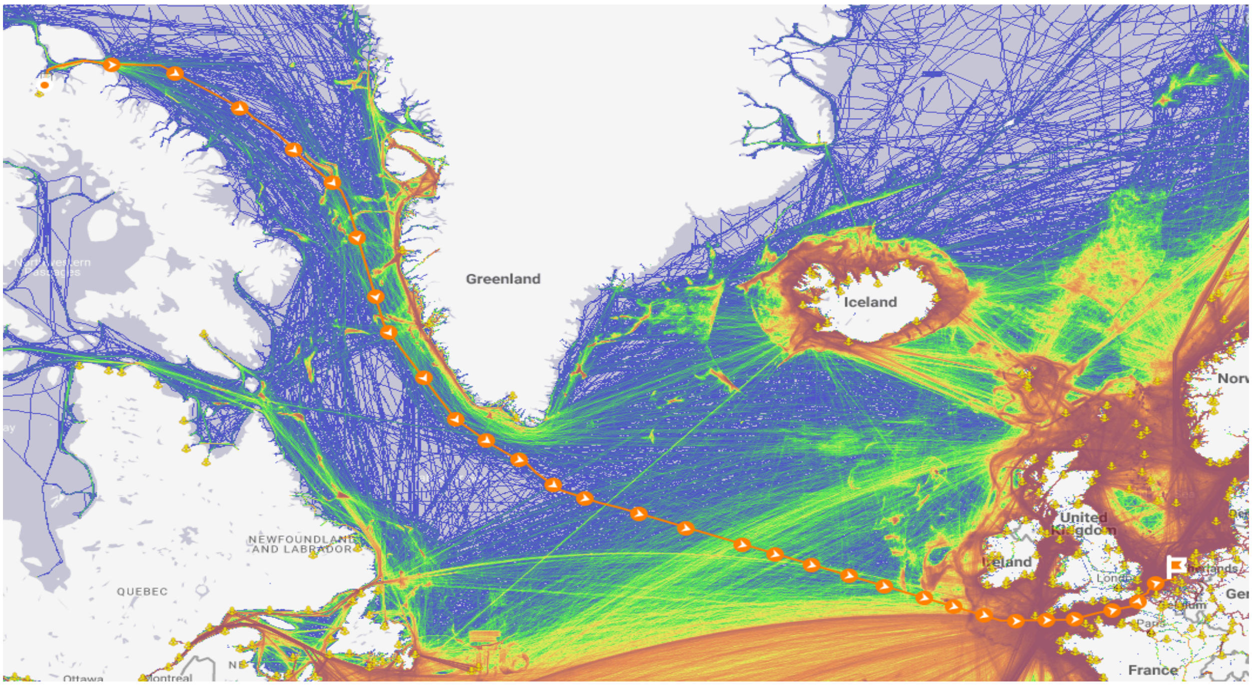


Figure 13 – Route between Rotterdam – Milne Inlet. Source: Marin Traffic.

4.5.4 Navigational characteristics

Most of the passage the ship is transiting in the open Atlantic Ocean (Figure 13), which has a low traffic density. However, heavy traffic is expected around Rotterdam port, especially when passing the English Channel for the Rotterdam approach (Figure 14).

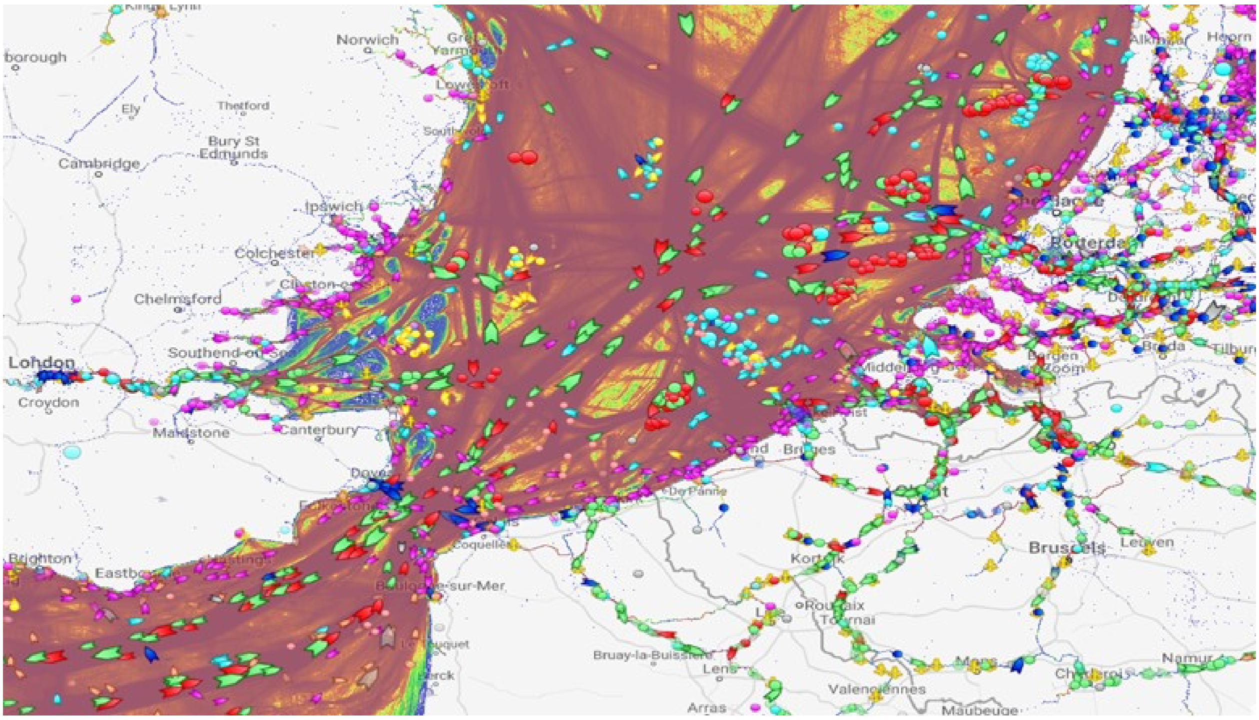


Figure 14 – Traffic density around the English Channel and Rotterdam. Source: Marin Traffic.

4.5.4.1 Weather and sea state limitations

For most of the transit, the vessel is travelling in the open ocean and is exposed to the larger weather systems in the North Atlantic. Consequently, it could be necessary to change route during the passage to avoid damage to vessel and cargo caused by heavy weather.

4.5.4.2 Ice limitations

Due to ice in the winter period, Milne Inlet is only fully open to shipping from approximately July to October. During the winter months, icebreakers are required to maintain the shipping route.

4.5.5 Ship manning and responsibilities

Table 8 illustrates the proposed minimum manning for this bulk carrier designed and operated according to the A3-B1 MASS category. Like the previous safe manning for the container feeder the responsibility of the Bridge/Deck department is designated to two bridge/deck operators and the engine department responsibility is designated to two engine operators.

Table 8 – Proposed safe manning on the bulk carrier

Department	Title	No.	STCW	Responsibility
Bridge/Deck	Bridge/Deck operators	2	II/2 II/5	Navigational supervision Cargo and deck operation Daily maintenance and operation of Deck machinery Daily maintenance and operation of Bridge equipment Daily preparation of food, general cleaning
Engine	Engine operators	2	III/2 III/5, III/6	Daily maintenance and operation of machinery Daily maintenance and operation electrical systems Daily preparation of food, general cleaning
Total		4		

4.5.6 Bridge manning philosophy

Likewise, the bridge manning philosophy is equivalent to the container feeder where the bridge is manned during arrival and departure.

Time in port	48 hours (16%)
Port manoeuvring time	2 hours (1%)
Transit time	240 hours/10days (83%)
Total turnaround time	290 hours
Manning characteristic	Bridge manned during Port manoeuvring

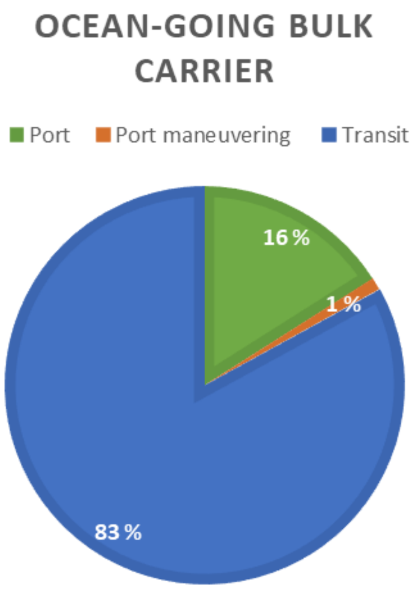


Figure 15 – Operational profile for the bulk carrier

Figure 15 illustrates the operational profile of the vessel. As the figure indicates, the majority of the turnaround time is spent on transit (83%). Furthermore, a 48hours port stay for unloading and loading the ship for a new voyage is expected. Only the remaining 1% of the operation will be spent on port manoeuvring, where the supervisor is required to attend the bridge continuously.

5 HAZID OF THE A3-B1 MASS CATEGORY (TASK 1. B)

This chapter documents Task 1.b in Part 1 of the SAFEMASS study; a hazard identification (HAZID) of the A3-B1 MASS concepts developed in Task 1.a. The HAZID is documented in Appendix B.

5.1 Focus areas

Building on the problem definition of SAFEMASS Part 1 (1) the HAZID's focus is primarily on challenges associated with low manning levels and longer periods with an unmanned bridge on three different types of A3-B1 category vessels.

As an extension of this focus, the needs for human intervention and system redundancy are assessed for scenarios where the automation system is faced with scenarios or conditions that exceed its pre-defined parameters for what constitutes its operational boundaries. As described in the following sub-chapters, answers to the following questions have made up the basis for identification of hazards associated with the A3-B1 level of autonomy and control:

- What constitutes abnormal situations and emergencies?
- Which parameters define operational boundaries?
- When and how the operator is informed?
- Degree and form of human involvement?
    - Supervision (within operational boundaries)
    - Opportunities to override/ intervene

5.1.1 Operational boundaries

As a part of preparing the HAZID, operational boundaries associated with the functions selected for analysis were defined. This is illustrated in Figure 16. Due to the analysis being conducted on a conceptual level it was not always possible to establish exact boundary *parameters*. Emphasis was therefore put on establishing definitions of boundary *conditions* specific enough for relevant hazards to be identified.

When applying the concept of "Minimum Risk Conditions" (MRC) as explained in chapter 4.1.1 (Figure 1) operational boundaries can be present when a MASS is;

- transitioning from a normal operational state to an abnormal situation, and
- transitioning from an abnormal situation to an MRC or last-resort MRC.

Furthermore, conditions which can represent such boundaries include;

- degradation or failure of functions which are critical to MASS operational performance and safety, or
- external threats which represent risks going beyond the MASS capabilities intended by design.

An example of an operational boundary could be a scenario where the MASS finds itself in a complex traffic situation where no auto-generated solutions would prevent the vessel from initiating MRC.

5.1.2 “Human-in-the-loop” and operator intervention

The A3-B1 level of autonomy and control implies potential “human-in-the-loop” challenges when it comes to operator intervention. By design, the operator can be left out of the MASS’s loop of automated control actions, potentially for long periods of time, before being required to enter the loop, often on short notice. In such cases, reliable human performance depends largely on the system’s ability to provide the operator(s) sufficient *situational awareness* to make and implement correct decisions.

Hence, an important part of preparing the HAZID was to define which part of a function requires human involvement, and which part is intended to be solved by the MASS system alone. The role of the operator in performing a function was defined using the following four categories /6/:

- **Detection**: Acquisition of information that is relevant for the control of a function. The information may be based on sensors and/or human perceptions.
- **Analysis**: Interpretation of the acquired information into a situational understanding relevant for the control of the function.
- **Planning**/ decision-making: Determination of needed changes in control parameters in order to keep the function performance within the applicable frames.
- **Action**: Effectuating the planned changes of control parameters, typically via actuators operated via a control system. This is however considered to be conventional systems based on existing technologies, accordingly this report assumes this part is handled by existing safety regimes.

In addition to labelling the operator’s role according to the abovementioned categories, descriptions of the required operator tasks were provided. More information is provided in chapter 5.2.1 about HAZID methodology.

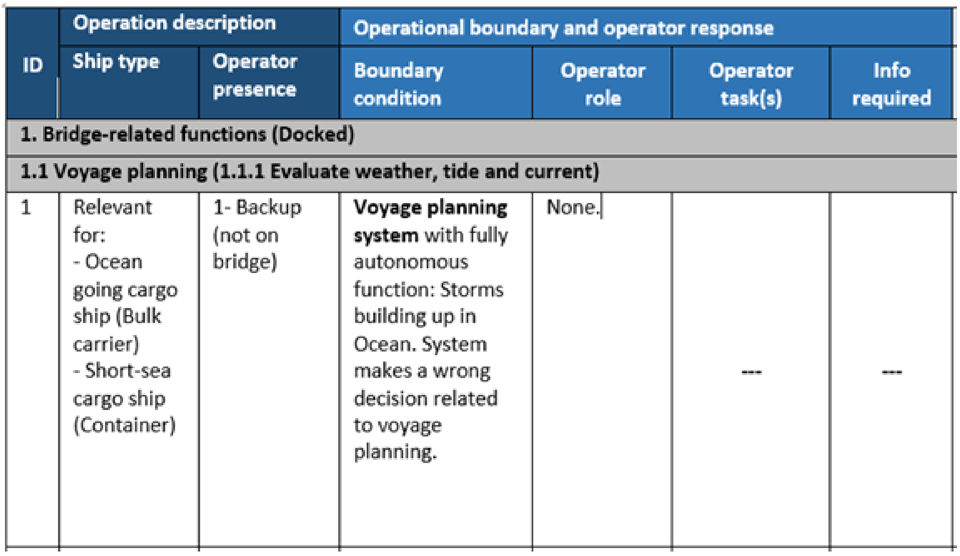
5.2 HAZID approach

The following sub-chapters explain the HAZID methodology, including the HAZID study nodes and process.

5.2.1 HAZID methodology

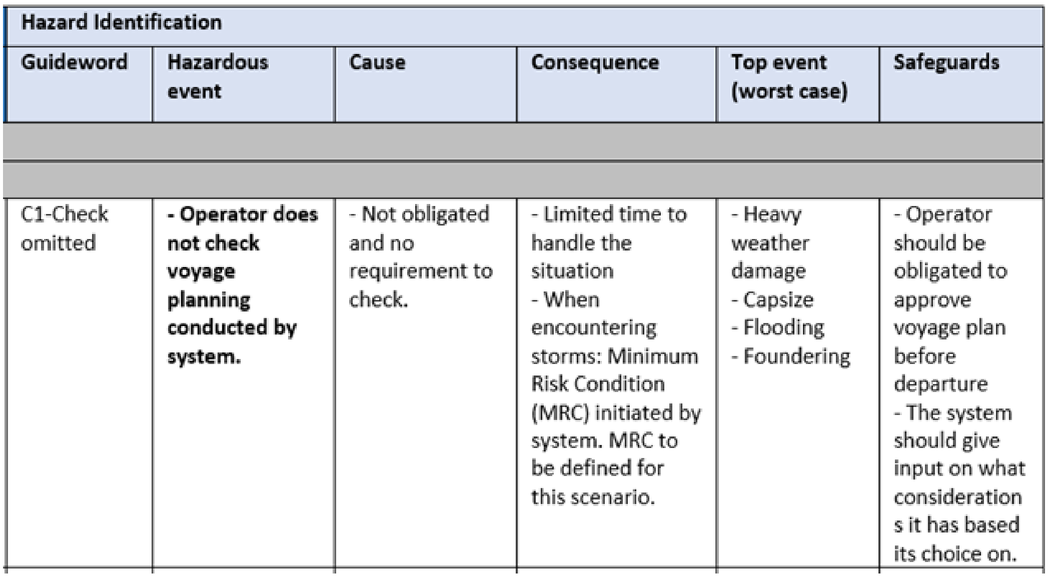
A HAZID log (Appendix B) was developed specifically to meet the objectives and address the focus areas of SAFEMASS Part 1. As can be seen in Figure 16 and Figure 17, the log sheet consisted of three main parts; a) operation description, b) operational boundary and operator response, and c) the hazard identification.

The two first parts, a) and b), combined with the functions used as HAZID nodes (chapter 5.2.2) made up the context and scenario for which hazard identification was performed.



ID	Operation description		Operational boundary and operator response			
	Ship type	Operator presence	Boundary condition	Operator role	Operator task(s)	Info required
1. Bridge-related functions (Docked)						
1.1 Voyage planning (1.1.1 Evaluate weather, tide and current)						
1	Relevant for: - Ocean going cargo ship (Bulk carrier) - Short-sea cargo ship (Container)	1- Backup (not on bridge)	**Voyage planning system** with fully autonomous function: Storms building up in Ocean. System makes a wrong decision related to voyage planning.	None.	---	---

Figure 16 – "Operation description" and "Operational boundary and operator response" columns in HAZID log sheet



Hazard Identification					
Guideword	Hazardous event	Cause	Consequence	Top event (worst case)	Safeguards
C1-Check omitted	**- Operator does not check voyage planning conducted by system.**	- Not obligated and no requirement to check.	- Limited time to handle the situation - When encountering storms: Minimum Risk Condition (MRC) initiated by system. MRC to be defined for this scenario.	- Heavy weather damage - Capsize - Flooding - Foundering	- Operator should be obligated to approve voyage plan before departure - The system should give input on what consideration s it has based its choice on.

Figure 17 – "Hazard identification" column in HAZID log sheet

The bullet-points below provide definitions for the column topics used in this study.

a) **Operation description (**Figure 16**)**, consisting of three columns for collecting the following data:

   i. *ID*; Hazard identification number.

   ii. *Ship type*; which of the three A3-B1 ship descriptions the hazard applies to;

      1. Short route domestic passenger ship

      2. Short-sea cargo ship (Container)

      3. Ocean going cargo ship (Bulk)

    iii. *Operator presence*; location and mode of the operator (see separate definitions below).

b) **Operational boundary and operator response** (Figure 16), consisting of four columns for collecting the following data:

    i. *Boundary condition*; events, e.g. failure modes or external threats, where the MASS transitions from a normal operational state into an abnormal situation or MRC.

    ii. *Operator role*; the role of the operator in managing the boundary condition (see separate definitions in chapter 4.1.1.

    iii. *Operator task(s)*; tasks required by the operator in his/her role.

    iv. *Info required*; information used by the operator in detecting, monitoring or diagnosing an event.

c) **Hazard identification**, consisting of six columns for collecting the following data:

    i. *Guideword*; human error guidewords for prompting relevant task failure modes, i.e. hazardous events (see Appendix C).

    ii. *Hazardous event*; event associated with MASS and/ or operators' response to the boundary condition which could contribute to an accident.

    iii. *Cause*; Factors which could cause the hazardous event to occur. In this study the *human-related hazards* listed in the FSA guideline /8/ were used as prompts.

    iv. *Consequence*; outcome or effects of the hazardous event, e.g. escalation.

    v. *Top event*; worst case accident for the assessed scenario. Used to identify potential events for inclusion in the fault tree analysis.

    vi. *Safeguards*; measures to prevent the hazardous event from occurring, or to mitigate its effects. Note that during the HAZID work sessions the emphasis was on identifying hazards, and not on risk mitigation. But when relevant safeguards where identified, these were noted as input for further considerations.

The definition of **operator presence** was based on the classification provided in ISO 23860 /7/ (with some custom modifications):

- *0 – None*: There is nobody available to man the control position.
- *1 – Backup (not on the bridge):* Person(s) is available to operate the control position, but they are not present. They need to be called and there will be a control latency, before they can resume full control.
- *2 – Available (on the bridge):* Person(s) is present at the control position, but they are not actively controlling the ship. The operator can regain full control of the ship at short notice and the control latency is significantly lower than for case 1 and is mainly related to the time the operator needs to establish sufficient situational awareness.

- *3 – In control (on the bridge):* Person(s) are at the control position and are in charge of and actively controlling the ship. The control latency is in principle zero.

5.2.2 HAZID nodes

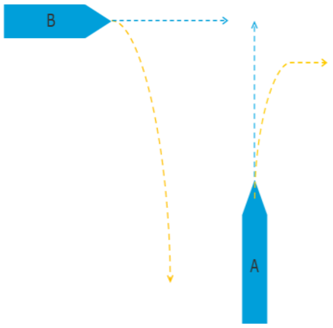
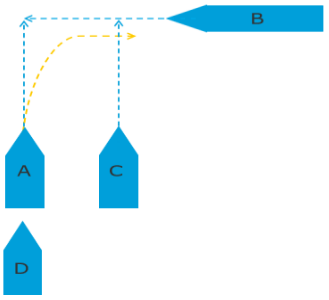
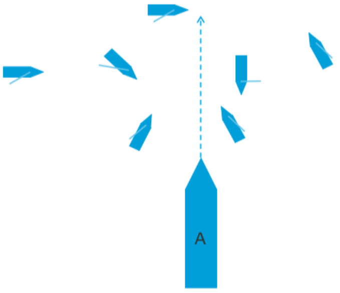
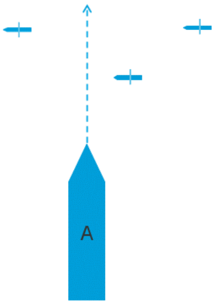
Functions identified as critical and relevant in the function breakdown (chapter 4.2) were initially included as the HAZID's study nodes, i.e. items subject to analysis. These are listed in Table 9. Hazards associated with other functions were logged as they emerged naturally from the workshop discussions, or from being prompted by HAZID guidewords.

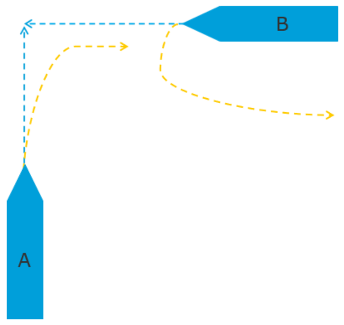
Table 9 – Functions initially selected for hazard identification

ID	Function
1.0	Bridge-related functions (Docked)
1.1	Voyage planning
1.2	Trim, stability & stress while docked
2.0	Deck-related function (Docked)
2.1	Cargo handling
2.4	Monitor mooring conditions
3.0	Bridge-related functions (Voyage)
3.1	Harbour manoeuvring
3.2	Navigation & manoeuvring during transit
3.4	Trim, stability & stress while docked
5.7	Maintenance and repairs of engine equipment

In addition, a set of scenarios were developed to be used as a context for hazard identification. This was particularly aimed towards analysis of functions related to navigation.

Table 10 – Scenarios used to aid hazard identification

ID	Scenario	Description	Graphic illustration
1	COLREG Crossing situation	- The first phase of scenario 1 describes a crossing situation where vessel B is on crossing course with MASS A. According to COLREG Reg.15, vessel B is required to give-way for vessel A. - In the next phase of the scenario, vessel B does not respond and instead maintains course and speed. - Vessel A may, in this case, take action to avoid collision by her manoeuvring according to COLREG Reg.17.	
2	COLREG Crossing situation	- Other ship B on a collision course (from SB). Collision warning alarm on ship A. However, ship A not able to follow COLREG (give way) because another ship C is on SB on same heading and speed and Ship D is astern.	
3	COLREG Crossing situation	- Scenario 3 describes a high-density traffic situation where the MASS encounters several sailboats attempting to cross (regatta). - Due to the complexity of the situation the system is not able to analyze (predict next movements).	
4	COLREG Crossing situation	Scenario 4 describes a high-density traffic situation of pleasure crafts (kayaks). System limitations with regards to object classification. E.g. not able to differentiate between timber and kayaks.	

ID	Scenario	Description	Graphic illustration
5	COLREG Crossing situation	- Scenario 5 describes a crossing situation where vessel A is required by COLREG to give-away for fishing vessel B - However, the fishing vessels intention is to turn around and not cross vessels B`s bow. Vessel B is attempting to communicate this to vessel A, but this is not perceived correctly by MASS system due to language barrier/dialect.	
6	Voyage Planning	- Scenario 6 describes a scenario where storms are building up in the North Atlantic Ocean. - MASS System is conducting voyage planning and makes a wrong decision related to voyage planning.	-
7	Trim, Stability and Stress while docked	- Scenario 7 describes issues related to Trim, stability & Stress while docked. - MASS bulk vessel is loading Iron when a deviation between calculated and actual stability condition occurs.	-
8	Heavy weather damage	- Scenario 8 describes a bulk cargo hatch being damaged due to heavy weather resulting in water ingress. -One of the cargo holds are flooding and MASS engages an MRC where the RPM is reduced, and heading is altered towards the weather. The operator is alerted and requested to take control.	-
9	Vessel in distress	- Scenario 9 describes a scenario where the bulk vessel encounters a sailboat in distress in the North Atlantic Ocean. - As no other assistance is available, the bulk vessel is designated as the on-scene commander (OSC) and is obliged to coordinate the search and rescue operation	-

5.2.3 HAZID process

The key activity in the hazard identification process was a two-day HAZID workshop facilitated by DNV GL on the 11th and 12th of September 2019 in Høvik, Norway. Representatives from EMSA, The Norwegian Maritime Authority (NMA), Wilhelmsen, the Norwegian Shipowners Association (NSA) and Finnish Traficom participated in the workshop together with DNV GL:

- Sifis Papageorgiou, Project Officer at EMSA
- Sondre Fagerli Øie, Principal Consultant at DNV GL (project manager)
- Peter Nyegaard Hoffmann, Head of Section at DNV GL (project sponsor)
- Hans Jørgen Johnsrud, Senior Consultant at DNV GL (workshop chair)
- Julie Huth Lindberg, Intern at DNV GL (scribe)
- Erlend Norstein, Consultant at DNV GL
- Are Jørgensen, Senior Principal Engineer at DNV GL
- Svein David Medhaug, Project Manager at Norwegian Maritime Administration
- Petter Kyseth, HSEQ Superintendent at Wilhelmsen Ship Management
- Jahn Viggo Rønningen, Director - Head of Ship Safety at Norwegian Shipowners' Association
- Marko Rahikainen, Chief Adviser at Traficom

A more detailed description of the participants profile can be read in APPENDIX A - SAFEMASS participants

With the purpose of facilitating efficient HAZID work sessions, the HAZID log sheet was initially pre-populated to some extent internally by DNV GL team members. This particularly concerned the parts related to the description of operations, boundary conditions, and operator response.

Three specific measures were made to ensure that the participants had sufficient background information for the task at hand:

- A week prior to the work session DNV GL issued pre-read to the external participants consisting of the function tree breakdown and the qualitative A3-B1 ship descriptions.
- The ship descriptions were reviewed and discussed as part of introducing the meeting.
- Relevant parts of the function tree were reviewed and discussed as part of introducing each HAZID study node.

The actual HAZID work session was chaired and recorded by DNV GL.

5.3 HAZID output

This report’s Appendix B includes the main deliverable from the HAZID. The log includes 57 rows with unique ID numbers. Hazards/ hazardous events, causes and consequences from 38 of the IDs were used to construct the fault tree models reported in chapter 6, which also documents what are considered the main risks. These are marked with a light “aqua” coloured IDs in the HAZID log. Two rows were considered not relevant due to hazards being addressed as part of other nodes. These are not marked with any colour. The remaining 17 rows marked with light “orange” coloured IDs are summarized in the sub-chapters below according to which HAZID node they belong to.

5.3.1 Monitor mooring conditions (HAZID node #2.4)

While at quay, the bridge may be unattended for longer periods of time (applies for all three vessels). In case the MASS system fails to automatically reduce mooring line tensions below its pre-defined and safe limits, the MASS operator must relocate him-/herself to the bridge and attend to the situation if not already present. Failure to correctly operate the winch or thrusters can ultimately result in a collision with other vessels or impact against the quay side.

5.3.2 Collison and grounding avoidance (HAZID node #3.2.4)

Most risks associated with collisions are addressed in the FTA (see chapter 6.1). However, the collision and grounding avoidance HAZID node revealed one specific hazard (ID 35) which is not addressed as part of the fault tree analysis. This was related to the MASS system’s ability to predict and handle shifting ground conditions in combination with being on collision course with other vessels. A scenario could be sailing in a narrow channel with dense traffic and uncertain or changing depth conditions due to sandbanks and/ or shifting water levels. In such cases all three ship concepts would likely have the bridge manned with the MASS operator available at the controls, ready to intervene. He- or she would still be confronted with a challenging task of monitoring the external environment in addition to continuously evaluating the MASS system’s performance. The need for intervening to resolve a potential conflict between either collision or beaching/ grounding may arise on a short notice. This puts high demands on the MASS operator’s ability to quickly enter the automation loop and take manual control. Furthermore, the physical controls and human-machine interface must be designed to support such actions. If this is lacking the probability of human error could be substantial.

5.3.3 Maintenance and repair of engine equipment (HAZID node #5.7)

All three MASS ship concepts described in this report assumes that the crew will perform some degree of maintenance and repairs. However, due to the low manning levels this is likely to be kept at a minimum, somewhat depending on equipment’s reliability. Instead maintenance and upgrades will have to be done while docked at quay, with assistance from external or internal service providers. Potential hazards can be insufficient or incorrect maintenance which the MASS crew is not made familiar of, loose objects left onboard, and equipment left in dangerous condition (e.g. hatches not closed properly, valves in incorrect position etc). Such hazards may not be unique to MASS, but due to the lower manning level there may be fewer opportunities for the MASS operators to control such risks (e.g. less frequent inspections).

5.3.4 Firefighting (HAZID node #6.1)

Several risks were identified for the fire-fighting function. For the passenger ferry, extinguishing a local fire (e.g. a battery in an electrically powered vehicle) manually could put high demands on parts of the manning, which is already low. In case of escalation, the crew members capacity to perform other emergency related tasks could be diminished, such as evacuating passengers and supervising MASS performance (e.g. entering an MRC). Another hazard relevant for all three ship concepts is the risk of automated activation of the firefighting system flooding the vessel. This could cause a complex situation with regards to vessel stability, for which human intervention will be required to prevent further escalation.

5.3.5 Abandon ship (HAZID node #6.2)

For the short route domestic passenger ship a highly relevant risk is that related to evacuation of passengers. This function is one which may not be the easiest to automate, considering the interpersonal and social aspects. The MASS crew will have to perform crisis management, including guiding the passengers towards the mustering stations, keeping track of personnel on board (POB), and supervise (semi-)automated activation of the maritime evacuation system (MES). The risk of unsuccessful evacuation could be caused by lack of crowd management, panic among passengers, challenges with injured or disabled individuals, or irrational behaviour. Such events could result in spending too long time evacuating and not being able to evacuate everyone in time.

An overarching and contributing factor could be the potential negative relationship between the number of passengers and the crew's crisis management capacity. This challenge can be similar for a conventional vessel, but it is expected that it will be even more prevalent with autonomous vessels as they provide an opportunity to reduce the number of crew members for normal operations even further. The evacuation function was also the main reason why two able seamen were added to the manning of this particular ship concept. It could be argued that the design philosophy behind a A3 level domestic passenger ferry would aim towards lowering the manning level even further by exploring smarter solutions for evacuation than what was assumed during the HAZID discussions (i.e. a semi-autonomous MES, conventional P&A and communication systems etc.).

5.3.6 Search and rescue (HAZID node 6.4)

During the HAZID workshop discussions it was argued that rescue operations performed by a A3-B1 MASS could prove to become particularly challenging. A scenario could be that the ocean going, or short-sea cargo ship encounters a sailboat in distress mid-ocean. An initial risk is that the MASS fails to detect that the vessels is in distress. If radio communication is down, the sailboat crew may be signalling for help solely by using hand gestures. This may be hard to detect if the MASS crew is not present on the bridge and performs lookout, which may not always be the case, especially mid-ocean.

An attempt would be made by the MASS crew to get the sailboat crew onboard, by use of a MOB boat. The low level of manning would require that the davit requires as few manual actions as possible and could be remotely operated. Two persons would need to be onboard the MOB boat to help rescue the people in the water or onboard the sinking sailboat, as well as to keep each other safe. One of the MASS crew members must remain on the bridge to supervise the rescue mission, leaving one crew member to either be present on deck (e.g. near the davit) or to supervise the MASS movements and performance. This presents a very vulnerable situation, and with little room for error, or coincidental events. If the rescue occurs at night two of the crew members would also have to be woken up and made ready on a short notice, something which could be argued to adds another layer of challenges.

5.3.7 Blackout (HAZID node #6.7)

In case of a blackout the MASS operators must ensure successful recovery. Although not explicitly stated as part of the concept descriptions, this could potentially involve several manual actions. Factors which could cause this action to fail are; the low number of crew members compared to the number and sequence of required actions; shortage of time, e.g. in case of drifting close to shore; a high degree of task complexity and unfamiliarity (unless trained on). This risk could be relevant for all the three MASS concepts.

5.3.8 Emergency communication (HAZID node #6.8)

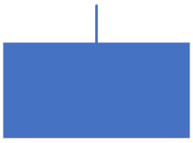
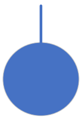
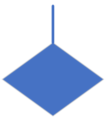
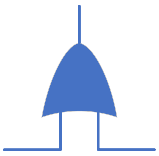
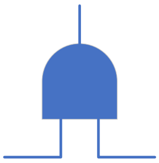
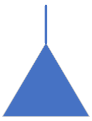
In case of abnormal situations such as fire, collision, grounding or flooding, it will be required to contact search and rescue (SAR) units. During the HAZID discussions it was discussed whether it is realistic to assume that the MASS system is capable of automatically broadcasting the safety messages which are required for successful operations, or whether this is likely to require assistance from the MASS operator. Such accident scenarios can often escalate in an unpredictable way, which could be hard to communicate with automated solutions. Worst case, the vessel will not get the necessary SAR assistance, or get it too late. This risk would be particularly relevant for the ocean-going cargo ship.

6 FAULT TREE ANALYSIS (TASK 1. C)

This chapter documents Task 1.c in Part 1 of the SAFEMASS study; a fault tree analysis (FTA) of potential accident scenarios related to the A3-B1 MASS concepts developed in Task 1.a.

Analytical fault trees were developed based on the hazards, causes and consequences identified in the HAZID. A standard approach to FTA has been applied, similar to what is outlined in the FSA guidelines /8/. Fault tree symbols are explained in Table 11.

Table 11 – Fault tree analysis symbols

	*Event symbol*: A *TOP* event denotes the system failure or accident to be examined. Its causes are deducted as chains (or fault tree branches) of intermediate, basic or undeveloped events. Events can be equipment failure, human errors or environmental factors or normal conditions.
	*Basic event symbol*: The basic event symbol indicates what are considered the most detailed level of causes to be examined, as determined by the purpose of the analysis and availability of data.
	*Undeveloped event symbol*: The undeveloped event symbol indicates events which are (by intention) not examined further in detail, either due to being outside the scope of the analysis or lack of available data.
	*OR-gate*: The OR-gate indicates that the higher-level output event occurs if any of the lower level input events happen.
	*AND-gate*: The AND-gate indicates that the higher-level output event only occurs if all the lower level input events happen at the same time.
	*Transfer-gate*: The transfer gates indicate a transition between other events (and branches) not illustrated in the same diagram, but described elsewhere, e.g. on the next page due to limitations in space.

The FTA's purpose is to provide a visual representation for *deductively* exploring the causal relationship between events which singly or in combination contributes to the occurrence of a higher-level event, commonly referred to as a *TOP* event. Lower level "intermediate" and "basic" events were sorted in a logic structure under two main *TOP* events:

- Collision between MASS and another vessel
- Capsize and sinking of MASS during voyage

The *TOP* events were selected based on what were the most frequently recorded Worst Case outcomes for hazardous events recorded in the HAZID log sheet. Other Worst-Case outcomes were not used as *TOP* events either due to the lack of relevant data captured in the HAZID, or due to not representing emerging risks which are unique to autonomous concepts. Hazards not included as part of the fault trees, but still considered relevant, are discussed in chapter 5.3. The fault tree models are made generic for all three A3-B1 MASS descriptions.

The FTA adopts the HAZIDs focus on operational boundaries (chapter 5.1.1) and the need for operator intervention (chapter 5.1.2). This implies that efforts were made to include and examine events which represent vulnerabilities related to common cause failures and the need for system redundancies. Exceptions can be other types of events which are important to include for overall understanding of the risk picture. A stop rule for what constituted basic events was the level on which events became too correlated and therefore could therefore not be presented as binary events under 'AND' or 'OR' gates.

The FTA diagrams are described in the following sub-chapters, together with descriptions of the fault tree accident scenarios in prose. Note that the diagrams are split into sets of branches due to the size of the fault tree in its entire format not being suitable for reporting on an A4 format. Transfer gates are used to denote the different branches' interfaces and relationships.

For both the fault tree models and the text summaries below, the following definitions are worth taking note of:

- **Vessels involved**: All vessels involved in the scenario, including MASS.
- **Other vessel(s)**: Other vessel(s) than MASS involved in the scenario.
- **MASS**: MASS as an entity, including both automation system and operator(s).
- **MASS system**: The technical automation system not including the operator(s).
- **MASS operator**: MASS operator involved in the scenario.

Basic events are also described using a table format in Appendix D, together with potential causes and RCMs suggested for each basic event. The FTA part of the table includes the following topic columns:

- **FTA ID**: Unique ID for the event – corresponds with the numbers used in the fault tree diagram.
- **Event description**: Brief description of an event identified as a cause contributing to the *TOP* event.
- **Event type**: Categorizes events as either basic events or undeveloped events.
- **Causes**: Failure mechanisms behind each event. In this study focus was on what in the FSA guideline /8/ is referred to as "human-related hazards".
- **Accident scenario**/ sequence of events: Chain of events leading to the *TOP* event.

A quantification of fault tree probabilities has not been performed. Valid data for the modelled events is not available and expert judgement is not considered to provide reliable estimates. Instead, the fault trees were analysed qualitatively to understand and extract *emerging risks* for which RCOs and RCMs were developed.

A summary of emerging risks are provided in sub-chapters 6.2 and 6.4.

6.1 *TOP* Event: Collision between MASS and other vessels

One of the *TOP* events selected for fault tree analysis was collision between MASS and other vessels (ref. scenarios 1-5 described in Table 10).

For this *TOP* event to occur, all the vessels involved first must perform navigational errors causing situations with a reduced safety margin for manoeuvring. Subsequently, either the other vessels and/or MASS must fail in performing last minute collision avoidance (Figure 18).

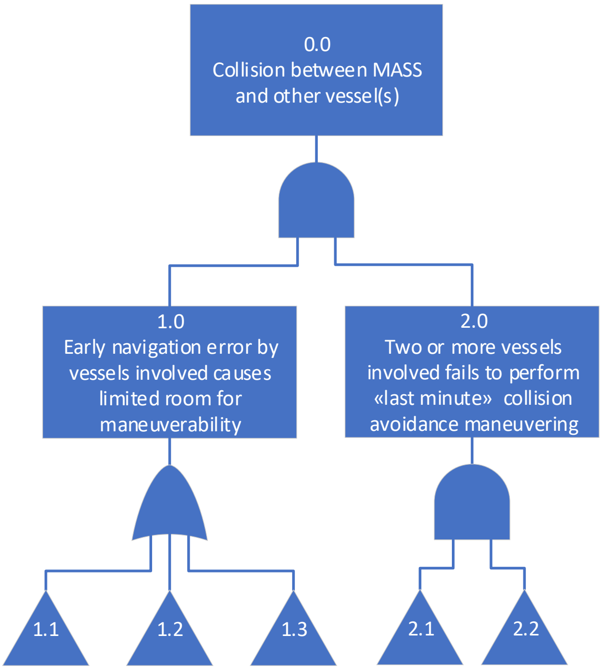

0.0
Collision between MASS and other vessel(s)
1.0
Early navigation error by vessels involved causes limited room for maneuverability
2.0
Two or more vessels involved fails to perform «last minute» collision avoidance maneuvering
1.1
1.2
1.3
2.1
2.2

Figure 18 – Fault tree branches for *TOP* event ID 0.0 (collision between vessels)

6.1.1 Initiating navigation errors

The other vessels (than MASS) can fail in navigating due to several well-known causes (Figure 19), such as officers on watch falling asleep, loss of manoeuvrability due to stuck rudder etc. However, the other vessels may also cause a close traffic situation due to not being willing to comply with rules. Reasons for this can be that they (over-) rely on the MASS to successfully steer away, based on experiences with similar situations previously. Another and perhaps more rare cause could be acts of sabotage or terror, with the intention to cause harm or damage.

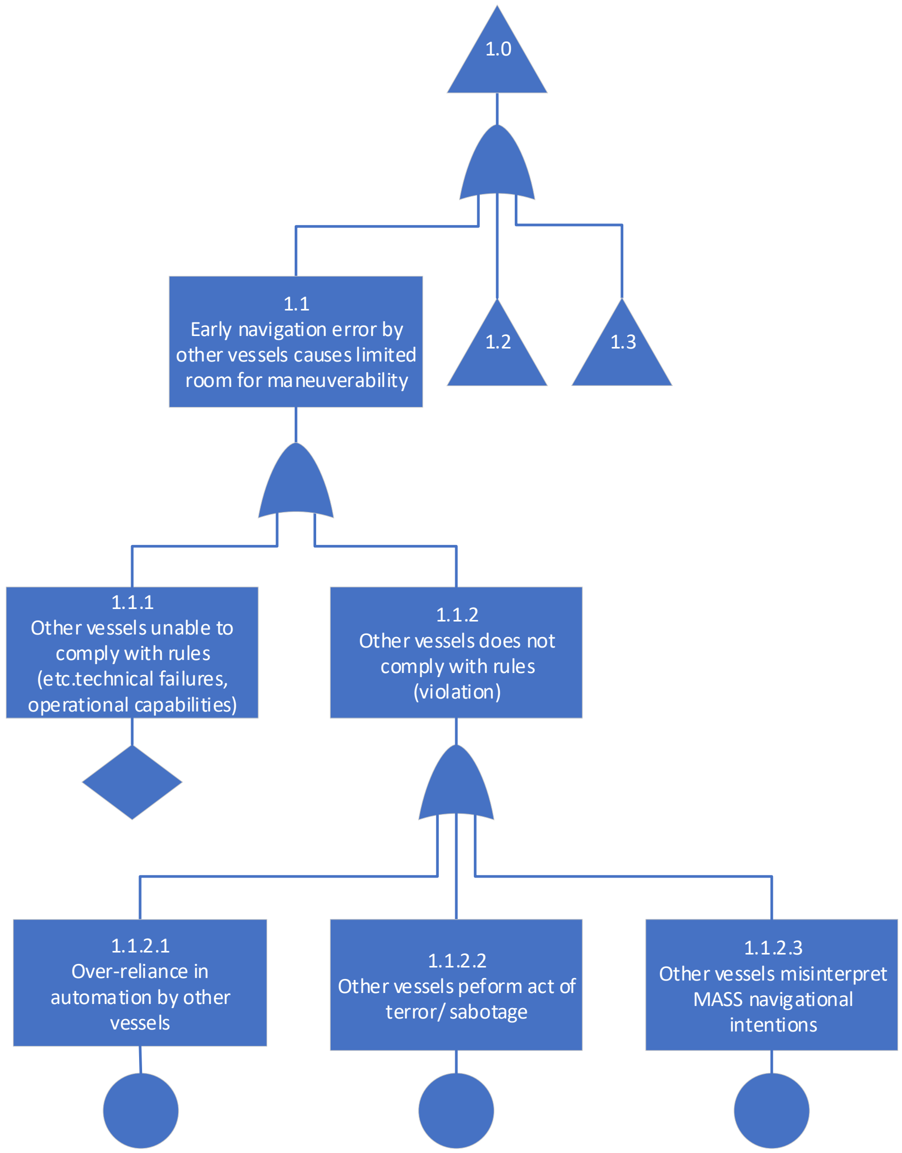

1.0
1.1
Early navigation error by other vessels causes limited room for maneuverability
1.2
1.3
1.1.1
Other vessels unable to comply with rules (etc.technical failures, operational capabilities)
1.1.2
Other vessels does not comply with rules (violation)
1.1.2.1
Over-reliance in automation by other vessels
1.1.2.2
Other vessels peform act of terror/ sabotage
1.1.2.3
Other vessels misinterpret MASS navigational intentions

Figure 19 – Fault tree branches for intermediate event ID 1.1

In case the other vessels navigate successfully, and incident can still be initiated by the MASS (Figure 20). Because navigation within the normal operational state is exclusively performed by the MASS automation system, causes can be attributed to software in addition to pure technical failures e.g. with the propulsion or steering system. The software can be faulty by design, but errors can also be introduced by human interactions, e.g. in case of updates, changes made in set-up and configurations etc.

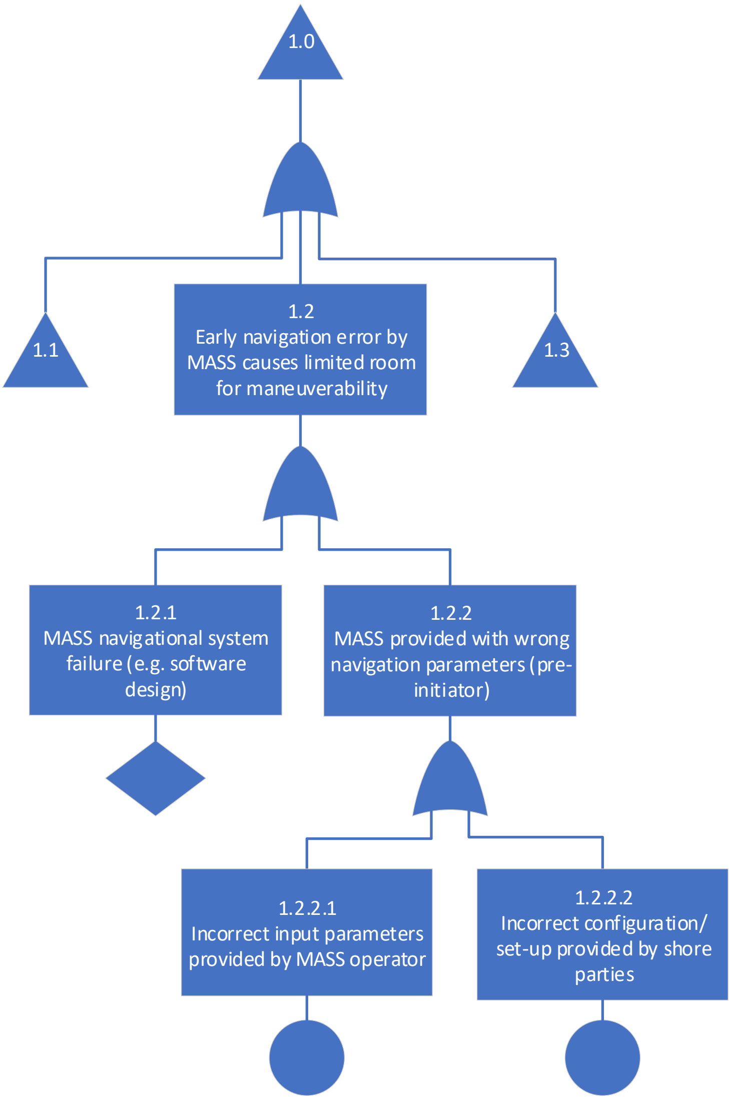

1.0
1.1
1.2
Early navigation error by MASS causes limited room for maneuverability
1.3
1.2.1
MASS navigational system failure (e.g. software design)
1.2.2
MASS provided with wrong navigation parameters (pre-initiator)
1.2.2.1
Incorrect input parameters provided by MASS operator
1.2.2.2
Incorrect configuration/ set-up provided by shore parties

Figure 20 – Fault tree branches for intermediate event ID 1.2

6.1.2 Communication failures

In case navigation errors are performed, a safeguard (but also precondition) for avoiding collision would be to establish communication between the involved vessels at an early stage. The purpose would be to agree on how the situation can be resolved, as explained in below. In case the other vessel intentionally does not comply with rules, for example due to overreliance in MASS automated manoeuvring (beliefs that MASS always will avoid collisions), communication may not always be a robust safeguard.

Both the MASS and other involved vessels can fail in communication (Figure 21). Other vessels can fail to communicate for many of the same reasons' navigation errors occur, e.g. due to the officer on watch falling asleep, breakdown their communication equipment, language challenges etc. The MASS can be unsuccessful at communicating due to technical or software failures in its automated communication system. It may also be able to communicate, but do so poorly, resulting in the message not being understood by the other vessels.

If the MASS' automated communication system fails; the MASS operators can provide some redundancy by acting as back-up. In such a situation the vessels may already have communicated, or attempted to do so, and the MASS operator may not have listened in on the conversations. This assumes he or she is not present at the bridge or in proximity of communication devices.

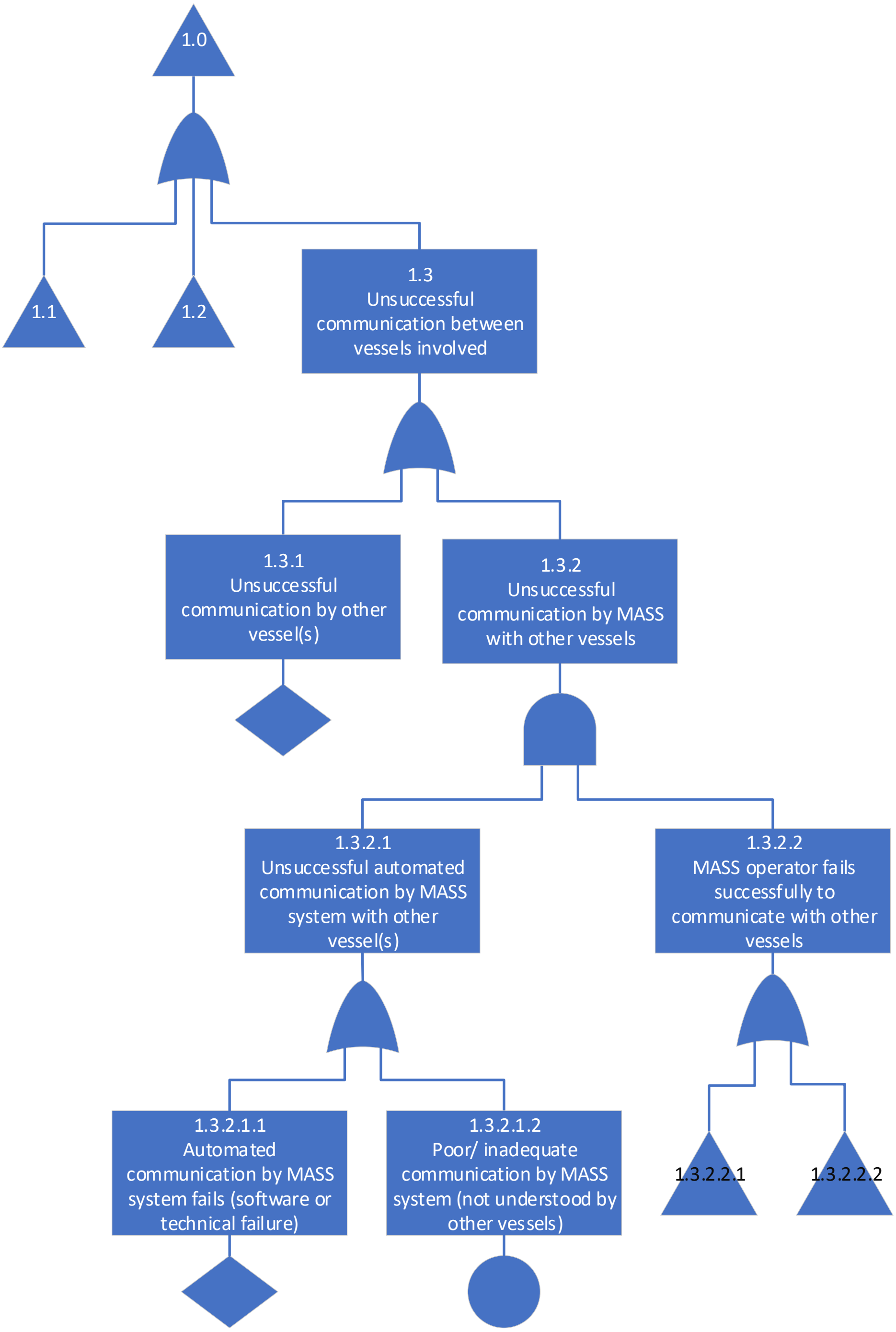

1.0
1.1
1.2
1.3
Unsuccessful communication between vessels involved
1.3.1
Unsuccessful communication by other vessel(s)
1.3.2
Unsuccessful communication by MASS with other vessels
1.3.2.1
Unsuccessful automated communication by MASS system with other vessel(s)
1.3.2.2
MASS operator fails successfully to communicate with other vessels
1.3.2.1.1
Automated communication by MASS system fails (software or technical failure)
1.3.2.1.2
Poor/ inadequate communication by MASS system (not understood by other vessels)
1.3.2.2.1
1.3.2.2.2

Figure 21 – Fault tree branches for intermediate event ID 1.3

Because the MASS operator depends on navigational information to successfully communicate with other vessels, he or she must muster on the bridge in due time to get access of human-machine interfaces (HMI displays) and communication equipment (Figure 22). One risk is that the MASS operator *intentionally* chooses not to muster to the bridge. This can happen because he or she on several previous occasions has experienced that the MASS system has been successful in performing similar operations, i.e. the MASS operator (incorrectly) over-relies in the automation. This effect can be strengthened in case the MASS operator(s) are occupied with other tasks also perceived as critical and/or important. Other influences can be the amount of workload and the lack of clear procedures or other instructions. Such factors can cause the operator to ignore the alarm and instruction about mustering on the bridge. Furthermore, if the alarm is not clear about the event criticality, this may also contribute to the operator relying on the MASS automation system to handle the situation.

The MASS operators may also *unintentionally* not muster on the bridge. This could happen if only one operator is on duty and the portable alarm system fails or for some reason is made unavailable (e.g. lost, dead battery etc.). If the off-duty MASS operator is also unavailable, for example asleep, sick or injured, the event can escalate unnoticed. The MASS operators can also be prevented from mustering on the bridge (or arrive too late), despite being informed about the event. This can happen if the operators are located too far away, compared to how early they are being notified by the alarm system. He or she may also be hindered in re-locating themselves, e.g. if performing work in hard-to-access locations.

Even if the MASS operator(s) successfully musters on the bridge in due time and gets access to communication systems and navigational information, they may still fail to successfully communicate with other vessels. Successful communication is likely to rely on the MASS operator having enough time available to gain sufficient situational awareness. The same causes which can *prevent* the MASS operators from unintentionally mustering to the bridge can also cause a delayed arrival (ref. causes above regarding re-locating, busy doing other tasks etc.). Assuming a delayed arrival, difficulties in achieving situational awareness can occur if the human-machine interfaces (HMI) displaying navigational information do not support quick information acquisition, e.g. due to complex or need for excessive navigation between the relevant images.

Assuming a timely arrival, threats to successful communication can be caused by the MASS operators' skills being degraded from not being familiar with the task due to automation and/or not encountering similar situations either through training or operations.

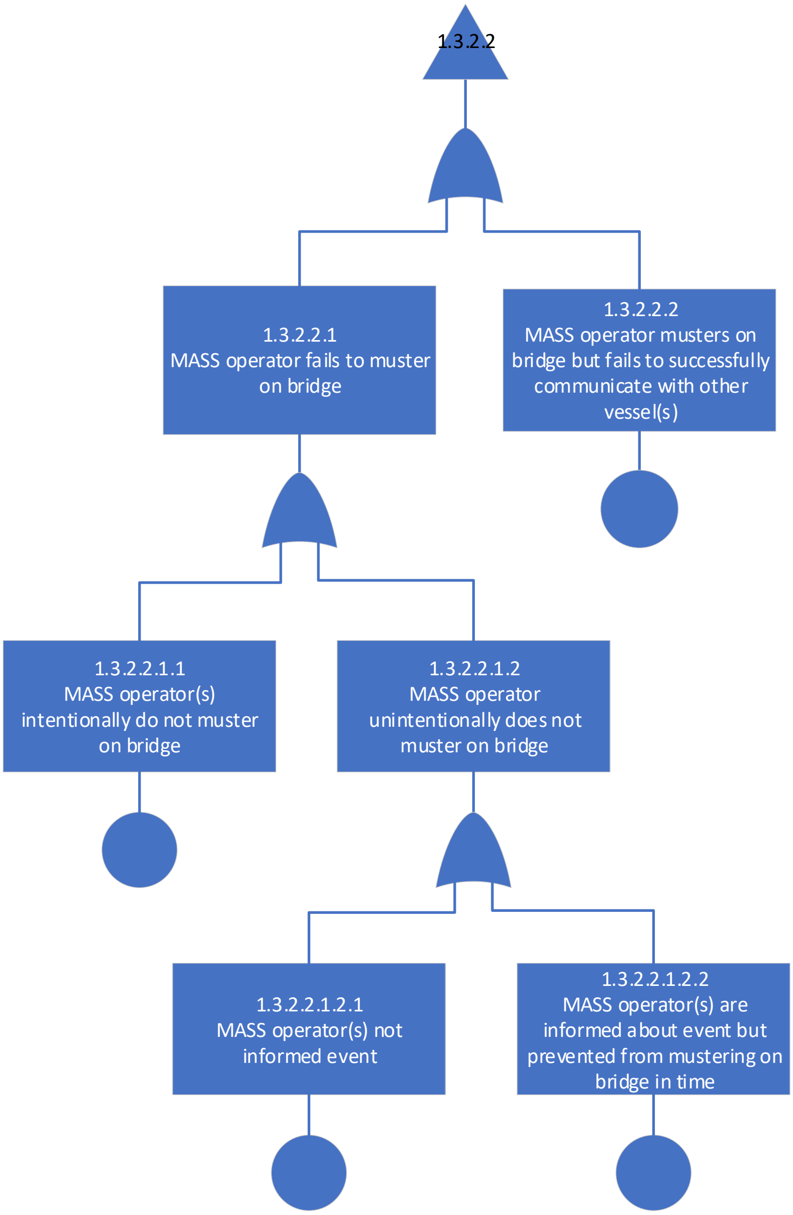

1.3.2.2
1.3.2.2.1
MASS operator fails to muster on bridge
1.3.2.2.2
MASS operator musters on bridge but fails to successfully communicate with other vessel(s)
1.3.2.2.1.1
MASS operator(s) intentionally do not muster on bridge
1.3.2.2.1.2
MASS operator unintentionally does not muster on bridge
1.3.2.2.1.2.1
MASS operator(s) not informed event
1.3.2.2.1.2.2
MASS operator(s) are informed about event but prevented from mustering on bridge in time

Figure 22 – Fault tree branches for intermediate event ID 1.3.2.2

6.1.3 Collision avoidance failures

In case the MASS and other vessels fail in correcting navigational errors at an early stage, safety relies on the ability to perform last minute collision. For a collision to occur, both the MASS and other vessel involved must fail in taking the necessary corrective actions (Figure 23). At this stage the margins are smaller, the vessels' behaviour can be more unpredictable, and there is less time to observe and respond. In such a scenario the MASS can fail by performing last minute navigational violations and thus causing a collision to happen (error of commission), or by failing to take the actions necessary to avoid collision (error of omission). Similar to how software issues could cause the MASS system to perform initial navigational errors, they can also be the sources of wrong actions (violations) being performed in a more complex traffic scenario.

Another and perhaps more critical scenario can occur if the MASS operator fails after incorrectly intervening with successful MASS system performance. This can happen if he or she does not trust or misinterprets the decisions and actions taken by the MASS system. Reasons for distrust can be earlier experiences with sub-optimal performance by MASS, or if the MASS behaviour appears as strange or unpredictable for the MASS operators. Another well-known phenomenon (e.g. from aviation) and source for misinterpretation is the human failure mode known as “mode confusion”. This occurs when the operator believes the system is doing something it is not, or in a different way.

Although the MASS may not be responsible for performing any manoeuvring violations or errors, it still needs to perform collision avoidance if the other vessels are close and maintains a collision course. At an early stage in the scenario the MASS system will continuously try to regain a normal operational state. Re-gaining normal operations can fail if the situation escalates to a point where the MASS system’s navigational capabilities are exceeded. Other failure mechanisms can be poorly designed/ faulty software, or incorrect configuration or input during operations. In any case, when exceeding a defined parameter, the MASS system will attempt to enter an MRC. This can fail for similar software-related reasons, but the most obvious source of failure is whether an MRC has been defined accurately enough for the encountered scenario.

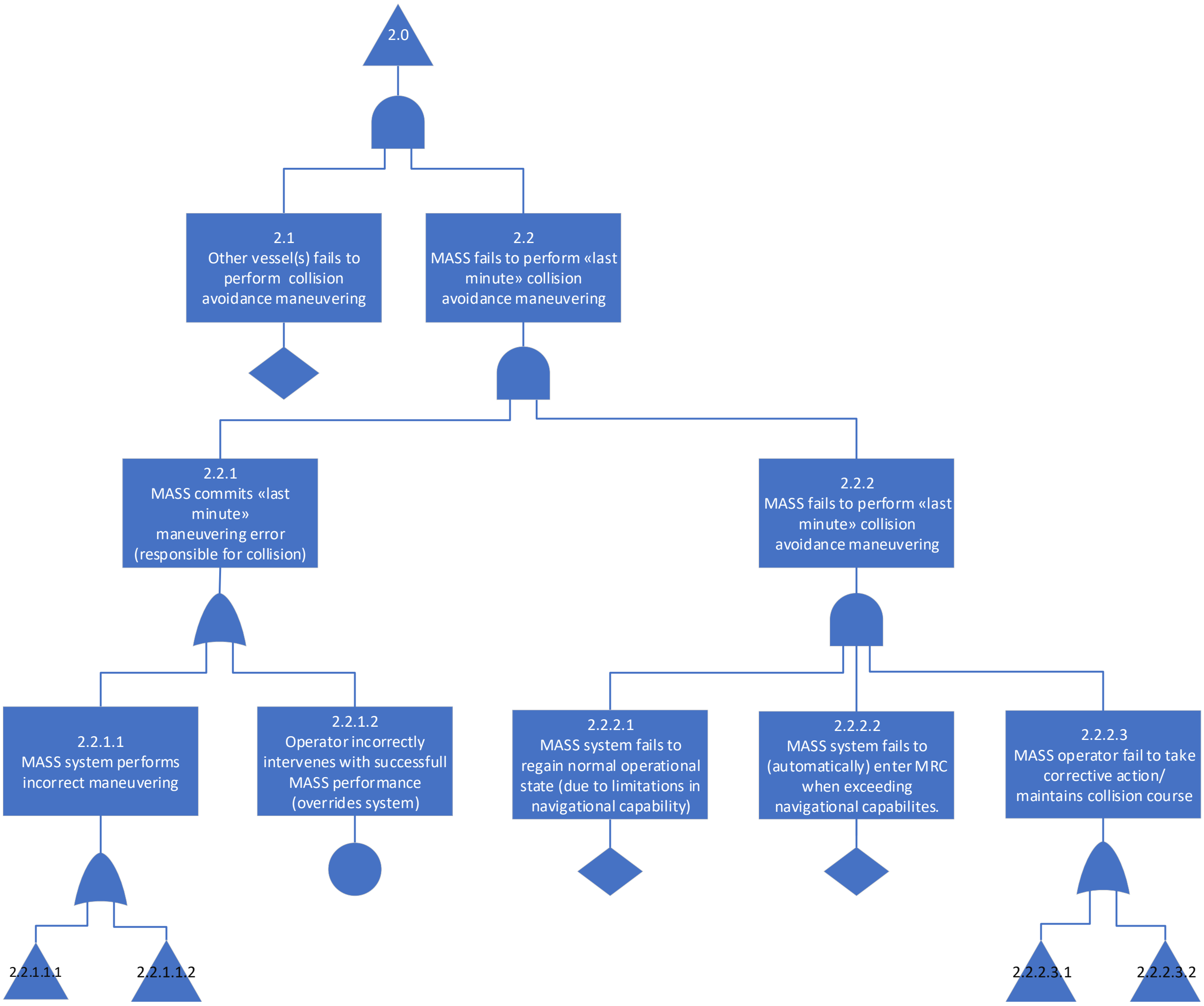

2.0
2.1
Other vessel(s) fails to perform collision avoidance maneuvering
2.2
MASS fails to perform «last minute» collision avoidance maneuvering
2.2.1
MASS commits «last minute» maneuvering error (responsible for collision)
2.2.2
MASS fails to perform «last minute» collision avoidance maneuvering
2.2.1.1
MASS system performs incorrect maneuvering
2.2.1.2
Operator incorrectly intervenes with successfull MASS performance (overrides system)
2.2.2.1
MASS system fails to regain normal operational state (due to limitations in navigational capability)
2.2.2.2
MASS system fails to (automatically) enter MRC when exceeding navigational capabilites.
2.2.2.3
MASS operator fail to take corrective action/ maintains collision course
2.2.1.1.1
2.2.1.1.2
2.2.2.3.1
2.2.2.3.2

Figure 23 – Fault tree branches for intermediate event ID 2.0

A safeguard for unsuccessful automated MRC is having notified and instructed the MASS operator to supervise the operation and intervene if required (Figure 24 and ID 2.2.2.3 in Figure 23). This way the MASS operator works as the final safeguard to prevent a collision. If the MASS operator fails to muster to the bridge, or musters too late, he or she is likely to fail in successfully overriding the system and take control. The casual mechanisms are similar as for communication failures (Figure 22) described above in sub-chapter 6.1.2 (see *intentionally/ unintentionally* not mustering on the bridge).

The MASS operator can fail in supporting the MASS system's attempt to enter an MRC despite being able to muster. If he or she is late, the above-mentioned challenges with gaining situational awareness soon enough are likely to be present. This can happen if the operator struggles with acquisition of information such as weather conditions, vessel location, speed and heading etc. Furthermore, in such a scenario the MASS operator will be supervising the MASS system before suddenly having to intervene, possibly on a short notice. So, even if situational awareness has successfully been gained, the MASS operator can still be prone to commit errors in performing the actions he or she decided to execute. Contributors to unreliable human performance can be that the HMI is not suitable for use in situations pressed on time. Also, as with the communication tasks – if manoeuvring is normally done by the

MASS system, the skills of the MASS operators may degrade unless they are being sufficiently compensated by proper training.

Lastly, the MASS operator can also muster on the bridge in due time but hesitate to intervene due to the impact of stress on decision-making. This hesitation can be strengthened if the MASS operators have more trust in the automated MASS system than in one's own skill set, e.g. as a result from skill degradation and insufficient training.

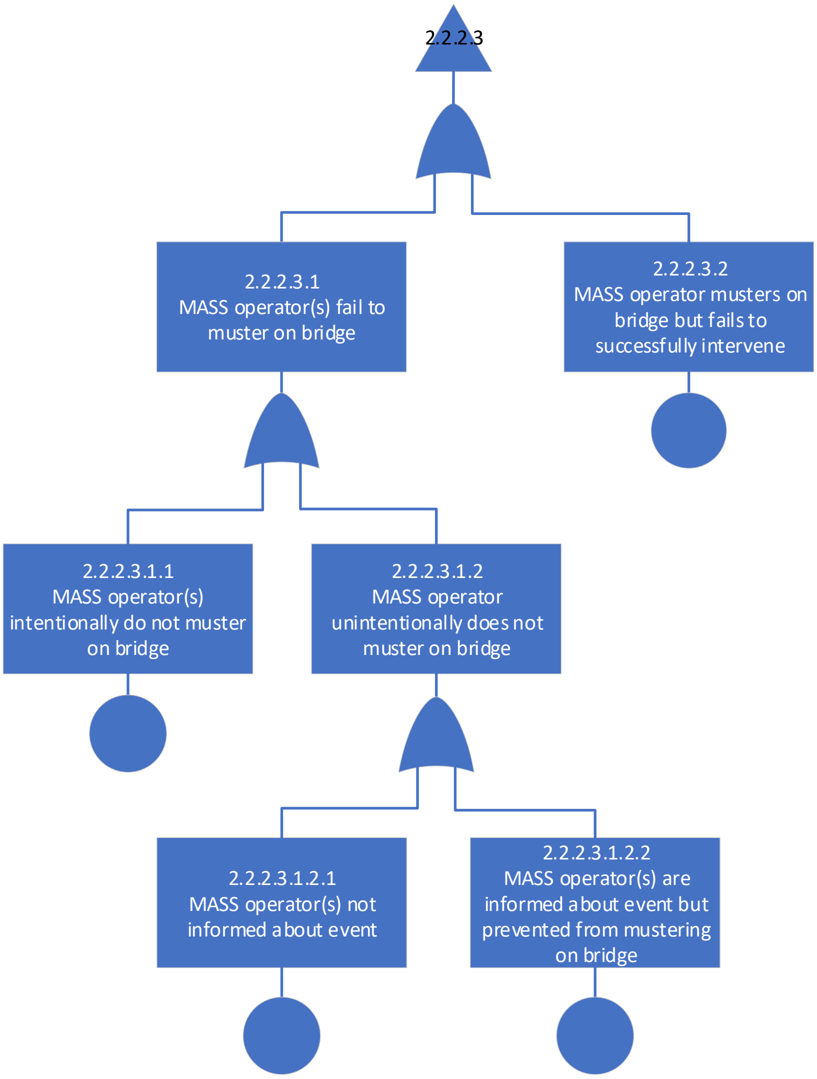

2.2.2.3
2.2.2.3.1 MASS operator(s) fail to muster on bridge
2.2.2.3.2 MASS operator musters on bridge but fails to successfully intervene
2.2.2.3.1.1 MASS operator(s) intentionally do not muster on bridge
2.2.2.3.1.2 MASS operator unintentionally does not muster on bridge
2.2.2.3.1.2.1 MASS operator(s) not informed about event
2.2.2.3.1.2.2 MASS operator(s) are informed about event but prevented from mustering on bridge

Figure 24 – Fault tree branches for intermediate event ID 2.2.2.3

6.2 Emerging risks associated with collision scenarios

When applying an interpretation of the A3-B1 level similar to what is described in chapter 4.1.2, the study suggests that several risks appear to emerge from "human-in-the-loop"-related issues. The following sub-chapters elaborate on some of the key risks mentioned in the *TOP* event description above.

6.2.1 Situational awareness challenges

Several of the human-in-the-loop issues, in various ways, represent factors which challenge the MASS operators' situational awareness (SA). SA can be defined as the perception of environmental elements and events with respect to time or space, the comprehension of their meaning, and the projection of their future status /9/. As can be seen in Figure 25 /10/, different contextual and individual factors can have an influence on the operator's ability to experience SA. The following sections explain how the A3-B1 level potentially can introduce factors which has a negative impact on the MASS operators' SA, decision-making and performance of action.

While the findings are primarily based on the FTA of collision scenarios, they are also relevant for other risks such as contingency response actions in FTA of loss of buoyancy/ stability events (see chapter 6.3).

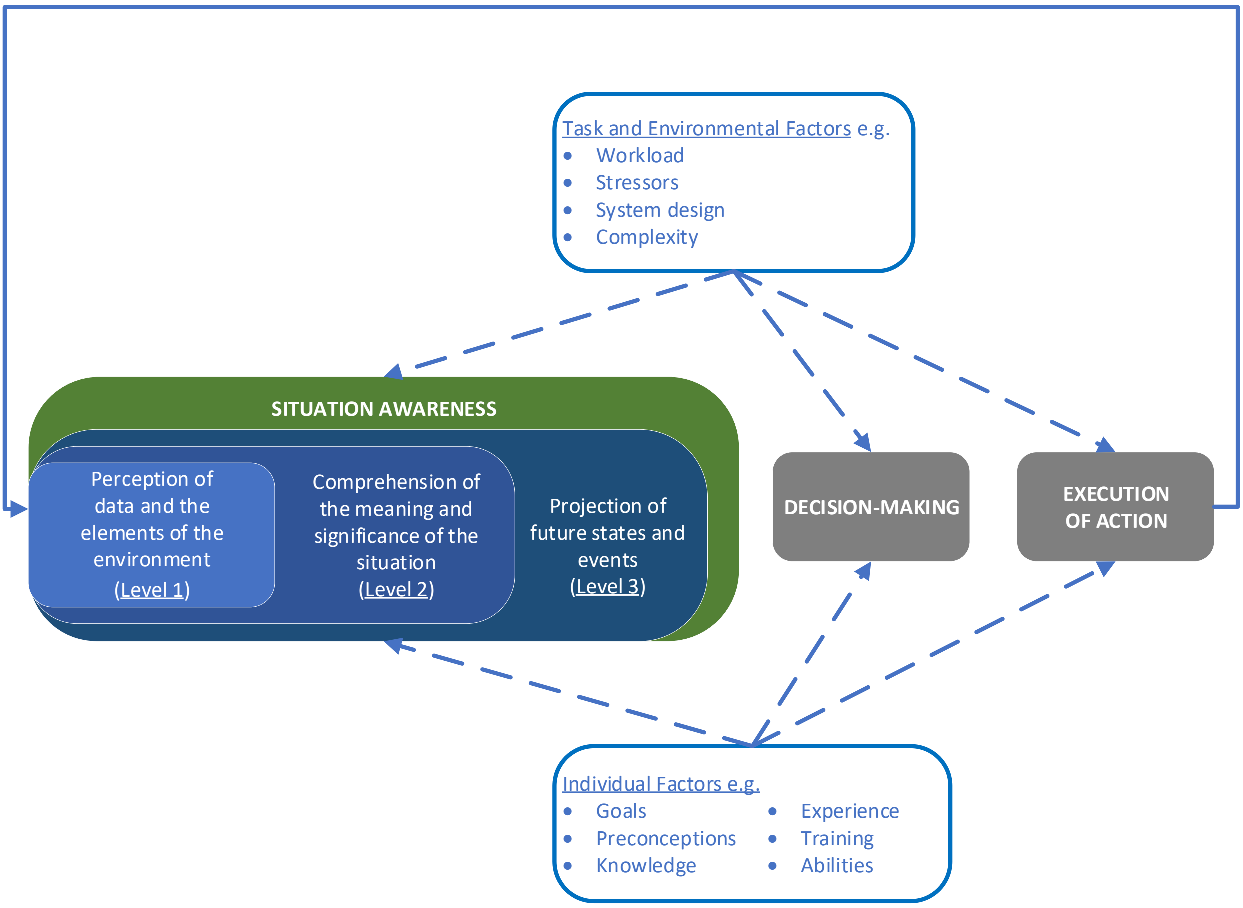

Task and Environmental Factors e.g.
Workload
Stressors
System design
Complexity
SITUATION AWARENESS
Perception of data and the elements of the environment (Level 1)
Comprehension of the meaning and significance of the situation (Level 2)
Projection of future states and events (Level 3)
DECISION-MAKING
EXECUTION OF ACTION
Individual Factors e.g.
Goals
Preconceptions
Knowledge
Experience
Training
Abilities

Figure 25 – Endsley's model of SA. This is a synthesis of versions she has given in several sources, notably Endsley (1995a) and Endsley et al (2000) /10/

By definition, with A3-B1 the MASS system is responsible for maintaining its own SA without any human involvement as long as it is operating inside the envelope of what is considered as normal operations. The MASS operator is periodically left out of the "automation loop" for shorter or longer periods of the time, meaning he or she does not supervise or monitor MASS operations unless notified to do so. Notifications, such as warnings and alarms, are only provided when the MASS recognizes it is outside pre-defined parameters or in emergencies.

The time available for the operator to gain SA, before potentially having to decide about whether and how to intervene, then depends on how these parameters are defined and what constitutes emergencies. One example of this is how early the MASS operator is notified in case of a vessel being on collision course.

It is assumed that a A3-B1 MASS both knows what these parameters are and is capable of recognizing when operator assistance is required. The parameters can be dynamic, for example by being more conservative for parts of a voyage considered to be more critical than others, e.g. due to high traffic density. The threshold for notifying the MASS operator can thus be made lower when the surroundings are complex and unpredictable.

Nevertheless, A3-B1 represents the highest level of automation, and by its definition it can be assumed that the MASS operator is primarily meant to override the system only in case boundary parameters are exceeded. This suggests that human intervention only happens on rare occasions.

Building on the knowledge gained from the study, successful human intervention is likely to depend on;

- the MASS operator(s) being informed by the MASS system (and in due time),
- the MASS operator(s), when informed, being able to (re-)locate him-/herself to the bridge or other location where the controls and information displays are available,
- the MASS operator(s) being able to obtain the required SA within the time available,
- the MASS operator(s) knowing how and when to respond and having the necessary skills to do so.

Table 12 summarizes the main risks identified in the HAZID and FTA which can potentially threaten successful human involvement in MASS designed and operated according the A3-B1 level of autonomy and control.

Table 12 – Summary of main risks associated with human intervention in case of collision

Human intervention	Main risks
The MASS operator(s) is informed by the MASS system, and in due time.	• Boundary parameters and MRCs are missing/ not defined, or incorrectly defined. • Alarms are not perceived, e.g. due to noisy environments, poor alarm design. • Alarm system fails, e.g. portable alarm runs out of battery.

Human intervention	Main risks
	• Operator does not carry or have the portable alarm device available.
The MASS operator(s) can, when informed, (re-)locate him-/herself to the bridge or other location where the controls and information displays are available.	The operator(s) intentionally does not muster to bridge due to: • Overreliance on the MASS system automation due to having frequently observed successful performance in similar situations. • Prioritizing other tasks due to high workload and/ or perceived importance and criticality of tasks. The operator(s) unintentionally does not muster to the bridge, or musters too late, due to: • Being located too far away from the bridge, or in a location which is time consuming to leave from (e.g. a tank). • Vulnerability associated with low manning level and not being able to be a back-up resource, e.g. the operator off-duty is asleep or sick, while the operator on-duty fails to observe and/ or respond to the alarm.
The MASS operator(s) is able to obtain the required SA within the time available.	• Design of human-machine interfaces (HMI) and other displays does not support (rapid) acquisition and analysis which enables the operator to fully enter the "automation loop" (i.e. enables correct decision making).
The MASS operator(s) knows how and when to respond and has the necessary skills to do so.	• Skill-deterioration due to high level of automation/ infrequent manual control (particularly of demanding operations. • Reliance and trust in automation over own skill set. • Mode confusion or distrust causing the operator to incorrectly override successful MASS system performance. • Decision-making being impacted by stressful situations, e.g. due to perceived criticality and limited available time. With the operator's role being to intervene when the A3-B1 exceeds its capabilities, this context can be expected.

6.2.2 Mode confusion and (dis-)trust in automation

As indicated in Table 11, the risk analysis identified "mode confusion" and level of trust or reliance in automation as a contributing cause for several human error related events, especially related to collision avoidance manoeuvring. Mode confusion /16/ occurs when the crew believes they are in a mode different than the one they are actually in and consequently make inappropriate requests or responses to the automation. In such a case it is likely that the MASS operator also has an incorrect or incomplete situational awareness, which causes him or her to wrongly override the system. The same faulty awareness can also be expected to induce human failure when taking manual control, in what can be a stressful situation with little or no room for making errors.

The level of (dis-)trust in automation is closely related to mode confusion in that they both can be caused by a lack of or incorrect situational awareness. It differs however by how the operator is more conscious about the automated system’s performance, compared to mode confusion which often occurs without the operator being aware of it. In the context of automation, trust can be defined as “the attitude that an agent (here: MASS system) will help achieve an individual’s goals in a situation characterized by uncertainty and vulnerability” /11/. A too high level of trust or overreliance can cause the operator to be complacent and indifferent of his or her role and responsibilities in the control loop. Oppositely, result of distrust is that the operator intentionally overrides the automated system because he or she have more trust in their decision-making and actions.

At first glance the FTA revealed that mode confusion, distrust and overreliance in automation were identified as risks both for events occurring at both an early and late stage in the accident sequence. This is reflected upon in chapter 6.1.3 and documented in the combined FTA and RCO table (Appendix D). However, a closer examination of the fault tree model also revealed that mode confusion and distrust represent some of the most critical hazards in case of last-minute collision avoidance. If the MASS operators incorrectly intervene with successful MASS performance, either in regaining a normal operational state, or in entering an MRC, there is a risk that two “last resort” barriers are lost at the same time. The first barrier is the MASS system attempting to enter a safe state, and the second barrier is the MASS operator who is supposed to assist the MASS system in case it exceeds its capabilities. This way mode confusion and distrust can be the mechanisms behind making the MASS operator a source of a “common cause failure”.

6.3 *TOP* Event: Loss of stability/ buoyancy during voyage

Another *TOP* event selected for FTA was Loss of stability/ buoyancy during voyage (ref. scenarios 6-8 described in Table 10).

In this scenario the *TOP* event (Figure 26) occurs when the vessel encounters a stability failure in heavy weather combined with being exposed to water ingress. Furthermore, the MASS system and MASS operator must jointly perform incorrect damage stability contingencies for loss of stability / buoyancy to occur. At the level of analysis performed in this study the risks would be comparable to those associated with collision avoidance identified in the FTA reported in chapter 6.1.3 (see fault tree branches for event ID 2.2 in Figure 23). The main difference would be that the MASS operator performs tasks related to stability contingencies instead of collision avoidance. As such, the FTA for loss of stability is limited to include this risk as an undeveloped event (see event ID 3.0 in Figure 26).

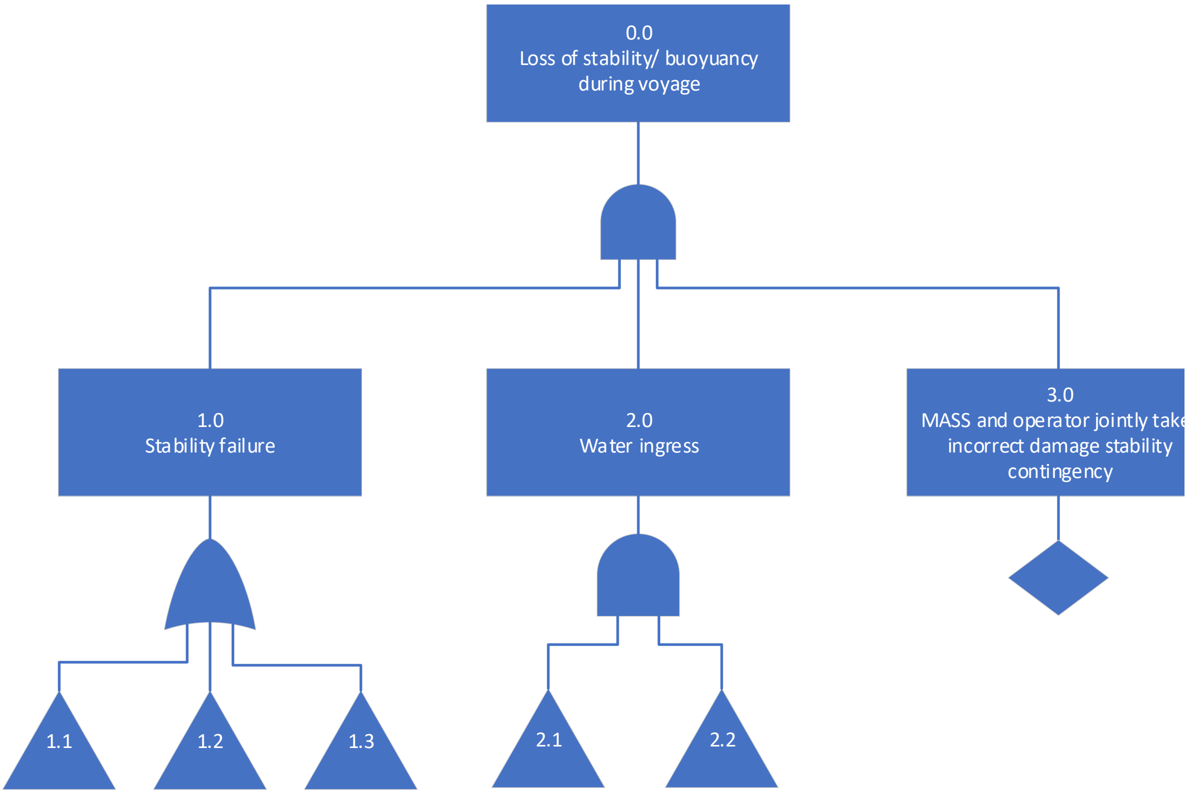

0.0
Loss of stability/ buoyuancy during voyage
1.0
Stability failure
2.0
Water ingress
3.0
MASS and operator jointly take incorrect damage stability contingency
1.1
1.2
1.3
2.1
2.2

Figure 26 – Fault tree branches for *TOP* event ID 0.0 (loss of stability/ buoyancy)

6.3.1 Stability failure

The stability failure encountered can mainly be caused by three initiating events. One is incorrect pre-departure stability condition; a second cause can be incorrect transfer of internal liquid loads (e.g. ballast water, fuel, fresh water etc); and a third is that cargo shifts during voyage. The latter cause will depend on ship type in question.

Incorrect pre-departure stability condition refers to the stability calculations which is conducted prior to voyage (Figure 27). It is during this stage that the MASS stability system or loading computer is interfaced with various sensors comparing calculated stability condition with online data. To achieve an accurate calculation the system depends on correct cargo data such as weight and volume. While most conventional vessels receive this data through the cargo manifest, the MASS can potentially check the actual weight through cargo handling system interface (e.g. crane, conveyor belt). Nevertheless, errors cannot be excluded which will result in an incorrect stability calculation. Likewise, wrong data can be received when loading fuel, fresh water, provision or when transferring ballast internally in port. On traditional ships, the actual draft of the vessel is inspected visually by the ship crew and compared with the calculated draft before departure. Lack of a similar control on MASS would increase the risk of stability failure.

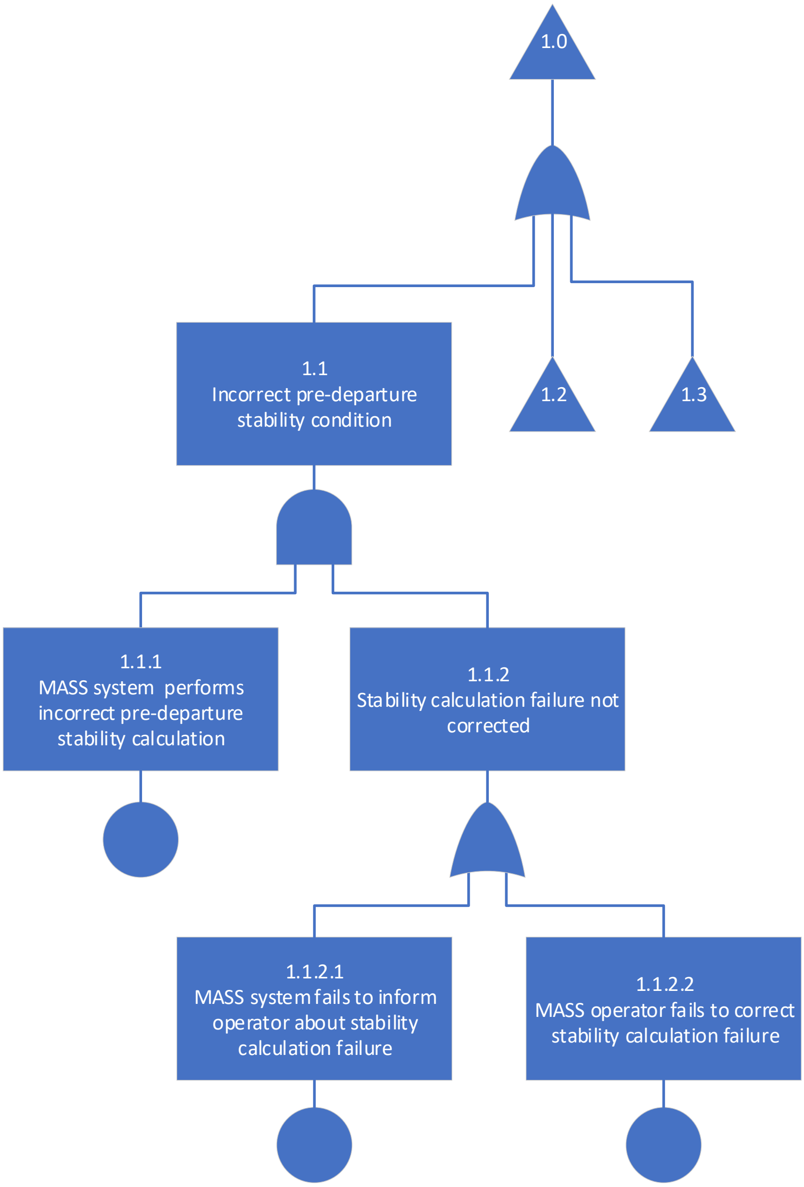

1.0
1.1
Incorrect pre-departure stability condition
1.2
1.3
1.1.1
MASS system performs incorrect pre-departure stability calculation
1.1.2
Stability calculation failure not corrected
1.1.2.1
MASS system fails to inform operator about stability calculation failure
1.1.2.2
MASS operator fails to correct stability calculation failure

Figure 27 – Fault tree branches for intermediate event ID 1.1

During transit the vessel is exposed to external factors such as wind or internal factors such as change of internal liquid loads (e.g. ballast water, fuel, fresh water etc). The MASS will attempt to manage these forces by transferring liquid loads to achieve best possible stability condition (Figure 28). However, such systems are dependent on correct sensor data which leaves it vulnerable to lack of robustness and redundancy. If for instance the system relies fully on one sensor which incorrectly indicates a high angle of heel, the system could continue transferring ballast until stopped by the operator. Similar errors could occur if tank sensors provide incorrect input such as indicating empty instead of full.

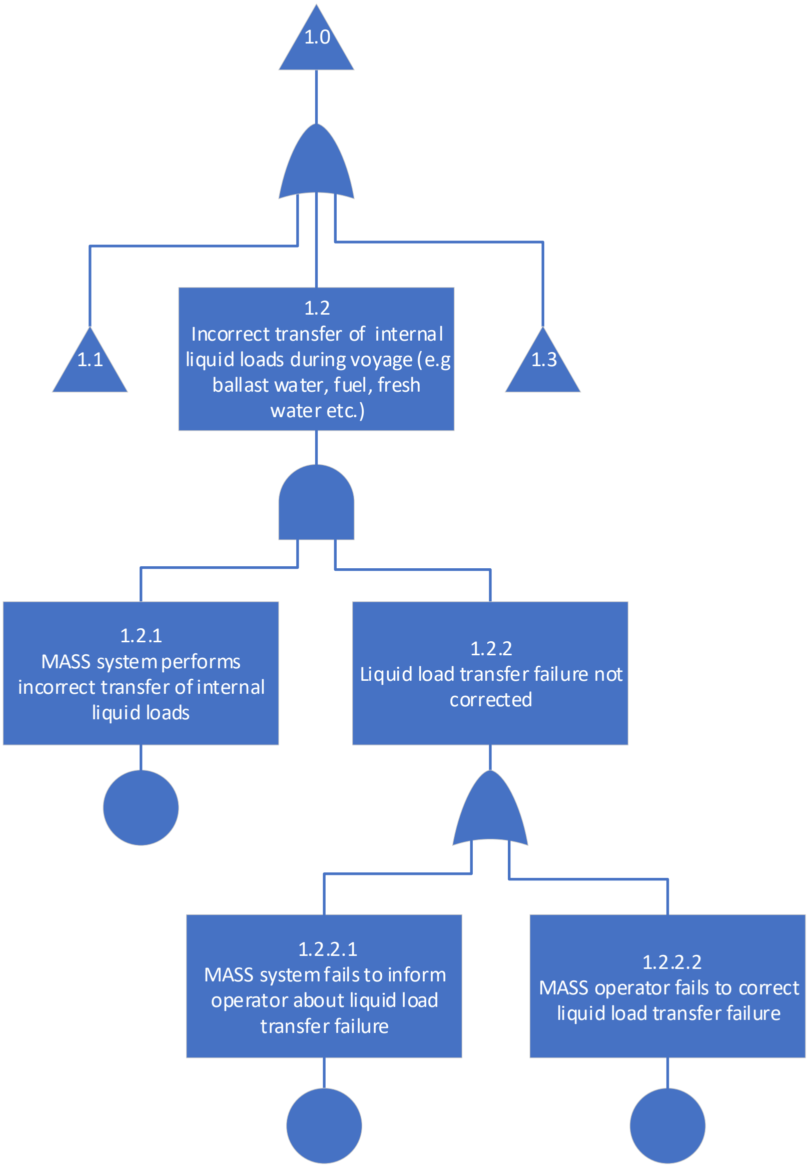

1.0
1.1
1.2
Incorrect transfer of internal liquid loads during voyage (e.g ballast water, fuel, fresh water etc.)
1.3
1.2.1
MASS system performs incorrect transfer of internal liquid loads
1.2.2
Liquid load transfer failure not corrected
1.2.2.1
MASS system fails to inform operator about liquid load transfer failure
1.2.2.2
MASS operator fails to correct liquid load transfer failure

Figure 28 – Fault tree branches for intermediate event ID 1.2

Furthermore, in the event of cargo shifting during a voyage, the result could be stability failure. However, the consequence of the stability failure depends highly on the ship type and cargo. Nevertheless, the reason for such an event to occur can largely be divided in to two factors; the quality of cargo securing and the degree of vessel movement (Figure 29). The cargo should be secured to withstand vessel movement within certain environmental parameters but cannot be expected to survive all conditions (e.g. hurricane).

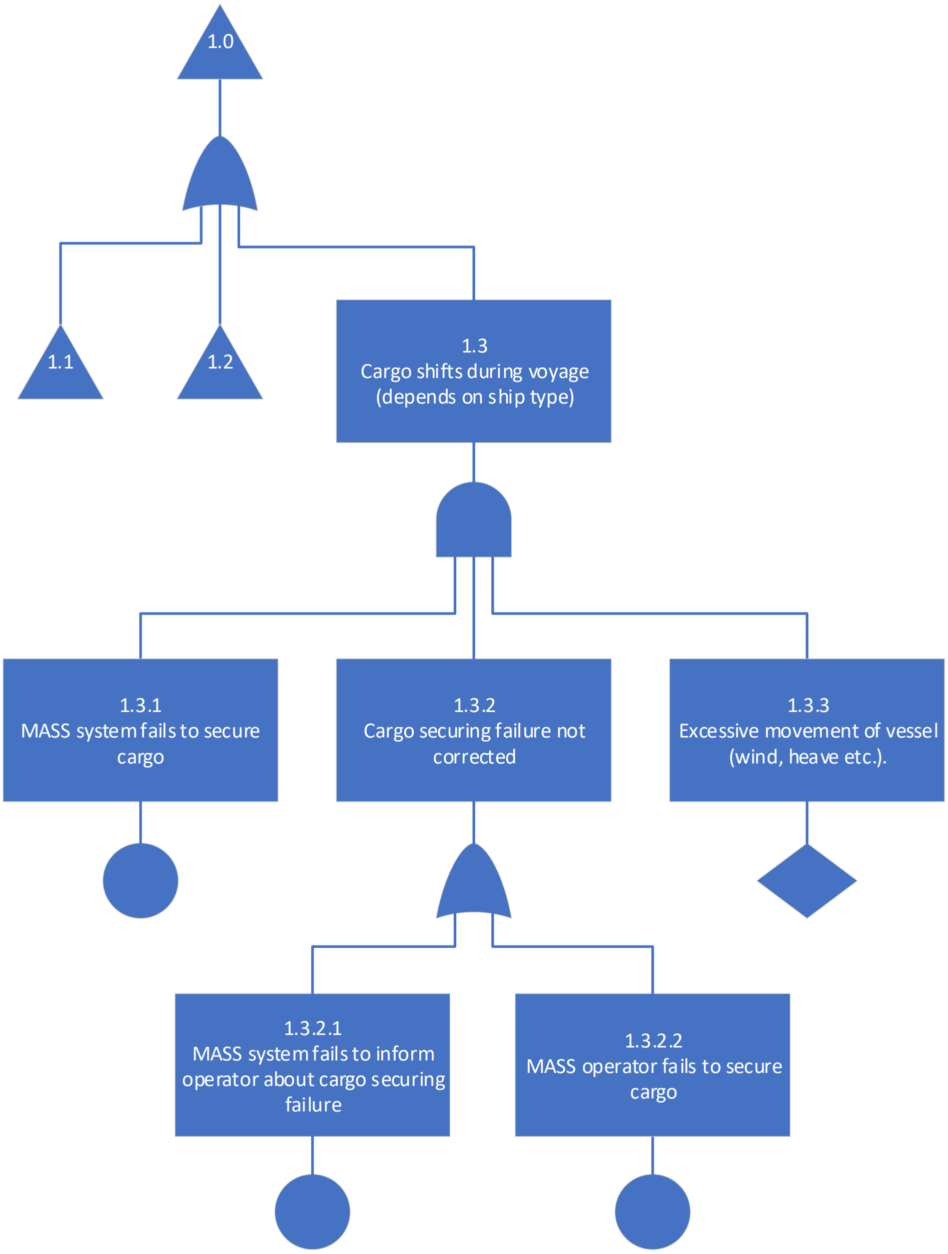

1.0
1.1
1.2
1.3
Cargo shifts during voyage
(depends on ship type)
1.3.1
MASS system fails to secure cargo
1.3.2
Cargo securing failure not corrected
1.3.3
Excessive movement of vessel (wind, heave etc.).
1.3.2.1
MASS system fails to inform operator about cargo securing failure
1.3.2.2
MASS operator fails to secure cargo

Figure 29 – Fault tree branches for intermediate event ID 1.3

6.3.2 Water ingress

Two main events can cause water ingress; loss of watertight integrity combined with green seas on deck. This scenario is exemplified based on the bulk vessel, but similar events would cause similar *TOP* events to occur for the other vessels.

The loss of watertight integrity for the bulk vessel is restricted to water ingress to the cargo holds which is caused either by an unsecured or damaged cargo hatch (Figure 30 and Figure 31). The MASS is equipped with a cargo hatch securing system with sensors indicating if the hatch is in secured position. Consequently, a change in sensor status could indicate a possibility for water ingress which would need to be inspected and corrected.

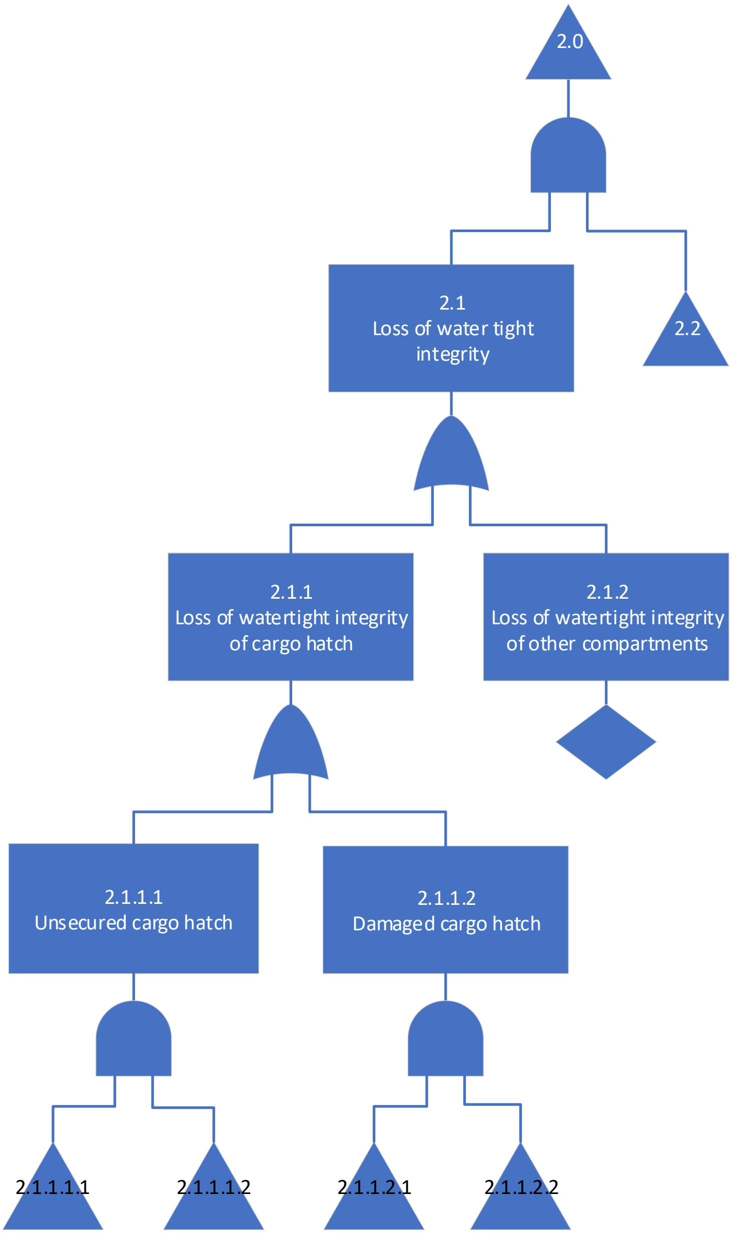

2.0
2.1
Loss of water tight integrity
2.2
2.1.1
Loss of watertight integrity of cargo hatch
2.1.2
Loss of watertight integrity of other compartments
2.1.1.1
Unsecured cargo hatch
2.1.1.2
Damaged cargo hatch
2.1.1.1.1
2.1.1.1.2
2.1.1.2.1
2.1.1.2.2

Figure 30 – Fault tree branches for intermediate event ID 2.1

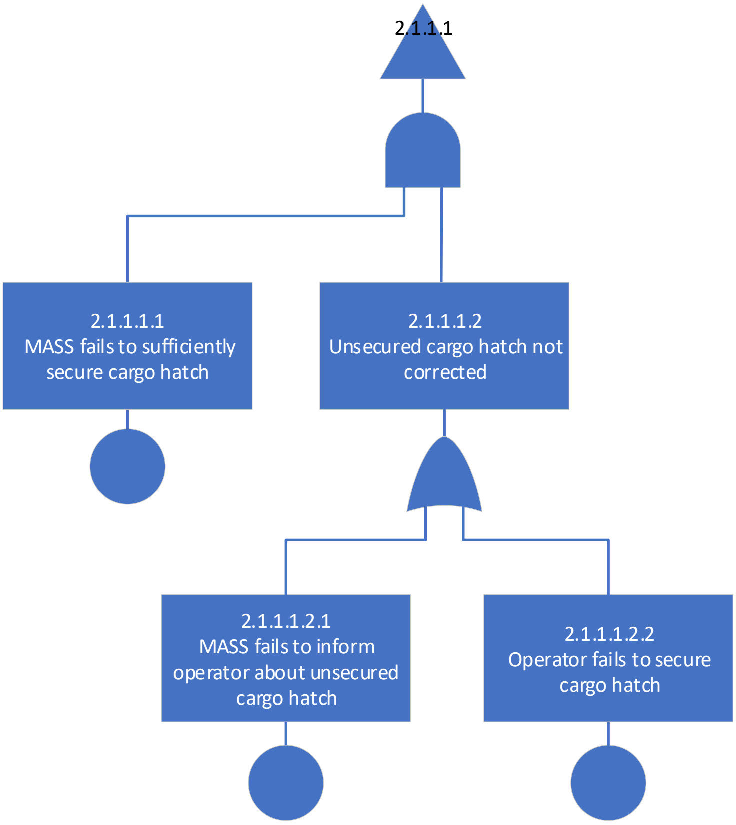

2.1.1.1
2.1.1.1.1
MASS fails to sufficiently secure cargo hatch
2.1.1.1.2
Unsecured cargo hatch not corrected
2.1.1.1.2.1
MASS fails to inform operator about unsecured cargo hatch
2.1.1.1.2.2
Operator fails to secure cargo hatch

Figure 31 – Fault tree branches for intermediate event 2.1.1.1

Likewise, a change of sensor status could indicate contact damage between cargo hatch and unsecured loose objects (Figure 32). As the MASS depends on third party personnel to conduct various service and maintenance in port an increased risk of leaving unsecured objects on deck can be expected. Especially if nobody is inspecting the vessel for loose objects prior to departure. The potential loose objects can range from smaller oil drums to larger cargo loading systems such as cranes or pallet trucks. Such objects may inflict damage on the cargo hatch depending on the object size and velocity. To mitigate this risk the MASS is equipped with a camera and sensor-based system to identify any potential loose objects.

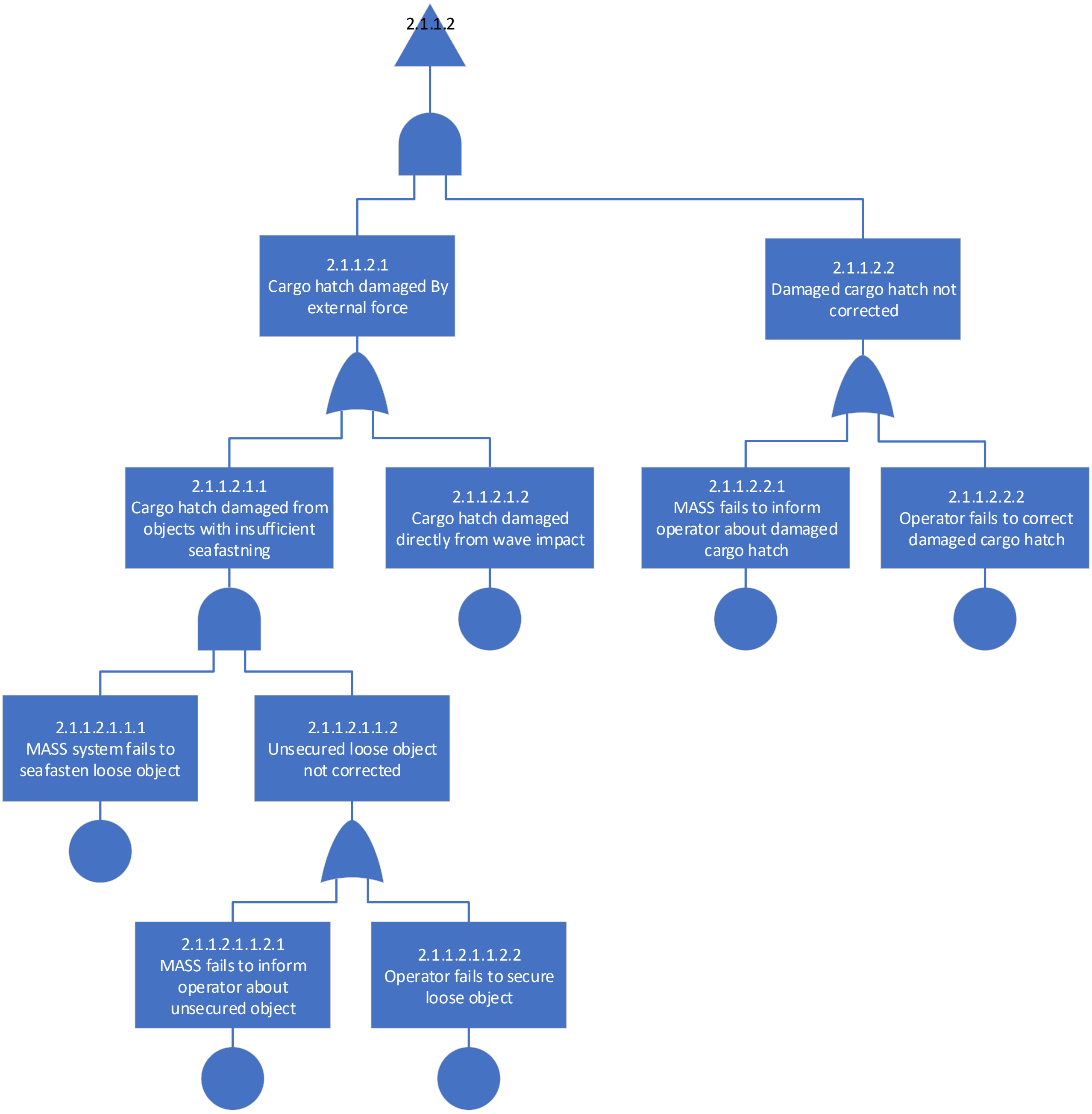

2.1.1.2
2.1.1.2.1
Cargo hatch damaged By external force
2.1.1.2.2
Damaged cargo hatch not corrected
2.1.1.2.1.1
Cargo hatch damaged from objects with insufficient seafastning
2.1.1.2.1.2
Cargo hatch damaged directly from wave impact
2.1.1.2.2.1
MASS fails to inform operator about damaged cargo hatch
2.1.1.2.2.2
Operator fails to correct damaged cargo hatch
2.1.1.2.1.1.1
MASS system fails to seafasten loose object
2.1.1.2.1.1.2
Unsecured loose object not corrected
2.1.1.2.1.1.2.1
MASS fails to inform operator about unsecured object
2.1.1.2.1.1.2.2
Operator fails to secure loose object

Figure 32 – Fault tree branches for intermediate event ID 2.1.1.2

Even though the cargo hatch is left exposed, water ingress will normally not occur without green seas on deck (Figure 33). For this to happen, the MASS system has either performed a poor voyage planning before departure or conducted a failure in weather routing / voyage optimization during voyage. Several factors can influence the quality of the voyage plan, but most concern the use of relevant data. In the bulk vessel case, the use of correct weather data is highly weighted. As the vessel is conducting a longer voyage, passing the exposed north Atlantic Ocean, the larger weather systems need to be considered. Such data can be retrieved from several data sources and can be weighed against each other. The risk of choosing the wrong data source in this phase could ultimately be to end up in a position where heavy weather damage is unavoidable.

Furthermore, green seas on deck can occur during voyage either by not responding to the changing weather conditions or conducting an incorrect change of route by prioritizing other parameters such as route optimization. The MASS system will constantly measure the current weather conditions through sensors and compare it to the latest weather conditions. This data will be used to calculate the best route to avoid weather damage and reduce transit time by voyage optimization. As a result, the risk of heavy weather damage will depend on the parameters for weighting the importance of voyage optimization versus avoidance of heavy weather. Common for all the above failure modes is that the system will attempt to notify the operator and request assistance in trouble shooting, and to resolve the problems which caused the notification or alarm. Emerging risks related to human element issues and system redundancy is discussed in more detail below.

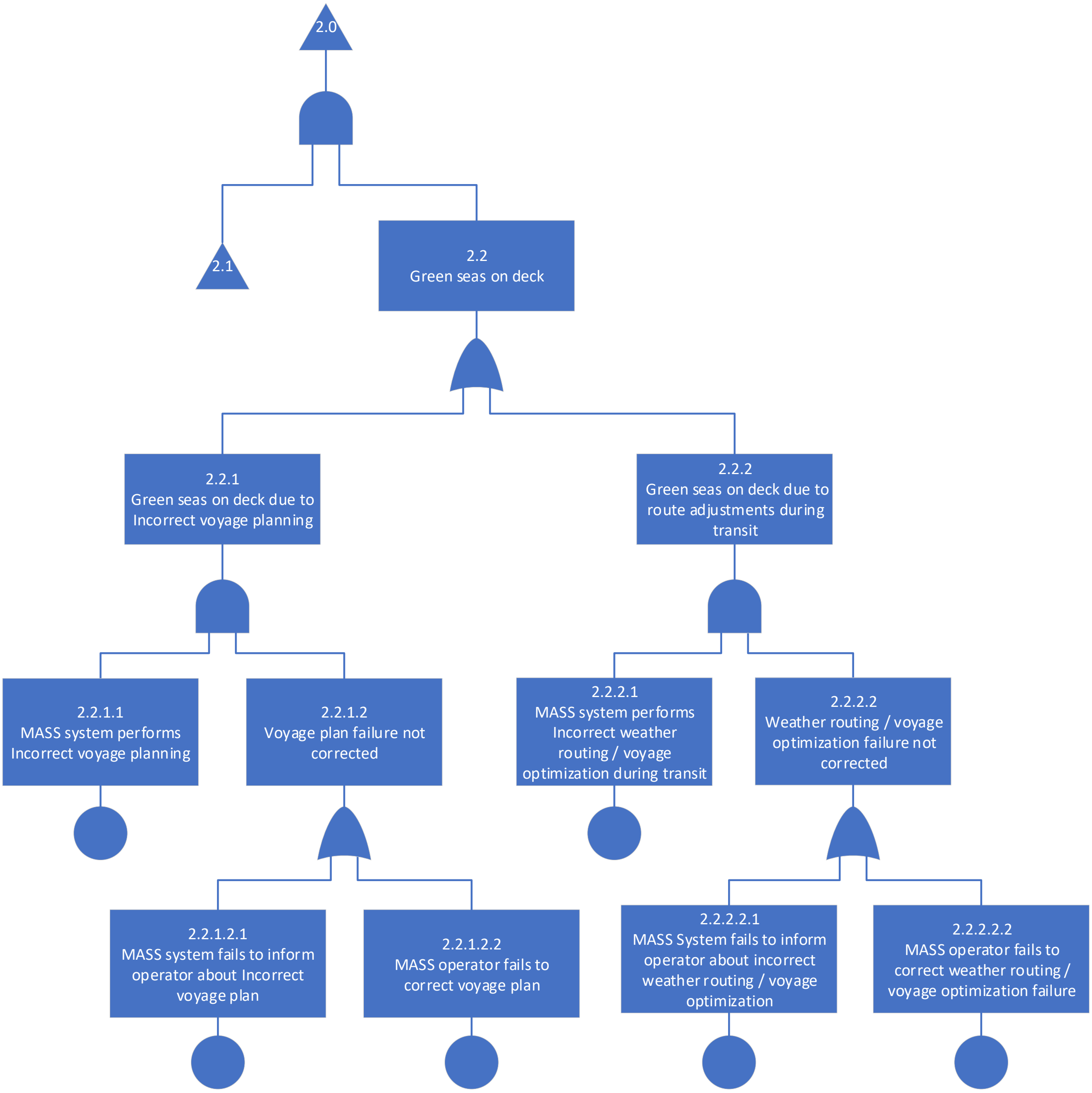

2.0
2.1
2.2
Green seas on deck
2.2.1
Green seas on deck due to Incorrect voyage planning
2.2.2
Green seas on deck due to route adjustments during transit
2.2.1.1
MASS system performs Incorrect voyage planning
2.2.1.2
Voyage plan failure not corrected
2.2.2.1
MASS system performs Incorrect weather routing / voyage optimization during transit
2.2.2.2
Weather routing / voyage optimization failure not corrected
2.2.1.2.1
MASS system fails to inform operator about Incorrect voyage plan
2.2.1.2.2
MASS operator fails to correct voyage plan
2.2.2.2.1
MASS System fails to inform operator about incorrect weather routing / voyage optimization
2.2.2.2.2
MASS operator fails to correct weather routing / voyage optimization failure

Figure 33 – Fault tree branches for intermediate event ID 2.2

6.4 Emerging risks associated with loss of stability scenarios

The sections below elaborate on some of the key risks mentioned in the *TOP* event description of loss of stability above. Due to how this FTA was limited to address more *initiating* causes rather than failure to respond to an event, reference is made to chapter 6.2 for discussions about the latter.

Induced by the high level of automation, the FTA suggests that the initiating failures are primarily caused by the MASS system failing in performing a function. There can be several causes for why the functions fail, but a common feature seems to be the lack of sensors and capability of performing crosschecks. For instance, the MASS system is more likely to fail when performing functions associated with pre-departure stability due to wrong data input, rather than a calculation error. Consequently, the use of different sensor types which can perform crosschecks seems like a common solution for most failures.

While increasing the number of sensors may help operability and (in some ways) safety, it also increases the likelihood of more frequent sensor failures. This can potentially result in additional alarms, which also creates a higher operator workload. The philosophies for all three ship concepts are that the bridge is only manned during port manoeuvring and transit (only for passenger vessel), and not while at port or being docked. This assumes that the MASS is capable of automated cargo handling, and that any assistance or supervision by the MASS operators is done on the ship deck or on dockside. However, in order to handle alarms, the MASS operator must relocate to the bridge, after being notified via the portable alarm device. The MASS operator(s) can be tempted to acknowledge or ignore alarms communicated via the portable alarm device and postpone investigating the alarm cause until after having completed (e.g.) a cargo handling operation. The probability of such a risk could arguably be the highest during a pre-departure phase, were the amount of workload potentially peaks and the delay of departure can have significant economic consequences.

Motives for ignoring or not investigating alarms could be that relocating from deck to the bridge is time consuming and exhausting, especially in the case of frequent demands. Several other factors could also be involved, such as the availability of other crew members to support, how the alarm is communicated via the portable device, and what the possibilities are for responding to the alarm remotely. The same motives would also be present during transit. As such, many of the same risks discussed in chapters 6.1.2 and 6.1.3 associated with the MASS operator *intentionally* or *unintentionally* not mustering at the bridge as part of collision avoidance, also applies for this scenario. Differences can be that the perceived criticality of isolated and seemingly unrelated alarms appears lower than those related to collision with other vessels or objects. Another difference is that there may be more time available to handle notifications and alarms about events identified in the loss of buoyancy scenario.

To reduce information-overflow the alarms about sensor failures or deviations communicated to the operator can be limited based on criticality. However, the risk of implementing such solutions is that the operator could have difficulties when trying to pinpoint the exact cause of the event and acknowledges the alarm without investigating. Consequently, several *latent failures* could remain in the system and cause hazardous events at a later stage when the conditions have changed (e.g. during voyage). For example, a tank sensor ignored during the pre-departure phase could be the initiating cause for incorrect transfer of internal liquid loads during transit. Such latent failures can be difficult for the MASS operator to identify and troubleshoot in case of escalation of events and emergencies.

In summary, an examination of the loss of stability/ buoyancy fault tree model reveals that most of the initiating events follow a common pattern:

- A combination of two or several events must occur on several event levels in the fault tree; this indicates system redundancy and a low *TOP* event probability.
- Redundancy is a result of how both the MASS system and MASS operator must fail on several functions for the *TOP* event to occur. The MASS system can also be made reliable by use of several and different types of sensors, having redundant control systems etc. If the MASS system fails, the MASS operator acts as an additional safeguard by being informed and correcting the problem manually.
- Most of the events which causes the *TOP* event to occur are isolated from each other both in space and time (i.e. there is no or little dependency). For example, an unsecured cargo hatch has little to do with incorrect pre-departure stability calculations.

The abovementioned bullet-points indicate that the MASS can be a highly reliable system, by use of automation and redundant functions. The same characteristics can however potentially introduce some new, emerging risks associated with the A3-B1 level:

- In case reliability is weakened, an increased number of sensors and instrumented functions can have the potential to produce a large amount of notifications and alarms for the operator to deal with. This can cause alarm fatigue.
- Isolated each of the alarms may not be perceived as critical and could potentially be ignored or acknowledged without any corrective actions. This tendency can be increased by factors such as low manning/ high workload or the cause of the alarm being located in inaccessible places (such as inside a tank) making it difficult or troublesome for the MASS operators to fix. Another factor which could influence the MASS operators to ignore alarms is the commercial pressures to leave port or maintain voyage speed.
- Not fully checking the alarm cause, the MASS operator may not have complete understanding of the MASS condition.
- Because the alarms can be produced (and ignored) both when being docked or during transit, and are produced from different systems, it may be difficult for the MASS operator interpret how a combination of failures can be critical.

As a result, the MASS could potentially operate with several *latent failures* in the system, such as an unsecured cargo or a damaged cargo hatch. Although seemingly uncritical when isolated, an accident can occur when the MASS is exposed to other hazards such as green seas on deck.

7 CHALLENGES WITH CURRENT REGULATIONS (TASK 1. D)

The current IMO regulatory framework presents compliance challenges concerning the A3 - B1 level of autonomy. This part of the study aims to identify where the A3-B1 vessel is not compliant with the main SOLAS, STCW, MARPOL, and COLREG provisions. We are assuming that the qualified crew onboard meets all competency requirements in order to perform all tasks required onboard to ensure safe operation, within areas such as navigation, engine control, firefighting, and SAR. The presence of qualified seafarers onboard will, therefore, delineate the compliance challenges as they can fulfil functions that specifically require a physical presence.

A review of relevant regulations and published articles on MASS was first performed as a desktop study, followed by input from discussions with technical DNV GL experts. Reviewed publications included:

- AAWA whitepaper /12/.
- Danish Maritime Authority (2017). Analysis of regulatory barriers to the use of autonomous ships /13/.
- Henrik Ringbom (2019). Regulating Autonomous Ships—Concepts, Challenges and Precedents, Ocean Development & International Law /14/.

7.1 COLREG

The assumption has been made that an A3-B1 ship is equipped with a COLREG compliant navigation system. The main challenges for an A3-B1 ship, relate to the replacement of continuous monitoring by automation. These provisions will not be possible to comply with by any of the ship descriptions within the A3-B1 autonomy level. New provisions will be required to allow the operation of autonomous ships. In the context of bridge crew compliance, lookout requirements are defined in COLREG Rule 5:

"Every vessel shall at all times maintain a proper lookout by sight and hearing as well as by all available means appropriate in the prevailing circumstances and conditions so as to make a full appraisal of the situation and of the risk of collision."

The main issue related to situational awareness, and the extent of a lookout, is if electronic instruments and equipment can replace the human function of observation. This assumption will have to be a prerequisite for all degrees of automation. COLREG Rule 5 refers to the human qualities "sight and hearing." This wording creates the assumption that human physical accessibility is considered indispensable in the monitoring role. The Rule applies explicitly at "all times," and COLREG offers no exemptions or possibilities for equivalent standards and applies to all ships. As technical developments and ship design has developed over the years, a more flexible interpretation of the Rule has evolved. E.g., when the increased use of enclosed bridges posed compliance issues concerning the hearing requirements, a formal amendment of SOLAS came as a response[1]. The regulation proposed an alternative solution. It justified a broader interpretation of the Rule adapted to current developments, which accepts that the prospect that human functions may be replaced by technology, at least as far as situational awareness is concerned /14/.The IMO has not adopted a strictly literal interpretation of the Rule 5 requirements in the past. It is, therefore, possible that electronic instruments and equipment can replace the human function of observation, assuming that the

[1] SOLAS V/19

technologies used are at least as effective and safe as diligent humans performing the lookout functions.

As mentioned above, a fundamental principle of COLREG is that ships are controlled by a human operator and that navigational decisions are based on a seamanlike assessment of the specific situation. This principle implies that the operator must be able to handle situations where the rules do not provide a safe solution. The requirement is elaborated in COLREG Rule 2:

A) Nothing in these Rules shall exonerate any vessel, […], from the consequences of any neglect to comply with these Rules or of the neglect of any precautions which may be required by the ordinary practice of seamen, […].

B) [...] due regard shall be had to all dangers of navigation and collision and to any special circumstances, […], which may make a departure from these Rules necessary to avoid immediate danger.

The incorporation of "good seamanship" into automated navigation may pose serious difficulties. As COLREG Rule 2 states, the ability to follow the rules is not sufficient. The ship must handle situations where the rules do not provide a safe solution. In short, COLREG requires "Navigator's common sense" in the:

- Principles of navigation
- Ability to predict scenarios
- Ability to evaluate risk
- Ability to plan several steps ahead

The required precedence of ordinary seamanship, therefore, poses a regulatory compliance issue to the A3-B1 level of autonomy when the operator is not attending the bridge and is only partially involved in navigational decisions.

7.2 STCW

The Standards of Training, Certification and Watchkeeping (STCW) Convention and Code provides a standard for all seafarers on conventional vessels. Nonetheless, some ship types deviate significantly from the standard and therefore require additional competence. The necessary training to fulfil this gap is today provided by the ship management company as required by the ISM Code. Considering this gap of competence, it could be a challenge for the ship management companies to fill the gap as the competence in need is not yet supplied. New guidelines and competency requirements should be defined in the STCW, notably guidelines concerning the new technology and Human Machine Interface (HMI). However, this challenge does not present any direct issues with the current STCW Convention and Code and does not prevent MASS operations.

The primary compliance issue to the A3-B1 ship, however, is the replacement of continuous monitoring by automation. Bridge crew compliance is not only required as part of COLREG but also further elaborated in the STCW Convention and Code. The main regulatory challenge is compliance with the watchkeeping requirements in the STCW Convention VIII/2.2:

"Administrations shall require the master of every ship to ensure that watchkeeping arrangements are adequate for maintaining a safe watch or watches, taking into account the prevailing circumstances and conditions and that, under the master's general direction:

.1 officers in charge of the navigational watch are responsible for navigating the ship safely during their periods of duty when they shall be physically present on the navigating bridge or in a directly associated location such as the chartroom or bridge control room at all times;

.2 […]

.3 officers in charge of an engineering watch, as defined in the STCW Code, under the direction of the chief engineer officer, shall be immediately available and on call to attend the machinery spaces and, when required, shall be physically present in the machinery space during their periods of responsibility;

The Code further elaborates, in Part A - VIII/2 para.24, that the officer in charge of the navigational watch shall keep the watch on the bridge and in no circumstances, leave the bridge until properly relieved. Furthermore, the STCW regulations state that; at no time shall the bridge be left unattended[2]. These regulations propose compliance issues related to the bridge being periodically unmanned.

7.3 SOLAS

The Safety of Life at Sea Convention is built on the assumption of human presence; i.e. the principle of having seafarers on board was central in the creation of the rules. Few compliance-related issues emerged when interpreting and comparing today's rules against the A3-B1 ship descriptions. The qualified seafarers on board the A3-B1 vessel are assumed to be available to perform various human intervention actions that are currently build into the regulations, such as manual operation, control and monitoring, casualty situations, and responding to alarms. Under this assumption, almost none of the current SOLAS regulations prevent A3-B1 MASS operations. However, the regulations do not address potential emerging risks that have been defined in the study, which should be further addressed.

The main issues regarding SOLAS compliance, as mentioned, were found in relation to safe manning; i.e. the requirement of a continuous watch on control stations, and bridge attendance. It is important to regard the SOLAS regulations in coherence with the assumption that there would be a minimum manning onboard. There could be numerous risks that are not accounted for in the regulations when the human role on board is altered. The current SOLAS convention is not adequate to give a good indication of what regulations we need to alter to accommodate the context and use of autonomous ships.

7.3.1 SOLAS Chapter II-1

Regulations concerning periodically unattended machinery spaces is accounted for in Part E and does not propose any compliance issues regarding the A3-B1 MASS category.

7.3.2 SOLAS Chapter II-2

According to SOLAS Regulations Chapter II-2/7.9.3, "Passenger ships carrying more than 36 passengers shall have the fire detection alarms for the systems required by paragraph 5.2 centralized in a continuously manned central control station". For the ship to be able to have a

[2] STCW Part A – VIII/2 Part 4-1 Regulation 18

periodically unattended machinery space, SOLAS requires a continuously manned control station in order to monitor and respond to alarms. This requirement is compliable as the alarms could be sent directly to the navigation bridge. The issue, however, emerges when the bridge is periodically unmanned. As discussed above, this regard will prevent MASS operation as it is in direct conflict with the current regulations.

Concerning fire safety, human presence is essential to perform regular checks and necessary monitoring. The necessary presence of crew is not always explicitly stated but often hidden in the required functionality, e.g., in the operation of manual equipment such as fire pumps and fire hoses, handling visual and audible alarms, and manual confirmation of closed doors. Regarding fire safety, it is also essential to consider the emerging risks that are caused by new automated equipment such as additional power supply and ventilation on devices that present new potential sources of fire.

7.3.3 SOLAS Chapter III

SOLAS Chapter III concerning lifesaving appliances does not present any specific compliance issues to our ship descriptions. The required placement of manual fire extinguishing equipment and survival suits could be considered amended and location adapted, as today's placement of such equipment is based on a minimum manning of people on the bridge and in the machinery room/ or machinery control station. The provisions on emergency training, evacuation, and drills present no regulatory challenges as there is a competent crew onboard with the required training to handle these situations. In the passenger ship description, the requirements of safe manning are considered by the equipment of additional personnel with compliance responsibilities. SOLAS Chapter III does not prevent MASS operation or regulatory compliance issues to the A3-B1 category.

7.3.4 SOLAS Chapter V

Safe manning is required by SOLAS Chapter V, Regulation 14, to make sure all ships are sufficiently and efficiently manned. Furthermore, it is up to the flag state to approve if the number of personnel and required qualifications is sufficient for the safe operation of the vessel. This process is aided by the IMO Resolution A.1047(27) /15/, which provides guidelines for the application of principles of safe manning. However, these regulations and guidelines are designed for conventional vessels and do not consider A3-B1. Consequently, the number of personnel, roles, and responsibilities of an A3-B1 vessel could differ from the safe manning of a similar conventional vessel. The A3-B1 vessel will be compliant to SOLAS Chapter V, as we assume that the qualified crew on board are competent and able to perform SAR operations and other tasks needed.

7.3.5 MARPOL

MARPOL requirements are unlikely to present compliance challenges. Responses to pollution emergencies outlined in The Shipboard Oil Pollution Emergency Plan (SOPEP) will have to be adapted to the response capabilities of the A3-B1 ship, depending on the qualifications of the crew.

7.4 Main challenges

The main identified challenges that will pose compliance issues to the A3-B1 ship, as mentioned above, are found in the replacement of continuous monitoring by automation. Both COLREG, STCW and SOLAS cover regulations that require a constant physical presence on the navigation bridge. The following four regulations are, therefore, identified as to prevent A3-B1 operation.

- COLREG 72, Pt. A, Rule 2, Responsibility
- COLREG 72, Pt B, Sec. I, Rule 5, Look-out
- STCW Convention VIII/2 Watchkeeping arrangements and principles to be observed
- SOLAS Ch. V/14 Ship’s manning

8 RISK CONTROL OPTIONS (TASK 1. E)

The study's final activity was to develop risk control measures (RCM) which could be implemented to prevent individual or combinations of the fault trees' basic events from being triggered, and consequently causing the *TOP* event to occur.

The sub-chapters below summarize (in prose) what are considered the most important RCOs and RCMs. Each summary is supplemented with a table listing all the RCMs considered to be categorized under the RCOs each sub-chapter intends to address, namely:

- RCO #1 – Ensure robust communication between MASS and other vessels
- RCO #2 – Ensure that MASS operator(s) are capable of mustering at the bridge when required
- RCO #3 – Ensure that task unfamiliarity and complexity does not impair human performance
- RCO #4 – Ensure sufficient levels of system redundancy and reliability in MASS design and operations

Furthermore, please note the following:

- The RCO numbering (i.e. 1-4) does not reflect an order of prioritization.
- Some of the RCMs correlates with more than one RCO and could in principle be listed under other RCOs as well. This is inevitable when dealing with systems engineering.
- Appendix D includes the complete list of RCMs combined with the FTA in a table format. This table shows the link between the various RCMs and the fault tree events for which they were identified.
- It is recommended to review the table in Appendix D for a more in-depth understanding of the justification behind each RCM.

8.1 RCO #1 – Ensure robust communication between MASS and other vessels

The FTA identified several challenges associated with using automated communication as a safeguard to prevent collision between vessels. Although not specified in great detail, the ship descriptions assumed that the MASS were capable of performing basic communication. Communication between humans is complex by nature – a large degree of variance can be expected due to differences in language and culture, as well as from communication needs. In reality, RCO will have to aim at making communication more robust and predictable, e.g. by introducing RCMs aiming at standardization. One solution could be to make the MASS system capable of communicating by use of standard marine communication phrases (SMCP). To provide an additional layer of safety, a second and even simpler form of communication could be used to prevent or mitigate emergencies. Solutions will to a large degree depend on the technology available, not only for implementation and use on MASS, but also for other types of vessels.

On board a A3-B1 MASS, communication should be made robust by RCMs like:

- Providing solutions which makes it easy for the MASS operator;
  - to listen in on on-going and previous communication, and

  - view basic navigational information from other locations than the bridge.
- Notifying MASS operator about;
  - communication being initiated between MASS and other vessels,
  - unsuccessful communication or failures in communication system on portable alarm device (if not already at bridge).
- Defining MRCs for what is considered failed communication.

A complete list of RCMs associated with RCO #1 is provided in Table 13.

Table 13 – RCMs associated with RCO #1 targeting robust communication

ID no.	Risk control measures
RCM-01	b) The MASS system should be able to interpret sound and light signals from other vessels according to COLREG rule 34.
RCM-04	a) MASS type/ status/ capabilities to be broadcasted to other vessels e.g. by AIS or navigation lights.
	b) MASS should be able to indicate its manoeuvring intensions with sound and light signals as specified in COLREG rule 34.
RCM-08	a) MASS operator to be notified about unsuccessful communication on portable alarm device (if not already at bridge).
RCM-09	a) MASS operator to be immediately alerted in case of failure on communication system.
RCM-10	a) MASS system to communicate with other vessels in due time by distributing and transmitting VHF messages according to the standard Marine Communication Phrases (SMCP).
	b) The MASS systems should be able to relay incoming radio traffic (VHF) to a MASS operator (if part of operation) and allow for human-human communication with other vessels.
	c) MASS operators to be notified when MASS system initiates communication with other vessels.
	d) Provide means so that it is easy for MASS operator to listen in on communication with other vessels from additional locations other than the bridge.
RCM-13	b) Communication equipment combined with displays showing navigational information located in a location additional to the bridge.
RCM-14	a) Combine use of training and actual field experience with communication equipment.

8.2 RCO #2 – Ensure that MASS operator(s) are capable of mustering at the bridge when required

One of the main risks for the A3-B1 level is that MASS operator(s) will not be able to muster to the bridge or arrive too late to perform the required tasks in a reliable manner. The combination of low manning and a high level of autonomy involves having periods of time where the bridge is unmanned. In such cases the MASS system will have to notify the MASS operator about having to muster to the bridge in due time.

For all the three ship concepts described in this report the controls and information displays used to monitor and control the MASS are located on the bridge. So, in case the MASS operator fails to muster in time, he or she will not be able to intervene and override the MASS system in case it operates outside operational parameters or enters emergencies. As described in 6.2.1, if the MASS operator arrives late, he or she may not be able to gain the situational awareness necessary to make the correct decisions and act accordingly. Several of the identified RCMs are therefore aimed at ensuring that the MASS operator is available to be present at the bridge in due time before expected to intervene.

One RCM is to provide the MASS operator with a portable alarm device with high reliability and availability. This includes both an interactive information display for alarm text and other critical information, as well as a speaker for audible alarms or communication purposes. Such a device was already described as part of the design prior to the HAZID and FTA. However, the risk analysis further emphasized the importance of this device’s functionality.

Specifically, the availability and reliability of such a device should be ensured through:

- Routines and procedures implemented for how to use the device, incl. when to carry it.
- Means for securing the device to the work wear (e.g. boiler suit).
- For all expected working conditions;
    - Sufficient visual and audio signal,
    - High quality, user-friendliness and sufficient IP rating,
    - Strong signals in all areas visited by operators,
- Notifying off-duty operator in case on-duty operator’s alarm is not acknowledged.
- Automatically adjust the time the notifications and alarms are issued depending on how far away from the bridge (or other control station) the operator is located.
- Indicate criticality of alarm.

Another RCM is to ensure that the MASS operator is made available by use of clear routines and procedures for when to muster or be present at the bridge for supervising the operation (regardless of any alarm). This is relevant for operations where the surroundings can change quickly and there is limited or no time to re-locate to the bridge. Examples can be sailing through areas with high traffic density or critical loading operations. By supervising the operation, the MASS operator’s situational awareness will be obtained continuously and in parallel with the MASS system. Procedures should be established for:

- When to muster, be in proximity of, or present at the bridge.

- Contingencies which ensure presence on bridge in case 1 out of 2 MASS operators (within a department) are indisposed.

The A3-B1 level includes the presence of qualified operators onboard the MASS. It is assumed that the operators are certified according to STCW and provided with additional MASS specific training to compensate for competence needs currently not covered by current regulations. This has not been specified but could be related to understanding how the automation works. However, the job positions are still split into Bridge and Deck categories, indicating that each role has unique competencies with little overlap. With having only two operators on-duty, and only two with similar competencies, the operations are vulnerable for situations where one of the operators are made indisposed, for example due to injury or sickness. An RCM could therefore be to provide cross-training for certain competencies, so that all MASS operators have the minimum amount of skills and knowledge necessary to maintain safe operations.

A complete list of RCMs associated with RCO #2 is provided in Table 14.

Table 14 – RCMs associated with RCO #2 targeting operator being available on bridge

ID no.	Risk control measures
RCM-11	a) Clear routines and procedures for when to muster/ be in proximity of/ or present on bridge. Criteria for presence can be traffic density, failures or limitations in the automation system, weather conditions and visibility, water depth, width of passage, and availability of infrastructure.
	b) Portable alarm system to indicate failure/ event criticality.
	c) Limit number of alarms/ notifications given to operator to avoid "alarm fatigue".
RCM-12	a) Ensure high reliability and availability of portable alarm device, e.g. by; - routine to always carry device - securely attachment of device - sufficient light and audio signal - good quality and sufficient IP rating - good signals in areas visited by operators - off-duty operator to be notified if alarm is not acknowledged
	b) Clear routines for how to act in case 1 out of 2 MASS bridge operators are indisposed.
RCM-13	a) Time until warning and/ or alarms should be defined by how far away from the bridge (or other control station) the operator is located.

8.3 RCO #3 – Ensure that task unfamiliarity and complexity does not impair human performance

Due to a high level of automation and infrequent human involvement inherent in the A3-B1 level there is a risk that several of the tasks presented to the MASS operator will be unfamiliar and, in some cases, complex. Another hazard is degradation of the MASS operators' skill set due to limited real-life practice.

RCMs for managing task unfamiliarity and complexity can differ depending on the context it occurs in. For tasks being performed in a relatively safe environment and with enough time available, procedures combined with training intended to increase system knowledge (e.g. coursework) can enable reliable operator performance. One example is to trouble-shoot an error in the otherwise automated voyage planning or pre-departure stability calculation.

For tasks being performed in more stressful circumstances and with limited time available, training intended to enhance operator skillset would be more beneficial. This refers to physical and cognitive skills required to e.g. manoeuvre a vessel safely in situations where there is no time for planning or use of procedures. For particularly rare and highly critical scenarios use of simulators would be useful. The MASS operator could also train during normal operations by performing manual actions with little or no assistance from automation. This will help prevent skill degradation.

The risk analysis also revealed hazardous aspects of task complexity commonly referred to as "mode confusion" and "(dis-)trust" in automation. As discussed in chapter 6.2.2 such factors can cause the operator to either incorrectly intervene with successful automated actions, or to incorrectly avoid intervening in case of unsuccessful automated actions. In either case, the same factors which caused the erroneous intervention, or lack thereof, is also likely to cause the MASS operator to fail in performing his or her actions. Error modes are likely to be related to one or several elements in situational awareness, such as perception, comprehension and projection of current events and future states. Recommended RCMs for preventing such errors modes include:

- Providing the MASS operators with sufficient training in MASS system automation, incl.:
  - The ability to perform system diagnostics in time critical situations.
  - Build knowledge MASS system reliability and failure prevention/ mitigation.
- HMI and automation designed according to "closed loop dynamics", i.e. include operator in the loop by interaction with automation and information flows creating situational awareness.
- HMI, other control panels and communication equipment should in general be designed with a high degree of usability to allow easy information acquisition and control possibilities.
- Provide the MASS operator with an opportunity to demand that the MASS system brings the vessel into an MRC in case he or she is uncertain of/ distrusts the outcome from automated actions.

A complete list of RCMs associated with RCO #3 is provided in Table 15.

Table 15 – RCMs associated with RCO #3 targeting task unfamiliarity and complexity

ID no.	Risk control measures
RCM-06	d) Apply principles of *error tolerant design* for software interfaces (see standards such as ISO 11064, ISO 9241-110 and ISO 9241-210).
RCM-14	b) Ensure high degree of *usability* on communication equipment and associated human-machine interfaces (see standards such as ISO 11064, ISO 9241-110 and ISO 9241-210).
RCM-19	a) Provide MASS operator with sufficient training in MASS system automation, incl.; - system diagnostics in time critical situations - share experiences about more and less reliable functions, and relevant mitigations - regular simulator training similar to BRM, courses.
	b) The MASS system should be designed according to principles of *closed loop dynamics* (include operator in the loop by interaction with automation and information flows creating situational awareness).
RCM-21	c) For each identified MRC, consider whether it is feasible for the MASS operator to aid the MASS system and/or function as a back-up in a reliable manner.
RCM-25	a) Use of Bridge Resource Management (BRM) simulator training combined with routines to perform navigational and manoeuvring tasks manually at a regular basis during normal operations.
	b) Ensure high degree of usability on navigational control panels and associated human-machine interfaces (see standards such as ISO 11064, ISO 9241-110 and ISO 9241-210).
RCM-28	a) MASS operator to perform automated functions manually at regular intervals to ensure task and system familiarity. Support with checklists and procedures.
	b) Ensure that routines/ shift schedules are optimized to reduce workload so that all necessary system checks can be performed in a reliable manner.
	c) Ensure that alarms are categorized and prioritized to avoid alarm flood, and that alarm presentation (text, sequence and availability) is based on the criticality of individual and combined alarms.
	d) Ensure high degree of *usability* on navigational control panels and associated human-machine interfaces (see standards such as ISO 11064, ISO 9241-110 and ISO 9241-210).
RCM-29	b) The MASS system should inform the operator about the intensions/ expected result of an operation before the operation is commenced.
	c) The MASS system should provide the operator with enough information to enable the operator to validate the correctness of the operation in question.
RCM-35	d) The MASS operator should be obligated to review and approve the voyage plan prior to departure.

ID no.	Risk control measures
	e) The MASS system should provide the MASS operator with input on what considerations it has based its choice on.
RCM-39	a) All personnel to be aware of the importance of securing all equipment and loose objects when working on MASS (incl. third party personnel providing service during port stay).
	d) MASS operator to be alerted if potential loose objects on deck are left unsecured.

8.4 RCO #4 – Ensure sufficient levels of system redundancy and reliability in MASS design and operations

Examination of the fault tree models revealed varying degrees of redundancy. This can be determined by identifying the number of AND- or OR-gates in a branch of event sequences. Several executive AND-gates can be an indication of redundancy and reliability, while OR-gates may represent the opposite.

The most apparent source of reliability is the use of MRCs, which is an RCO already assumed to be implemented in the MASS ship descriptions. However, the FTA allowed for some more nuanced considerations. For the collision *TOP*-event one of the risks is that the MASS system performs navigation errors which causes the vessel to enter an (abnormal) state where the risk of collision is increased due to limited room for manoeuvrability. Due to the criticality and operational importance of the navigation function it is essential that it is made with a reliable design. RCMs to avoid navigational errors include making the MASS system capable of analysing surrounding traffic and act according to COLREG. Making a control system COLREG compliant create high demands for reliability and it may not be capable of predicting all possible future events. In case the error is caused by a failure in the control system responsible for navigation there is a risk that the system is not capable of recognizing its own wrongdoing. For MASS designed with a high level of automations, such as A3-B1, an RCM could therefore be to have a separate control system being responsible for taking control in critical abnormal situations and ensure that the MASS either regains normal operational state or enters an MRC.

Highly critical functions such as navigation should also be protected from software failures. As such, only allow qualified personnel to work on software, e.g. by strict access control. Care should also be taken in case of performing updates or upgrade of software when sailing.

For A3-B1 redundancy is to a large extent provided by having the MASS operator intervene in case automation fails. Due to the inherent “human-in-the-loop” challenges associated with the A3-B1 level, an RCM is therefore to assess how feasible it is for the MASS operator to act as a reliable safeguard in case of failure in automated functions, and in different scenarios. At the design stage, this can be done by using well-established human factors and human reliability analysis methods, such as those referred to in the IMO FSA guideline /8/. During operations the role and responsibilities of the MASS operator as a back-up to failed automation must be made clear by use of procedures supported by training.

Additional RCMs to ensure the MASS operators’ availability and reliability are described in chapters 8.2 and 8.3 above.

Examination of the fault tree for the loss of stability *TOP*-event also revealed the need for high reliability in several different functions. As explained in 6.4, the need for reliability could emerge from a combination of operability and safety. A large number of unreliable functions can cause the MASS operator to experience a high workload due to having to respond to alarms with seemingly low criticality. This, in turn, can make the MASS operator acknowledge alarms and override systems without resolving the issue. The result can be latent failures which contribute to hazardous events at a later stage, for example during the voyage. As such, an RCM would be to introduce a capability which allows the MASS system to perform self-diagnostics and corrections by use of redundant sensors and instrumentation, including methods for voting and weighting input etc. This could potentially represent large costs, which would have to be considered against costs associated downtime and/ or manning levels required to either be responsible for performing the tasks up front or correct any problems not resolved by use of automation.

As an end note; one thing to keep in mind is that the fault tree models developed in this study illustrate sequences and combinations of accident events on a relatively high (system) level. At this level of analysis redundancy is likely to be less evident. The event probabilities however, if quantified, would likely have been low. If the modelling had been done on a more detailed (component) level it would probably have been possible to illustrate more redundancy, especially for the technical failure modes.

A complete list of RCMs associated with RCO #4 is provided in Table 16.

Table 16 – RCMs associated with RCO #4 targeting system redundancy and reliability

RCO ID	RCM
RCM-01	a) The automated navigation system should be verified to fully comply with the navigational parts of COLREG, including Rule 2 and rule 17 which describe actions needed in order to avoid collision when the other vessel is not behaving as expected.
RCM-02	a) Consider acts of violation (e.g. to COLREG) by other vessels when defining MRCs.
RCM-03	a) High level of security for control system responsible for initiating MRC, incl. being independent from control system responsible for normal operations.
	b) MASS to be ISPS compliant and recognize emerging terror scenarios.
RCM-04	c) The automated navigation system should be verified to fully comply with the navigation parts of COLREG, including rule 8 which among other things states that all actions to avoid collisions shall be performed in ample time, and be readily apparent for other vessels.
RCM-05	a) The automated navigation (control) system should be verified towards established rules and standards by an independent party.
	b) Implement proper assurance framework of control systems, providing assurance of both products and process.
	c) The automated navigation system should automatically be monitored for failures and sub-par performance.
	d) Sufficient test of all safety critical components (e.g. simulator test of COLREG system, test of object detection systems).
	e) The MASS should at all times have the possibility to enter at least one pre-defined minimum risk condition (MRC) in the case of significant equipment failures.
RCM-06	a) There should be a strict separation between parameters that are expected to be changed during operation, and parameters that are NOT expected to be changed during normal operation.

RCO ID	RCM
	b) Parameters that are NOT expected to be changed during operation should be protected by special access-control measures and should NOT be changeable while the system is in operation.
	c) Software updates and changing of the basic system configuration should NOT be possible while the system is in operation.
RCM-07	a) After changes are performed on software or the system configuration, a thorough verification process should be successfully executed before the system is put back into operation.
RCM-12	c) The MASS should at all times have the possibility to enter at least one pre-defined minimum risk condition (MRC) in the case of operator inaction within time criteria pre-defined for critical events and failures.
RCM-15	a) Define (as part of design) MRCs for when the MASS system recognizes it is not able to re-enter a normal operational state (i.e. comply with COLREG).
RCM-21	a) There should at all times be more than one MRC available for the MASS to enter.
	b) Ensure that system responsible for taking the MASS into an MRC is independent of the MASS navigational system.
	d) Test and verify that the MASS system is able to detect all scenarios where MRC should be initiated.
RCM-26	a) The MASS (automation) system should be able to crosscheck weights on loading manifest.
	b) MASS system should be able to crosscheck loading condition, e.g. by checking against physical observations of draft marks.
	c) Sub-systems should report status to a master-system which keeps track of the aggregated state of the vessel (including all relevant sub-systems) and initiates transition to a minimum risk condition (MRC) when needed.
RCM-29	a) The MASS system should include self-check and diagnostics functions able to detect failures in e.g. sensors.
RCM-32	a) Ensure that the MASS always has a cargo securing system which is compatible with the actual cargo being loaded.
RCM-35	a) The MASS system should diagnose and compare forecasted weather from different MET data sources.
	b) The MASS system should retrieve and consider all applicable route and reporting information (ships routing).
	c) The MASS system should be able to retrieve and evaluate all info for the route in ENC, such as IHO and IALA info.

RCO ID	RCM
	f) The MASS system to be able to detect local NAV conditions when planning the voyage.
	g) The MASS system should be able to detect deviations between actual and forecasted weather conditions.
	h) The MASS system's parameters for heavy weather damage should always be prioritized over voyage optimization.
RCM-39	b) MASS system to be able to monitor, detect and inspect potential loose objects.
	c) MASS system to be able to secure or remove loose objects.

9 CONCLUDING REMARKS

The following sub-chapters suggests some concluding remarks regarding the practical and theoretical implications made evident from the findings in this study.

9.1 Ironies of automation

A goal with automation is often to reduce or eliminate risks associated with human error by removing the human from the "loop". The challenge, however, is to make the systems reliable enough for this to actually happen. Instead what often happens is that the human is left with the unappreciative task of resolving problems not solved by automation. Identifying and taking account for all such problems is also often neglected or too challenging to address. This phenomenon is commonly known as the "ironies of automation", a term which was coined already in the early eighties /19/. When interpreting and applying the A3-B1 level as was done in this study, findings suggest that "ironies of automation" may still have to be dealt with. To counteract this tendency, it is important that future efforts made to increase automation adopts principles of human-centred design and applies established Human Factors Engineering techniques and standards.

9.2 Use of "Levels of Autonomy" (LoA) models

As a starting point the study attempted to apply one (definite) level of autonomy and control to the ship concepts on an overall basis, i.e. the A3-B1 level for all relevant functions, in all operational modes, and for all scenarios. One of the main findings of the study is that this approach is neither useful nor practical. For engineers and other system designers working with developing MASS-like technologies, this may seem obvious. But nevertheless, and for reasons unknown, attempts to use level of autonomy (LoA) models when explaining and defining MASS technology and operations persists both in academia and among industry actors.

The reason why LoA models is not considered suitable for practical applications stems from the phenomenon they are meant to describe. Even at a conceptual stage, such as in this study, MASS appears to be considerably more complex and multi-dimensional than the models themselves. This becomes clear when trying to compare or distinguish the A3 and A2 levels of autonomy described in Table 1. When only reading the definitions provided in the table, it may appear as if the A2 level is as autonomous as A3, with the only difference being that the qualified operator is worse off in A3. For A3 the qualified operator is not "always informed" and cannot "override the system at any stage" as in A2. Instead he/she is "[only?] informed in case of emergency or when ship systems are outside of defined parameters", which is also [the only time?] when the operator can override the ship systems. In both levels the ship systems do not require permission from the operator to execute functions, decisions or actions, indicating a similar level of autonomy. Furthermore, it is not clear why the A3 level states that the qualified operator performs "human supervision" as long as boundaries are not exceeded, when the title of the A2 level is *Supervised* (possibly due to how the operator is "always informed", instead of "in case of emergency or going outside defined parameters, as for A3).

Returning to the discussion regarding practical applications, the feasibility and need for automating vessel functions can be expected to vary depending on a combination of several factors, such as maturity of technology, a vessel's operational goals, and the surroundings in which it operates. As made evident in this study, automation design should therefore not be made at a global, ship level, as suggested by LoA models. Instead it should be made function by function on a system and task level. Here, the allocation of functions between the MASS automation system and operator(s) in various situations and operational modes can be defined more accurately and purposefully. The allocation should be based on a relative comparison of the human's or available technologies' capabilities to (jointly or individually) perform the required functions.

To do so, autonomy level-models should be adjusted to include/ or supported by additional human and system performance models, similar to those used in this study. As a minimum, such models should define;

- Responsibilities in execution of functions such as those related to detection, analysis, planning and implementation of control actions.
- Operator roles in different degrees of automation, e.g. manual control, decision-making, supervision etc.
- Operator presence and availability.

Using such models and definitions will allow a more granular and multi-dimensional assessment of automation. It also eliminates some of the problems with understanding how one level of automation differs from the other adjacent levels, which often is the case with current models.

A pre-requisite for using such models is a mapping of which functions are required in various operational modes, including abnormal states such as critical failures and MRCs. This practice is currently being promoted by industry guidelines such as the one issued by DNV GL /6/. Performing a complete mapping of all functions in a MASS concept may appear overly comprehensive and time consuming. The introduction of increased automation can however be expected to occur gradually, on a system-by-system basis. This will allow MASS functionality to be introduced using risk- and goal-based approaches, instead of having to rely on development of prescriptive rules limiting the opportunities for innovation.

10 REFERENCES

/1/ IMO (1974). The International Convention for the Safety of Life at Sea (SOLAS) 1974.

/2/ IMO (1978). International Convention on Standards of Training, Certification and Watchkeeping for Seafarers (STCW).

/3/ IMO (1973). International Convention for the Prevention of Pollution from Ships (MARPOL)

/4/ IMO (1972). Convention on the International Regulations for Preventing Collisions at Sea (COLREGs), 1972.

/5/ DNV GL (2018). Position Paper: Remote-Controlled and Autonomous Ships

/6/ DNV GL (2018). DNVGL-CG-0264 Class Guideline-Autonomous and remotely operated ships. Edition September 2018.

/7/ ISO 23860 standard on MASS terminology (in progress).

/8/ IMO (2018). Guidelines for Formal Safety Assessment (FSA) for use in the IMO rule-making process

/9/ Endsley, M.R. (1995b). "Toward a theory of situation awareness in dynamic systems". Human Factors. 37 (1): 32–64.

/10/ Figure drawn by Drawn by Dr. Peter Lankton, May 2007. Found in https://en.wikipedia.org/wiki/Situation_awareness

/11/ Lee, J. D. and See, K. A. 2004. Trust in technology: Designing for appropriate reliance. Human Factors, 46, 1, 50-80.

/12/ Rolls-Royce (2016). AAWA whitepaper Remote and autonomous ships - the next steps.

/13/ Danish Maritime Authority (2017). ANALYSIS OF REGULATORY BARRIERS TO THE USE OF AUTONOMOUS SHIPS.

/14/ Ringbom, Henrik. (2018). Regulating Autonomous Ships—Concepts, Challenges and Precedents. Ocean Development and International Law.

/15/ IMO, Assembly Resolution A.1047 (27), Principles of Safe Manning, 2011.

/16/ Joshi, A., Miller, S. P., Heimdahl, M. P. E. Mode confusion analysis of a flight guidance system using formal methods. Published in the Proceedings of the 22st Digital Avionics Systems Conference (DASC'03), Indianapolis, Indiana, Oct. 12- 16, 2003.

/17/ EMSA Tender Request: Study of the Risks and Regulatory Issues of Specific Cases of Maritime Autonomous Surface Ships (SAFEMASS). Published11.02.2019. Tender reference number: EMSA/OP/4/2019.

/18/ Bye A. et al. (2017). The Petro-HRA guideline. Rev. 1. ISBN (printed): 978-82-7017-901-5. Found in: https://ife.brage.unit.no/ife-xmlui/handle/11250/2601973

/19/ Bainbridge, L. (1983). Ironies of automation. Automatica, Volume 19, Issue 6, November 1983, Pages 775-779.

APPENDIX A - SAFEMASS PARTICIPANTS (PART 1)

Name and position	Role	Expertise
Sifis Papageorgiou Project Officer	Participant - EMSA representative	Sifis is project officer in EMSA, working in the Ship Safety Unit, dealing mainly with passenger ship safety.
Sondre Fagerli Øie Principal Consultant	Participant - expert on Human Factors	Sondre delivers technical advisory services and management consultancy to clients in various high-risk industries, such as petroleum, rail and hydro-power. Sondre has 11+ years of experience and areas of expertise include: Human Reliability Analysis (HRA), Risk and barrier management, various risk analysis techniques and Human Factors Engineering (HFE). For the last 8 years Sondre has been working mostly with offshore safety and major accident risk management.
Hans Jørgen Johnsrud Senior Consultant	Facilitator – expert on risk management	Hans Jørgen has over 10 years' experience from risk management services within the maritime industry, specialising in the use of risk-based techniques. Hans Jørgen delivers services within safety risk management, technical safety, safety barrier management, and technology qualification. He has managed several ship traffic and navigational risk assessments for government bodies and port authorities. Hans Jørgen also has experience from other projects concerning autonomous ship concepts.
Erlend Norstein Consultant	Participant – expert on ship operations and navigation	Erlend is certified as a Master Mariner and has over ten years' experience as a deck officer at sea. He holds two Master of Science degrees within the maritime segment, MSc in Management of Demanding Marine Operations from NTNU, and MSc in Technical Maritime Management from USN.
Peter Nyegaard Hoffmann Head of Section/ Project sponsor	Participant – expert on risk management	Peter is Head of Section responsible for Safety, Risk & reliability in Maritime Advisory region Norway. Peter has extensive experience with quantitative as well as qualitative risk methods ranging from HAZID workshops to building sophisticated risk models. Peter also has experience from other projects concerning autonomous ship concepts.
Are Jørgensen Senior Principal Engineer	Participant – expert on autonomous ships	Are is specialist within autonomous and remotely operated ships. He is project manager for the development of DNV GL's rules and guidance within this area. Participated in several initiatives and (research) projects regarding autonomous ships. Are has 20+ years of experience covering; Analysis of equivalent safety levels for unmanned vessels, Technology qualification for novel technologies in the context of ship automation and autonomy, Approval of manufacturers regarding system and software

Name and position	Role	Expertise
		engineering and Integrated Software Dependent Systems (ISDS), Root cause analysis++
Julie Huth Lindberg Intern @ DNV GL	Scribe	Julie is an intern at DNV GL as part of her bachelor's degree in Shipping Management at The Norwegian University of Science and Technology. The program involves risk management, maritime law, economics, and logistics.
Svein David Medhaug Project Manager	Participant – expert on autonomous ships	Svein David Medhaug is an experienced project manager employed at the Norwegian Maritime Authority (NMA). He is project manager for all work relating to digitalization and automation, and in charge of the work with autonomous and remote vessels at the NMA. Svein David has also been responsible for e-navigation since 2009. With this position, Medhaug has chaired in several correspondence groups for e-navigation in IMO. He has also led the work titled: "Guidelines for harmonized display for navigation information received via communication equipment" in IMO.
Petter Kyseth HSEQ Superintendent	Participant – expert on ship operations and navigation	Petter works as HSEQ Superintendent in Wilhelmsen Ship Management. Petter has previously been working as; Assistant Crew Manager, Captain and Chief Officer.
Jahn Viggo Rønningen Director - Head of Ship Safety at Norwegian Shipowners' Association	Participant – expert on maritime safety	Jahn Viggo is responsible for all ship safety matters for the association's members in the segments deep-sea, shortsea and offshore service. This includes technical matters, autonomous shipping and digitization. Group secretary for the panels "Environment, Safety and Operation Committee for Ships" and the "Offshore Service Vessel's forum for Health, Security, Environment and Quality". Participates regularly in IMO safety meetings with the Norwegian delegation in addition to other international-, regional and national regulatory development. Participate in boards and steering/reference groups in miscellaneous maritime safety projects. NSA representative in Norwegian Forum for Autonomous Ships (NFAS).
Marko Rahikainen Chief Adviser at Traficom	Participant – expert on autonomous ships	Marko is Chief Adviser at Liikenne- ja viestintävirasto (Traficom / Transport- och kommunikationsverket Traficom). Marko is adviser on Maritime Safety in IMO and EU meetings with related tasks for meeting arrangements, coordination and implementation of international regulations. Maritime legislation, maritime cooperation, IMO and EU member states representation as head of delegation, delegate, representative or alternate. Responsible for implementing and development of national coordination, interest group consultation and preparation for meetings.

Table 17 – Involvement of expertise in Part 1 of the SAFEMASS study

Name/ roles	Company	Position/ role	Area of expertise	Task 1. a) Ship descriptions	Task 1. b) Hazard identification	Task 1. c) Fault tree analysis	Task 1. d) Review of regulations	Task 1. e) Risk control options
Sifis Papageorgiou	European Maritime Safety Agency (EMSA)	Project officer/ Marine engineer	• MASS/ remote operations • Maritime safety • Rules and regulations		√			
Sondre Fagerli Øie	DNV GL	Principal consultant/ project manager	• MASS/ remote operations • Human element • FSA/ Risk analysis • Control centre design		√	√		√
Erlend Norstein	DNV GL	Consultant/ Master mariner	• Navigation/ operations • Risk management • Human element	√	√	√	√	√
Hans Jørgen Johnsrud	DNV GL	Senior consultant	• MASS/ remote operations • FSA/ Risk analysis	√	√			

Name/ roles	Company	Position/ role	Area of expertise	Task 1. a) Ship descriptions	Task 1. b) Hazard identification	Task 1. c) Fault tree analysis	Task 1. d) Review of regulations	Task 1. e) Risk control options
			• Maritime safety					
Peter Nyegaard Hoffmann	DNV GL	Head of section/ project sponsor	• MASS/ remote operations • FSA/ Risk analysis • Maritime safety • Rules and regulations		√		√	
Are Jørgensen	DNV GL	Senior principal engineer	• MASS/ remote operations • Control systems/ software • Maritime safety • Rules and regulations	√	√			√
Øystein Engelhardtsen	DNV GL	Senior researcher/ QA	• MASS/ remote operations • Control systems/ software	√				
Rolf Skjong	DNV GL	Chief Scientist/ QA	• MASS/ remote operations				√	

Name/ roles	Company	Position/ role	Area of expertise	Task 1. a) Ship descriptions	Task 1. b) Hazard identification	Task 1. c) Fault tree analysis	Task 1. d) Review of regulations	Task 1. e) Risk control options
			• Rules and regulations • Maritime safety • FSA/ Risk analysis					
Julie Huth Lindberg	DNV GL	Intern	• Rules and regulations	√				
Svein David Medhaug	Norwegian Maritime Authority (NMA)	Senior engineer	• MASS/ remote operations • Digitalization • Maritime safety • Rules and regulations		√			
Petter Kyseth	Wilhelmsen Ship Management	HSEQ Superintendent/ Master mariner	• Navigation/ operations • Operations • HSE management • Maritime safety		√			

Name/ roles	Company	Position/ role	Area of expertise	Task 1. a) Ship descriptions	Task 1. b) Hazard identification	Task 1. c) Fault tree analysis	Task 1. d) Review of regulations	Task 1. e) Risk control options
Marko Rahikainen	Finnish Transport and Communications Agency (Traficom)	Chief advisor/ Master mariner	• Navigation/ operations • Operations • HSE management • Maritime safety		√			
Jahn Viggo Rønningen	Norwegian Shipowners Association (NSA)	Head of ship safety/ Master mariner	• Navigation/ operations • MASS/ remote operations • HSE management • Maritime safety		√			

APPENDIX B – HAZID LOG

Table 18 – Log sheet from HAZID workshop (IDs with a light "aqua" colour are further addressed in the FTA, while IDs marked with a light "orange" colour are addressed separately)

ID	Operation description		Operational boundary and operator response				Hazard Identification					
	Ship type	Operator presence	Boundary condition	Operator role	Operator task(s)	Info required	Guideword	Hazardous event	Cause	Consequence	TOP event (worst case)	Safeguards
1. Bridge-related functions (Docked)												
1.1 Voyage planning (1.1.1 Evaluate weather, tide and current)												
1	Relevant for: - Ocean going cargo ship (Bulk carrier) - Short-sea cargo ship (Container)	1- Backup (not on bridge)	**Voyage planning system** with fully autonomous function: Storms building up in Ocean. System makes a wrong decision related to voyage planning.	None.	---	---	C1-Check omitted	**- Operator does not check voyage planning conducted by system.**	- Not obligated and no requirement to check.	- Limited time to handle the situation - When encountering storms: Minimum Risk Condition (MRC) initiated by system. MRC to be defined for this scenario.	- Heavy weather damage - Capsize - Flooding - Foundering	- Operator should be obligated to approve voyage plan before departure - The system should give input on what considerations it has based its choice on.
2	Relevant for: - Ocean going cargo ship (Bulk carrier) - Short-sea cargo ship (Container)	1- Backup (not on bridge)	**Voyage planning system** with partial autonomous function: Storms building up in Ocean. System makes a wrong decision related to voyage planning.	Decision making	Operator is required to verify voyage plan.	- Route, waypoints, ETA, expected weather conditions etc.	C2-Check incomplete	**Operator approves the plan without understanding the hazards/ implications or evaluations performed by the system.**	- Configuration of autonomous planning tool. - Degree of safety or efficiency being weighted.	- Limited time to handle the situation - When encountering storms: Minimum Risk Condition (MRC) initiated by system. MRC to be defined for this scenario.	- Heavy weather damage - Capsize - Flooding - Cargo damage	See safeguards in ID 1

ID	Operation description		Operational boundary and operator response				Hazard Identification					
	Ship type	Operator presence	Boundary condition	Operator role	Operator task(s)	Info required	Guideword	Hazardous event	Cause	Consequence	TOP event (worst case)	Safeguards
3	Relevant for: - Ocean going cargo ship (Bulk carrier) - Short-sea cargo ship (Container)	1- Backup (not on bridge)	**Voyage planning system** with partial autonomous function: Storms building up in Ocean. System makes a wrong decision related to voyage planning.	Decision making	Operator is required to verify voyage plan.	- Route, waypoints, ETA, expected weather conditions etc.	C2-Check incomplete	**- Operator does not properly check voyage planning conducted by system.**	- Overreliance in the system - Prioritize other tasks	- Limited time to handle the situation - When encountering storms: Minimum Risk Condition (MRC) initiated by system. MRC to be defined for this scenario.	- Heavy weather damage - Capsize - Flooding - Cargo damage	See safeguards in ID 1
1.2 Trim, stability & Stress while docked												
4	Relevant for: All three ship types	1- Backup (not on bridge)	**Stability calculation system:** Deviation between calculated and actual stability condition	Decision making	- Confirm actual stability and stress condition	- GM - Camera	S2-Wrong selection made	**- Operator ignore/ disregard stability and stress limitations.**	- Quality of metadata - Overreliance in the system	- Lack of control and stability - MRC to be defined	- Capsize	- MRC (stop loading). - Visibly control of draft marks - Loading computer - Integrated smart loading system - Camera surveillance - Visibly control of cargo hold and density - Cross checking multiple sensors - Ballasting
2. Deck-related functions (Docked)												
2.1 Cargo handling (2.1.4 Secure cargo)												

ID	Operation description		Operational boundary and operator response				Hazard Identification					
	Ship type	Operator presence	Boundary condition	Operator role	Operator task(s)	Info required	Guideword	Hazardous event	Cause	Consequence	TOP event (worst case)	Safeguards
5	Ocean going cargo ship (Bulk)	1- Backup (not on bridge)	**Cargo monitoring system:** Ensure locking of cargo hatches. Vessel has motion sensors and is fully autonomous.	None	No input from operator required.	N/A	C1-Check omitted	**- Cargo hatch not properly secured**	- Sensor malfunction - Not enough redundancy	MRC to be defined	- Heavy weather damage - Capsize - Flooding - Cargo damage	Sensor validation and calibration
6	Ocean going cargo ship (Bulk)	1- Backup (not on bridge)	**Cargo monitoring system:** System identifies open hatch.	Action (Take control)	Identify hatch and evaluate situation	- Notification about hatch number	A9-Operation incomplete	**- Fail to identify hatch**	Lack of info	- System does not approve voyage start	Voyage not started	- Check hatches before departure
2.4 Monitor mooring conditions												
7	Relevant for: All three ship types	1- Backup (not on bridge)	**Mooring monitoring system:** Tension limit exceeded.	Action (Take control)	- Reduce tension on moorings (Pay-out on winch or push alongside with thruster) - Apply additional mooring lines		A9-Operation incomplete	**Fail to reduce tension**	- Technical - Human error	- Vessel damage due to uncontrolled movement in harbor	- Collision with other vessels or quay side	
8	Relevant for: All three ship types	1- Backup (not on bridge)	**Mooring monitoring system:** Ramp/mooring system/magnet malfunction	Action (Take control)	- Regain position by use of thrusters.		A9-Operation incomplete	**- Unable to regain position.**	- Malfunction of thruster	- Initiate wrong action	- Collision with other vessels or quay side	
3.0 Bridge-related functions (Voyage)												
3.1 Harbour manoeuvring												

ID	Operation description		Operational boundary and operator response				Hazard Identification					
	Ship type	Operator presence	Boundary condition	Operator role	Operator task(s)	Info required	Guideword	Hazardous event	Cause	Consequence	TOP event (worst case)	Safeguards
9	Relevant for: All three ship types	---	---	---	---	---	---	**Many of the same risks as in transit, see hazards below for collision**	---	---	---	---
10	Relevant for: All three ship types	3- In control (on bridge)	Assistance by tug boat in port approach and berthing	Action (Take control)	Maneuvering Communication	---	---	**Many of the same risks as for conventional ships**	---	---	---	---
3.2 Navigation & manoeuvring during transit (3.2.1 Maintain ship position, course and speed according to track)												
11	Relevant for: All three ship types	1- Backup (not on bridge)	**Navigation system**: Inaccurate vessel position: - Loss of GNSS - Jamming and spoofing of GNSS	Decision making	Operator to select option: Stop, continue etc.	Ship position	S2-Wrong selection made	**Select wrong option**	Lack of info		Ship accident	- Additional reference system - Terrestrial navigation system (Radar, LIDAR, visual bearing)
3.2 Navigation & manoeuvring during transit (3.2.2.4 Monitor geographical and environmental conditions; depth, sea-state, tide, fog, current, ice, weather and visibility)												
12	Relevant for: All three ship types	1- Backup (not on bridge)	**System for environmental monitoring:** Sudden increase in wind and waves requires the vessel to change course, reduce speed or seek shelter	Decision making	Operator to select option: - Continue ahead - Go around		S2-Wrong selection made	**Select wrong option**	- Lack of info - Lack of situational awareness - Lack of system/ship limitations		Ship accident	System ability/capability to override "faulty human action" to be defined
3.2 Navigation & manoeuvring during transit (3.2.4 Collison and grounding avoidance)												

ID	Operation description		Operational boundary and operator response				Hazard Identification					
	Ship type	**Operator presence**	**Boundary condition**	**Operator role**	**Operator task(s)**	**Info required**	**Guideword**	**Hazardous event**	**Cause**	**Consequence**	**TOP event (worst case)**	**Safeguards**
13	Relevant for: All three ship types	1- Backup (not on bridge)	**Collision avoidance system (ship A):** Other ship B on collision course from PS and does not give way. Ship A send request to operator for presence on bridge.	Monitoring	Acknowledge alarm	- Which system needs assistance - Alarm criticality - CPA - TCPA	C1-Check omitted	**- Operator does not attend bridge**	- Crew asleep - Occupied with other tasks related to high noise environment - Does not have alarm - Alarm fatigue - Sickness - Injuries/ accidents	- System executes function independently of the operator; Successfully or enters MRC	- Collision	
14	Relevant for: All three ship types	1- Backup (not on bridge)	**Collision avoidance system (ship A):** Other ship B on collision course from PS and does not give way. Ship A send request to operator for presence on bridge.	Monitoring	Acknowledge alarm	- Which system needs assistance - Alarm criticality - CPA - TCPA	C1-Check omitted	**- Operator deliberately does not attend bridge**	- Alarm fatigue - Mis-understanding responsibility - Accidents - Overreliance in system	- System executes function independently of the operator; Successfully or enters MRC	- Collision	
15	Relevant for: All three ship types	1- Backup (not on bridge)	**Collision avoidance system (ship A):** Other ship B on collision course from PS and does not give way. Ship A send request to operator for presence on bridge.	Monitoring	Acknowledge alarm	- Which system needs assistance - Alarm criticality - CPA - TCPA	R1: Information not obtained	**- Officer/ master operator not informed**	- Technical issues	- System executes function independently of the operator; Successfully or enters MRC	- Collision	

ID	Operation description		Operational boundary and operator response				Hazard Identification					
	Ship type	Operator presence	Boundary condition	Operator role	Operator task(s)	Info required	Guideword	Hazardous event	Cause	Consequence	TOP event (worst case)	Safeguards
16	Relevant for: All three ship types	1- Backup (not on bridge)	**Collision avoidance system (ship A):** Other ship B on collision course from PS and does not give way. Ship A send request to operator for presence on bridge.	Monitoring	Acknowledge alarm	- Which system needs assistance - Alarm criticality - CPA - TCPA	C1-Check omitted	**- Does not attend bridge** **- Operator does not acknowledge the criticalness of the situation**	- Overreliance in system - False alarm and tuning of inaccurate alarm settings	- System executes function independently of the operator; Successfully or enters MRC - Failure to take action	- Collision	
17	Relevant for: All three ship types	1- Backup (not on bridge)	**Collision avoidance system (ship A):** Other ship B on collision course from PS and does not give way. Ship A send request to operator for presence on bridge.	Monitoring	Monitor system performance; - detection - analysis - planning - action	- Which system needs assistance - Alarm criticality - CPA - TCPA	C1-Check omitted	**- Incorrect prioritization**	- Need to choose or prioritize between different alarms	- System executes function independently of the operator; Successfully or enters MRC	- Collision	
18	Relevant for: All three ship types	1- Backup (not on bridge)	**Collision avoidance system (ship A):** Other ship B on collision course from PS and does not give way. Ship A send request to operator for presence on bridge.	Monitoring	Monitor system performance; - detection - analysis - planning - action	- Which system needs assistance - Alarm criticality - CPA - TCPA	I1-Information not communicated	**- Operator changes the parameter without proper information given to the new operator in a watch handover.**	- Lack of satisfactory routines in watch handover.	- System executes function independently of the operator; Successfully or enters MRC	- Collision	

ID	Operation description		Operational boundary and operator response				Hazard Identification					
	Ship type	Operator presence	Boundary condition	Operator role	Operator task(s)	Info required	Guideword	Hazardous event	Cause	Consequence	TOP event (worst case)	Safeguards
19	Relevant for: All three ship types	1- Backup (not on bridge)	**Collision avoidance system (ship A):** Other ship B on collision course from PS and does not give way. Ship A send request to operator for presence on bridge.	Action (Take control)	Communication	- Log of system action - System status update - Time available	D3- Incorrect decision based on wrong/missing information	**- Wrong action, due to lack of information**	- Poor HMI - Poor communication: Language, culture, technical issues	Escalation of situation, less time to avoid collision	- Ship collision	System ability/capability to override "faulty human action" to be defined
20	Relevant for: All three ship types	1- Backup (not on bridge)	**Collision avoidance / communication system (ship A):** Other ship B on collision course (from SB), ship A not able to follow COLREG (give way) because another ship C is on SB on same heading/course and same speed. Thus, ship A in "locked" position. Also ship C astern.	Action (Take control)	Communication with ship C on SB (to request that they change course SB, to give our ship more space)	- Log of system action - System status update - Time available	I3- Information communication incomplete	**- Insufficient communication**	- Poor communication: Language, culture, technical issues - Different ship standards regarding communication, anti-collision	Escalation of situation, less time to avoid collision	- Ship collision	

ID	Operation description		Operational boundary and operator response				Hazard Identification					
	Ship type	Operator presence	Boundary condition	Operator role	Operator task(s)	Info required	Guideword	Hazardous event	Cause	Consequence	TOP event (worst case)	Safeguards
21	Relevant for: All three ship types	1- Backup (not on bridge)	**Collision avoidance / communication system (ship A):** Other ship B on collision course (from SB), ship A not able to follow COLREG (give way) because another ship C is on SB on same heading/course and same speed. Thus, ship A in "locked" position. Also ship C astern.	Action (Take control)	Communication with ship C on SB (to request that they change course SB, to give our ship more space)	- Log of system action - System status update - Time available	A1- Operation too long/short	**- Lack of available time -> System gives operator too little time to analyze and act -> Human uses too long time to analyze and act**	- Vessel speed - Vessel send request to late (alarm boundaries) - Time to reach bridge - Unpredictable action by other vessels	Escalation of situation, less time to avoid collision	- Ship collision	
22	Relevant for: All three ship types	1- Backup (not on bridge)	**Collision avoidance / communication system (ship A):** Other ship B on collision course (from SB), ship A not able to follow COLREG (give way) because another ship C is on SB on same heading/course and same speed. Thus, ship A in "locked" position. Also ship C astern.	Action (Take control)	Manoeuvring and navigation	- Log of system action - System status update - Time available	A9- Operation incomplete	**- Lack of ability to correctly manoeuvre the ship, due to inadequate level of seamanship and unfamiliarity with vessel**	- Insufficient training	Escalation of situation, less time to avoid collision	- Ship collision	

ID	Operation description		Operational boundary and operator response				Hazard Identification					
	Ship type	Operator presence	Boundary condition	Operator role	Operator task(s)	Info required	Guideword	Hazardous event	Cause	Consequence	TOP event (worst case)	Safeguards
23	Relevant for: All three ship types	1- Backup (not on bridge)	**Collision avoidance / communication system:** Other ship A on collision course (from SB), own ship not able to follow COLREG (give way), "locked" position due to other ship B on SB and ship C astern	Action (Take control)	Manoeuvring and navigation	- Log of system action - System status update - Time available	A9-Operation incomplete	**- Unfamiliar with task**	- Task not performed frequently by crew - Insufficient training to compensate infrequent operation -> Hands on Maneuvering -> Complexity	Escalation of situation, less time to avoid collision	- Ship collision	- Frequent execution of various tasks. - Operator must perform Maneuvering, docking etc. to maintain acceptable level of skills.
24	Relevant for: All three ship types	1- Backup (not on bridge)	**Collision avoidance / communication system:** Other ship A on collision course (from SB), own ship not able to follow COLREG (give way), "locked" position due to other ship B on SB and ship C astern	Action (Take control)	Manoeuvring and navigation	- Log of system action - System status update - Time available	D4-Failure to make a decision (impasse)	**- Operator does not do anything**	- Stress - Panic - Freezing - Complexity	Escalation of situation, less time to avoid collision	- Ship collision	

ID	Operation description		Operational boundary and operator response				Hazard Identification					
	Ship type	**Operator presence**	**Boundary condition**	**Operator role**	**Operator task(s)**	**Info required**	**Guideword**	**Hazardous event**	**Cause**	**Consequence**	**TOP event (worst case)**	**Safeguards**
25	Relevant for: All three ship types	1- Backup (not on bridge)	**Collision avoidance / communication system:** Other ship A on collision course (from SB), own ship not able to follow COLREG (give way), "locked" position due to other ship B on SB and ship C astern	Action (Take control)	Manoeuvring and navigation	- Log of system action - System status update - Time available	A1-Operation too long/short	**Operator uses too long time to act**	Complexity	Escalation of situation, less time to avoid collision	- Ship collision	
26	Relevant for: All three ship types	1- Backup (not on bridge)	**Collision avoidance / communication system:** Other ship A on collision course (from SB), own ship not able to follow COLREG (give way), "locked" position due to other ship B on SB and ship C astern	Action (Take control)	Manoeuvring and navigation	- Log of system action - System status update - Time available	C6-Wrong check on wrong object	**- Task confusion** **- Wrong focus**	- Poor HMI - Inadequate information - No visual contact - To much information	Escalation of situation, less time to avoid collision	- Ship collision	
27	Relevant for: All three ship types	1- Backup (not on bridge)	**Collision avoidance / communication system:** Other ship A on collision course (from SB), own ship not able to follow COLREG (give way),	Action (Take control)	Manoeuvring and navigation	- Log of system action - System status update - Time available	D4-Failure to make a decision (impasse)	**- Lack of bridge team, fail to execute action**	- Operator alone on bridge, no one to discuss actions with	Escalation of situation, less time to avoid collision	- Ship collision	

ID	Operation description		Operational boundary and operator response				Hazard Identification					
	Ship type	Operator presence	Boundary condition	Operator role	Operator task(s)	Info required	Guideword	Hazardous event	Cause	Consequence	TOP event (worst case)	Safeguards
			"locked" position due to other ship B on SB and ship C astern									
28	Relevant for: All three ship types	2- Available (on bridge, at control position)	**Collision avoidance / communication system:** Other ship A on collision course (from SB), own ship not able to follow COLREG (give way), "locked" position due to other ship B on SB and ship C astern	Action (Take control)	Manoeuvring and navigation	- Log of system action - System status update - Time available	--	**- Same hazards as when operator is in backup, but with lower risk (due to more time to analyze and act).**	--	--	--	--
29	Relevant for: All three ship types	2- Available (on bridge, at control position)	**Collision avoidance / communication system:** Other ship A on collision course (from SB), own ship not able to follow COLREG (give way), "locked" position due to other ship B on SB and ship C astern	Action (Take control)	Maneuvering and navigation	- Log of system action - System status update - Time available	A8- Operation omitted	**- Unable to take action**	- Technical or software failure	Escalation of situation, less time to avoid collision	- Ship collision	

ID	Operation description		Operational boundary and operator response				Hazard Identification					
	Ship type	Operator presence	Boundary condition	Operator role	Operator task(s)	Info required	Guideword	Hazardous event	Cause	Consequence	TOP event (worst case)	Safeguards
30	Relevant for: All three ship types	2- Available (on bridge, at control position)	**Collision avoidance / communication system:** Other ship A on collision course (from SB), own ship not able to follow COLREG (give way), "locked" position due to other ship B on SB and ship C astern	Monitoring	Monitor	- Log of system action - System status update - Time available	A9- Operation incomplete	**- Lack of operator vigilance**	Boredom and/or fatigue	Escalation of situation, less time to avoid collision	- Ship collision	
31	Relevant for: All three ship types	2- Available (on bridge, at control position)	**Collision avoidance / communication system:** Other ship A on collision course (from SB), own ship not able to follow COLREG (give way), "locked" position due to other ship B on SB and ship C astern	Action (Take control)	Maneuvering and navigation	- Log of system action - System status update - Time available	D2- Incorrect decision based on right information	**- Interfering with system planned actions**	- Distrust in automation - Confusion of controller mode (operator or system) - Latency	Escalation of situation, less time to avoid collision	- Ship collision	

ID	Operation description		Operational boundary and operator response				Hazard Identification					
	Ship type	Operator presence	Boundary condition	Operator role	Operator task(s)	Info required	Guideword	Hazardous event	Cause	Consequence	TOP event (worst case)	Safeguards
32	Relevant for: All three ship types	2- Available (on bridge, at control position)	**Collision avoidance / communication system:** Other ship A on collision course (from SB), own ship not able to follow COLREG (give way), "locked" position due to other ship B on SB and ship C astern	Monitoring	Monitor	- Log of system action - System status update - Time available	A9-Operation incomplete	**- System malfunction** **- Multiple sensor failure** **- Bug**	Technical fault	MRC to be defined	Ship accident	Technical shore support office
33	Relevant for: All three ship types	2- Available (on bridge, at control position)	**Collision avoidance system:** High density traffic of pleasure crafts and kayak with. System limits in object classification. E.g. not able to differentiate between timber and kayaks. Collision risk.	Decision making	Analysis: - Visual identification - Takeover (adjust course, speed)	- Graphic images of the potential objects. - System classification uncertainties	S2-Wrong selection made	**- Incorrect object classification**	- Fog, distance, visibility - Quality of information	Escalation of situation, less time to avoid collision	- Ship collision	- If the system is in doubt it shall treat all object as potential navigational hazards

ID	Operation description		Operational boundary and operator response				Hazard Identification					
	Ship type	Operator presence	Boundary condition	Operator role	Operator task(s)	Info required	Guideword	Hazardous event	Cause	Consequence	TOP event (worst case)	Safeguards
34	Relevant for: All three ship types	1- Backup (not on bridge)	**Collision avoidance system:** High density traffic of pleasure crafts - Several sailboats in front, one or several attempt to cross. System not able to analyze (predict next movement)	Decision making	Select best option, e.g.: - 1. Continue ahead - 2. Turn SB 15d - 3. MRC (reduce speed, stay at position, etc.) -Identification, analysis, planning, action	- Log of system action - System status update - Time available	D3- Incorrect decision based on wrong/ missing information	**- The operator thinks that the system options are the only options available and takes a quick decision without evaluating other options that might be better.**	- Over trust system - Pressed for time, need to select option	Escalation of situation, less time to avoid collision	- Ship collision	
35	Relevant for: All three ship types	2- Available (on bridge, at control position)	Shifting ground conditions. Ship on collision course in narrow channel with uncertain and/or changing depth conditions due to sandbanks. Uncertain parameter.	Action (Take control)	Resolve the conflict between grounding and collision.	- Position - Speed - Direction of vessel - Depth - Distance to land - Seabed conditions	A9- Operation incomplete	**Conflict between collision avoidance and grounding avoidance**	- Environment (Current, weather) - Other traffic - Short cuts in order to optimize the route	- Beaching (if sand or seabed is shallow)	Ship collision or grounding	

ID	Operation description		Operational boundary and operator response				Hazard Identification					
	Ship type	Operator presence	Boundary condition	Operator role	Operator task(s)	Info required	Guideword	Hazardous event	Cause	Consequence	TOP event (worst case)	Safeguards
36	Relevant for: All three ship types	1- Backup (not on bridge)	**Collision avoidance system:** High density traffic of pleasure crafts - Several sailboats in front, one or several attempt to cross. System not able to analyze (predict next movement)	Decision making	Select best option: - 1. Continue ahead - 2. Turn SB 15d - 3. MRC (reduce speed, stay at position, etc.) - Identification - analysis - planning - action	- Log of system action - System status update - Time available	D2- Incorrect decision based on right information	**- Operator does not trust any of the options (although one is correct), and overrides the system**	- Lack of trust in system - Excessive belief in own capacity		- Ship collision	
3.2 Navigation & Maneuvering during transit (3.2.5 Communication with surroundings)												
37	Relevant for: All three ship types	1- Backup (not on bridge)	**Communication system:** Ship on collision course (e.g. with fishing vessel). Automated communication system not able to understand (language barrier/dialect) request from other ship.	Action (Take control)	- Communication with fishing vessel (call on VHF) - Based on communication, decide if takeover is needed	- Log of system action - System status update - Time available	A1- Operation too long/short	**- Communication failure**	- Operator spend too much time before communicating with the fishing vessel	- Unsolved risk continues - System deals with the situation	- Ship collision	

ID	Operation description		Operational boundary and operator response				Hazard Identification					
	Ship type	Operator presence	Boundary condition	Operator role	Operator task(s)	Info required	Guideword	Hazardous event	Cause	Consequence	TOP event (worst case)	Safeguards
38	Relevant for: All three ship types	1- Backup (not on bridge)	**Communication system:** Ship on collision course (e.g. with fishing vessel). Broken signal and lack of radio quality (technical error)	Action (Take control)	- Communication with fishing vessel (call on VHF) - Based on communication, decide if takeover is needed	- Log of system action - System status update - Time available	A1- Operation too long/short	- **Communication failure**	- Operator spend too much time before communicating with the fishing vessel	- Unsolved risk continues - System deals with the situation	- Ship collision	
39	Relevant for: All three ship types	1- Backup (not on bridge)	**Automated communication and navigation systems**	None	---	---	I3- Information communication incomplete	**Risk that autonomous vessels can create additional risk for its surroundings (other ships)**	- Communication by MASS not understood	Escalation of situations	Ship accident	
3.4 Trim, Stability & Stress during transit												
40	Relevant for: - Ocean going cargo ship (Bulk carrier) - Short-sea cargo ship (Container)	2- Available (on bridge, at control position)	**Ballast system:** Change of ballast water during transit. System start the process of changing the ballast water without being able to finish the operation due to heavy weather or shallow waters.	Decision making	- Decide if ballast exchange is to be continued or aborted.		A2- Operation mistimed	- **Misjudgment of environmental conditions.** - **Misjudgment of internal stability and stress conditions (free surface, hogg, sag)**	Swell, heave, shallow waters	-Lowering ship stability and affecting draft and trim	Capsizing	- Ballast treatment system

ID	Operation description		Operational boundary and operator response				Hazard Identification					
	Ship type	Operator presence	Boundary condition	Operator role	Operator task(s)	Info required	Guideword	Hazardous event	Cause	Consequence	TOP event (worst case)	Safeguards
6. Abnormal situations												
6.2 Abandon ship (Evacuation by partial- automated MES. MES needs activation by operator - sequence is automated)												
41	Short route domestic passenger ship	1- Backup (not on bridge)	**Evacuation system:** Evacuation of grounded passenger ferry.	Action (Take control)	- Crisis management - Get passenger to muster station - Instruct - Evacuation - Acceptance of MES activation - Counting the passengers		A1- Operation too long/short	**Fail to evacuate/ unsuccessful evacuation**	- Lack of crowd management - Passenger panicking - Passenger occupying crew - Disabled or injured passengers, children - Distrust in system - Irrational behaviour	- Use too long time to evacuate - Not able to evacuate - Passengers left onboard	Injuries Loss of life	- Automated system capabilities - Automatic people count - Automatic launch - Big sign boards - Audio evacuation instructions
42	Short route domestic passenger ship	1- Backup (not on bridge)	**Evacuation system:** Evacuation of grounded passenger ferry. Lack of stability, water ingress and fire.	Action (Take control)	- Maintain vessel watertight integrity and stability during evacuation		A9- Operation incomplete	**Fail to handle situation**	- Lack of info - Lack of situational awareness - Complexity - Stress	MRC to be defined	Vessel sinking Vessel capsizing	Automated systems: - Ballast management - Bilge management - Cross flooding arrangements
6.1 Fire (Fire-fighting measures)												
43	Short route domestic passenger ship	1- Backup (not on bridge)	**Fire system:** Fire in car on Ro-Ro deck. Operator unable to locate the fire and start fire extinguishing measures immediately.	Action (Take control)	- Identify and extinguish		A1- Operation too long/short	**Fail to handle situation**	- Lack of info - Lack of situational awareness - Complexity - Stress	MRC to be defined	Fire escalating	

ID	Operation description		Operational boundary and operator response				Hazard Identification					
	Ship type	Operator presence	Boundary condition	Operator role	Operator task(s)	Info required	Guideword	Hazardous event	Cause	Consequence	TOP event (worst case)	Safeguards
44	Relevant for: All three ship types	1- Backup (not on bridge)	**Fire system:** Fully automated fire system.	Action (Take control)	- Identify and extinguish		A7-Wrong operation on right object	**- Applying total flooding when not needed.**	Incorrect configuration of automated system	MRC to be defined	Equipment damage	- Confirmation of hazard upon activation of fire system - Option to abort action - However this would occupy operator availability, and be a complex task to conduct
45	Relevant for: All three ship types	1- Backup (not on bridge)	**Fire system:** Conditional automated fire system. Unable to determine source of fire	Action (Take control)	- Identify and extinguish		A1-Operation too long/short	**- Operator unable to locate the fire**	- Occupied with other tasks - Lack of information	MRC to be defined	Fire escalating	
46	Relevant for: All three ship types	1- Backup (not on bridge)	**Fire system**: System constraints in detecting situation escalation (both positive and negative)				R1-Information not obtained	**- Fire escalates without the system detecting the escalation**	Unable to detect relatively small changes in flames, heat etc.	MRC to be defined	Fire escalating	
6.4 Search and Rescue (SAR)												

ID	Operation description		Operational boundary and operator response				Hazard Identification					
	Ship type	Operator presence	Boundary condition	Operator role	Operator task(s)	Info required	Guideword	Hazardous event	Cause	Consequence	TOP event (worst case)	Safeguards
47	Relevant for: - Ocean going cargo ship (Bulk carrier) - Short-sea cargo ship (Container)	1- Backup (not on bridge)	**Rescue craft operation:** Encounter sailboat in distress in the middle of the ocean. Constraint to get the people in distress on board	Action (Take control)	Get sailboat crew onboard, MOB craft - MOB team: 2 - Davit operator: 0 (remote controlled) - Master Operator:1		A1- Operation too long/short	**- Malfunction of the Davit system** **- Operator alone on bridge**	- Crew occupied with MOB (rescue op). - Only 2 persons onboard	- One operator can do manual handling of the davit system	Unsuccessful sailboat rescue	
48	Relevant for: - Ocean going cargo ship (Bulk carrier) - Short-sea cargo ship (Container)	1- Backup (not on bridge)	**Rescue craft operation:** Encounter sailboat in distress in the middle of the ocean. Constraint to get the people in distress on board	Action (Take control)	Get sailboat crew onboard, MOB craft - MOB team: 2 - Davit operator: 0 (remote controlled) - Master Operator:1		A1- Operation too long/short	**- Other tasks that needs to be dealt with by the crew, parallel to MOB craft operation** **- Multi-error fire alarm** **- flooding**	- Crew occupied with MOB (rescue op). - Only 2 persons onboard		Unsuccessful sailboat rescue	
49	Relevant for: All three ship types	1- Backup (not on bridge)	**Object detection:** Sailboat in distress. Sailboat has no (or broken) radio communication. Signals for help only with hand gestures.	None	---	---	R1- Information not obtained	**- Not identifying the situation**	No operators on bridge	- The people in distress are not saved	Injuries Loss of life	- Possibility to identify all type of distress signals including hand gestures (waving)?

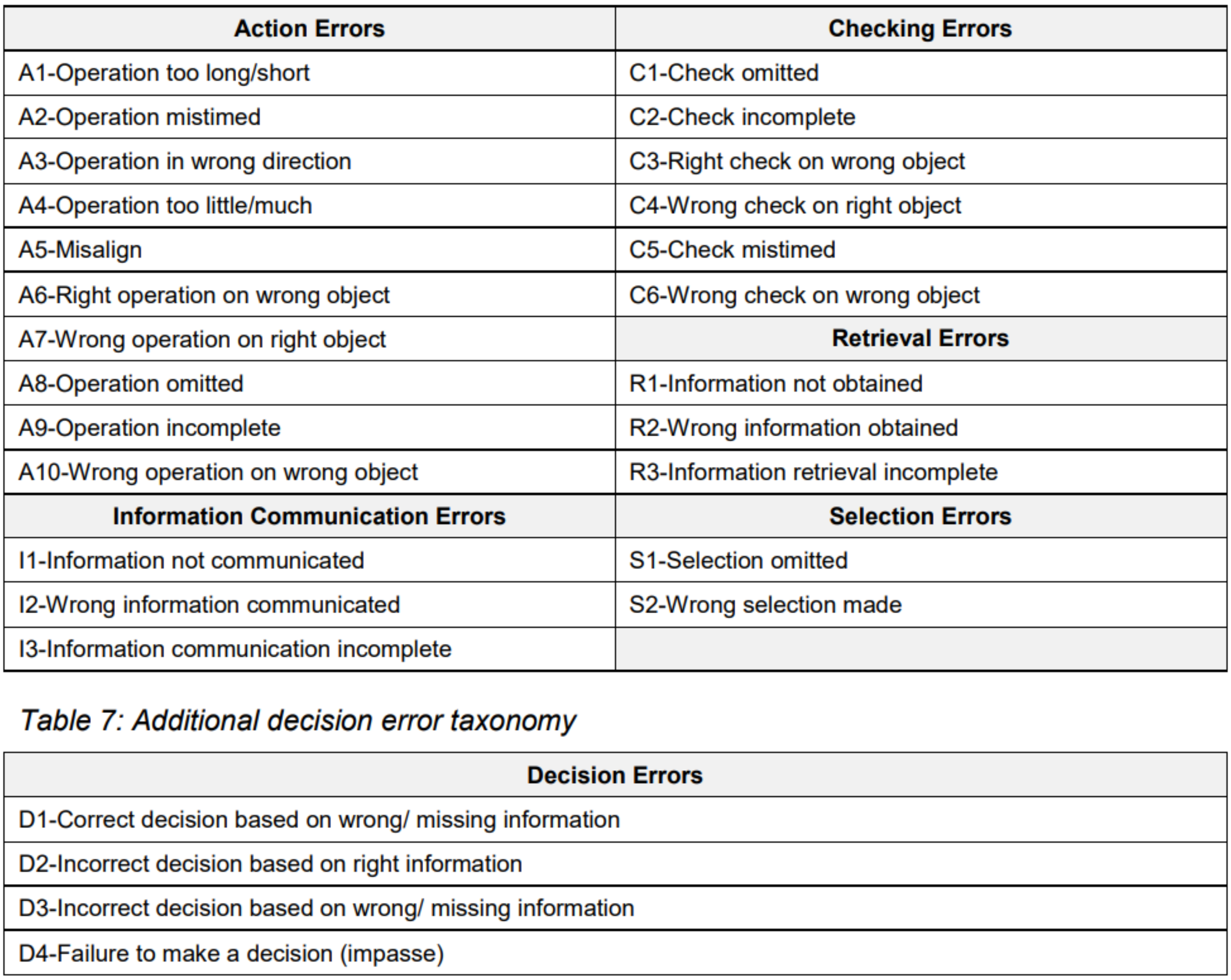
ID	Operation description		Operational boundary and operator response				Hazard Identification					
	Ship type	Operator presence	Boundary condition	Operator role	Operator task(s)	Info required	Guideword	Hazardous event	Cause	Consequence	TOP event (worst case)	Safeguards
50	Relevant for: All three ship types	2- Available (on bridge, at control position)	**Object detection:** Sailboat in distress. Sailboat has no (or broken) radio communication. Signals for help only with hand gestures.	Monitoring	- Lookout		C2-Check incomplete	**- Not identifying the situation**	- Workload / fatigue - Lack of human resources	- The people in distress are not saved	Injuries Loss of life	
6.6 Damage control (6.6.4 Heavy weather damage)												
51	Ocean going cargo ship (Bulk)	1- Backup (not on bridge)	**Cargo securing**: Bulk cargo hatch damaged due to heavy weather resulting in water ingress. Green sea.	Action (Take control)	- Situational evaluation	- Information from sensors. - Hatch motion securing sensors - ingress sensor - water detection	A4-Operation too little/much	**- Not able to do the correct action with limited manpower**	- Crew shortage.	Water ingress	- Heavy weather damage - Capsize - Flooding - Cargo damage	- MRC. Adjust heading and speed - Manoeuvre up against the wind, to limit water ingress - Ballasting - Secure cargo hatch
52	Ocean going cargo ship (Bulk)	1- Backup (not on bridge)	Collision with iceberg resulting in water ingress. Hull damage and water ingress.	Action (Take control)	- Assess damage stability and contingency - Communicating with SAR - Position keeping - Minimize further damage	- Information from sensors. - Hatch motion securing sensors - ingress sensor - water detection	A4-Operation too little/much	**- Not able to do the correct action with limited manpower**	- Crew shortage.	Water ingress	- Heavy weather damage - Capsize - Flooding - Cargo damage	- MRC. Adjust heading and speed - Manoeuvre up against the wind, to limit water ingress - Ballasting - Secure cargo hatch - Position keeping
6.7 Blackout												

ID	Operation description		Operational boundary and operator response				Hazard Identification					
	Ship type	Operator presence	Boundary condition	Operator role	Operator task(s)	Info required	Guideword	Hazardous event	Cause	Consequence	TOP event (worst case)	Safeguards
53	Relevant for: All three ship types	1- Backup (not on bridge)	Blackout	Action (Take control)	Ensure successful blackout recovery		A9- Operation incomplete	**Fail to recover from blackout**	- Crew shortage - Complexity - Stress - Lack of training	Escalation of situation	Ship accident	- Automated blackout recovery systems - Means of blackout prevention
6.8 Emergency communication												
54	Ocean going cargo ship (Bulk)	2- Available (on bridge, at control position)	**Abnormal conditions:** Fire, collision, grounding, flooding e.g.)	Action (Take control)	Contact SAR		A4- Operation too little/much	**- Insufficient safety message broadcast**	- System not able to relay safety message due to the complexity of the situation	- Vessel does not receive correct emergency assistance	- Escalation of abnormal situation	
Maintenance and repairs												
1.4 Maintenance and repairs of Bridge-equipment												
2.8 Maintenance and repairs of Deck-equipment												
5.7 Maintenance and repairs of Engine-equipment												
55	Relevant for: All three ship types	1- Backup (not on bridge)	Insufficient cleaning, tidying of workplace.	None	---	---	A9- Operation incomplete	**- Oil and lube leakage** **- Unsecured object**	- Insufficient cleaning - Lack of routine - Fatigue, boredom	- Fire - Unsecured object	Fire	- Cleaning and tidying procedures - Object detection system/alarm - Automated cleaning
56	Relevant for: All three ship types	1- Backup (not on bridge)	Insufficient maintenance and repairs	None	---	---	A9- Operation incomplete	**- Insufficient maintenance and repairs**	- Unable to detect or rectify maintenance and repair	- Malfunction of critical equipment	Fire	
57	Relevant for: All three ship types	1- Backup (not on bridge)	Insufficient maintenance and repairs conducted	None	---	---	A9- Operation incomplete	**- Lack of ownership** **- Unfamiliar with vessel**	- Outsourced company spend limited time onboard.	- Malfunction of critical equipment	Fire	

ID	Operation description		Operational boundary and operator response				Hazard Identification					
	Ship type	Operator presence	Boundary condition	Operator role	Operator task(s)	Info required	Guideword	Hazardous event	Cause	Consequence	TOP event (worst case)	Safeguards
			by outsourced company					**characteristics.**				

APPENDIX C – GUIDEWORDS

Table 19 – SHERPA taxonomy (found in Petro-HRA guideline /18/)



Action Errors	**Checking Errors**
A1-Operation too long/short	C1-Check omitted
A2-Operation mistimed	C2-Check incomplete
A3-Operation in wrong direction	C3-Right check on wrong object
A4-Operation too little/much	C4-Wrong check on right object
A5-Misalign	C5-Check mistimed
A6-Right operation on wrong object	C6-Wrong check on wrong object
A7-Wrong operation on right object	**Retrieval Errors**
A8-Operation omitted	R1-Information not obtained
A9-Operation incomplete	R2-Wrong information obtained
A10-Wrong operation on wrong object	R3-Information retrieval incomplete
Information Communication Errors	**Selection Errors**
I1-Information not communicated	S1-Selection omitted
I2-Wrong information communicated	S2-Wrong selection made
I3-Information communication incomplete	

Table 7: Additional decision error taxonomy

Decision Errors
D1-Correct decision based on wrong/ missing information
D2-Incorrect decision based on right information
D3-Incorrect decision based on wrong/ missing information
D4-Failure to make a decision (impasse)

Human-related hazards from the FSA guideline /8/.

Personal factors

.1 Reduced ability, e.g. reduced vision or hearing;

.2 Lack of motivation, e.g. because of a lack of incentives to perform well;

.3 Lack of ability, e.g. lack of seamanship, unfamiliarity with vessel, lack of fluency of the language used on board;

.4 Fatigue, e.g. because of lack of sleep or rest, irregular meals; and

.5 Stress.

Organizational and leadership factors

.1 Inadequate vessel management, e.g. inadequate supervision of work, lack of coordination of work, lack of leadership;

.2 Inadequate shipowner management, e.g. inadequate routines and procedures, lack of resources for maintenance, lack of resources for safe operation, inadequate follow-up of vessel organization;

.3 Inadequate manning, e.g. too few crew, untrained crew; and

.4 Inadequate routines, e.g. for navigation, engine-room operations, cargo handling, maintenance, emergency preparedness.

Task features

.1 Task complexity and task load, i.e. too high to be done comfortably or too low causing boredom;

.2 Unfamiliarity of the task;

.3 Ambiguity of the task goal; and

.4 Different tasks competing for attention.

Onboard working conditions

.1 Physical stress from, e.g. noise, vibration, sea motion, climate, temperature, toxic substances, extreme environmental loads, night-watch;

.2 Ergonomic conditions, e.g. inadequate tools, inadequate illumination, inadequate or ambiguous information, badly-designed human-machine interface;

.3 Social climate, e.g. inadequate communication, lack of cooperation; and

.4 Environmental conditions, e.g. restricted visibility, high traffic density, restricted fairway.

APPENDIX D – FTA AND RCM TABLE

	Fault tree analysis			Risk control measures		
FTA ID	**Event description**	**Causes**	**Accident scenario/ sequence of events**	**RCM ID**	**Topics**	**RCM descriptions**
0.0	**TOP event: Collision**					
1.1.1	Other vessels unable to comply with rules (etc. technical failures, operational capabilities).	Multiple causes, such as officer falls asleep etc - risk as today/ not an emerging risk.	-> 1.1 Early navigation error by other vessels causes limited room for manoeuvrability --> 1.0 Early navigation error by vessels involved causes limited room for manoeuvrability *AND* ---> 2.0 Two or more vessels involved fails to perform collision avoidance manoeuvring ----> 0.0 Collision between MASS and other vessel(s)	**RCM-01**	MASS to take early actions to avoid collisions.	a) The automated navigation system should be verified to fully comply with the navigational parts of COLREG, including Rule 2 and rule 17 which describe actions needed in order to avoid collision when the other vessel is not behaving as expected. b) The MASS system should be able to interpret sound and light signals from other vessels according to COLREG rules 34.
1.1.2.1	Over-reliance in automation by other vessels.	i. Non-MASS have frequently experienced that MASS successfully avoids collisions.	->1.1.2 Other vessels not willing to comply with rules (violation) -->1.1 Navigation error by other vessels causes limited room for manoeuvrability --->1.0 Navigation error by vessels involved causes limited room for manoeuvrability *AND* --->2.0 Two or more vessels involved fails to perform collision avoidance manoeuvring ----> 0.0 Collision between MASS and other vessel(s)	**RCM-02**	MASS system to consider violation scenarios performed by external parties as part of design.	a) Consider acts of violation when defining MRCs.

	Fault tree analysis			Risk control measures		
FTA ID	**Event description**	**Causes**	**Accident scenario/ sequence of events**	**RCM ID**	**Topics**	**RCM descriptions**
1.1.2.2	Other vessels perform act of terror/ sabotage.	Commercial, political or ideological motive - risk as today/ not an emerging risk.	-> 1.1.2 Other vessels not willing to comply with rules (violation) --> 1.1 Navigation error by other vessels causes limited room for manoeuvrability ---> 1.0 Navigation error by vessels involved causes limited room for manoeuvrability *AND* ---> 2.0 Two or more vessels involved fails to perform collision avoidance manoeuvring ----> 0.0 Collision between MASS and other vessel(s)	**RCM-03**	MASS system to consider violation scenarios performed by external parties as part of design.	a) High level of security for control system responsible for initiating MRC, incl. being independent from control system responsible for normal operations. b) MASS to be ISPS compliant and recognize emerging terror scenarios.
1.1.2.3	Other vessels misinterpret MASS navigational intentions	i. Other vessel crew not familiar with MASS design and operation.	-> 1.1.2 Other vessels not willing to comply with rules (violation) --> 1.1 Navigation error by other vessels causes limited room for manoeuvrability ---> 1.0 Navigation error by vessels involved causes limited room for manoeuvrability *AND* ---> 2.0 Two or more vessels involved fails to perform collision avoidance manoeuvring ----> 0.0 Collision between MASS and other vessel(s)	**RCM-04**	Create predictability about MASS capabilities and movements within the maritime community (other vessels, vessel traffic service etc.)	a) MASS type/status/capabilities to be broadcasted to other vessel e.g. by AIS or navigation lights. b) The MASS should be able to indicate it's manoeuvring intensions with sound and light signals as specified in COLREG rule 34. c) The automated navigation system should be verified to fully comply with the navigation parts of COLREG, including rule 8 which among other things states that all actions to avoid collisions shall be performed in ample time, and be readily apparent for other vessels.
1.2.1	MASS navigational system failure (e.g. software design).	i. Faulty software design ii. Incorrect software coding iii. Poor object detection e.g. due to sensor failures, environmental conditions. iv. System state deteriorated but not detected, e.g. actuator failure not detected	-> 1.2 Early navigation error by MASS causes limited room for manoeuvrability --> 1.0 Navigation error by vessels involved causes limited room for manoeuvrability *AND* --> 2.0 Two or more vessels involved fails to perform collision avoidance manoeuvring ---> 0.0 Collision between MASS and other vessel(s)	**RCM-05**	Ensure sufficient control system reliability.	a) The automated navigation (control) system should be verified towards established rules and standards by an independent party. b) Implement proper assurance framework of control systems, providing assurance of both products and process. c) The automated navigation system should automatically be monitored for failures and sub-par performance. d) Sufficient test of all safety critical components (e.g. simulator test of COLREG system, test of object detection systems). e) The MASS should at all times have the

	Fault tree analysis			Risk control measures		
FTA ID	Event description	Causes	Accident scenario/ sequence of events	RCM ID	Topics	RCM descriptions
						possibility to enter at least one pre-defined minimum risk condition (MRC) in the case of significant equipment failures.
1.2.2.1	Incorrect input parameters provided by MASS operator.	i. Insufficient competence ii. Inadequate procedures/ routines iii. Useability of software/ interfaces	-> 1.2.2 MASS provided with wrong navigation parameters (pre-initiator) --> 1.2 Early navigation error by MASS causes limited room for manoeuvrability ---> 1.0 Navigation error by vessels involved causes limited room for manoeuvrability *AND* ---> 2.0 Two or more vessels involved fails to perform collision avoidance manoeuvring ----> 0.0 Collision between MASS and other vessel(s)	**RCM-06**	Implement measures to prevent human error when working on navigation software.	a) There should be a strict separation between parameters that are expected to be changed during operation, and parameters that are NOT expected to be changed during normal operation. b) Parameters that are NOT expected to be changed during operation should be protected by special access-control measures and should NOT be changeable while the system is in operation. c) Software updates and changing of the basic system configuration should NOT be possible while the system is in operation. d) Apply principles of error tolerant design for software interfaces (see standards such as ISO 11064, ISO 9241-110 and ISO 9241-210).
1.2.2.2	Incorrect configuration/ set-up provided by shore parties	i. Insufficient competence ii. Inadequate procedures/ routines iii. Useability of software/ interfaces	-> 1.2.2 MASS provided with wrong navigation parameters (pre-initiator) --> 1.2 Early navigation error by MASS causes limited room for manoeuvrability ---> 1.0 Navigation error by vessels involved causes limited room for manoeuvrability *AND* ---> 2.0 Two or more vessels involved fails to perform collision avoidance manoeuvring ----> 0.0 Collision between MASS and other vessel(s)	**RCM-07**	Implement measures to prevent human error when working on navigation software.	Same as: - RCM-06 a) to d) - and in addition; a) After changes are performed on software or the system configuration, a thorough verification process should be successfully executed before the system is put back into operation.

	Fault tree analysis			Risk control measures		
FTA ID	Event description	Causes	Accident scenario/ sequence of events	RCM ID	Topics	RCM descriptions
1.3.1	Unsuccessful communication by other vessel(s).	Multiple causes - risk as today/ not an emerging risk.	-> 1.3 Unsuccessful communication between vessels involved --> 1.0 Navigation error by vessels involved causes limited room for manoeuvrability *AND* --> 2.0 Two or more vessels involved fails to perform collision avoidance manoeuvring ---> 0.0 Collision between MASS and other vessel(s)	**RCM-08**	MASS to take mitigating actions in case adjacent vessels fail to respond/ communicate.	Same as: - RCM-01 a), - and in addition; a) Notify MASS operator about unsuccessful communication on portable alarm device (if not already at bridge).
1.3.2.1.1	Automated communication by MASS system fails (software or technical failure).	i. Faulty software design ii. Incorrect software coding iii. Poor object detection e.g. due to sensor failures, environmental conditions. iv. System state deteriorated but not detected, e.g. actuator failure not detected	-> 1.3.2.1 Unsuccessful automated communication by MASS system with other vessel(s) *AND* -> 1.3.2.2 MASS operator fails successfully to communicate with other vessels --> 1.3.2 Unsuccessful communication by MASS with other vessels ---> 1.3 Unsuccessful communication between vessels involved ----> 1.0 Navigation error by vessels involved causes limited room for manoeuvrability *AND* ----> 2.0 Two or more vessels involved fails to perform collision avoidance manoeuvring -----> 0.0 Collision between MASS and other vessel(s)	**RCM-09**	Ensure sufficient redundancy/ reliability in the communication function.	Same as: - RCM-05 a) to e) - and in addition; a) MASS operator to be immediately alerted in case of failure on communication system.

	Fault tree analysis			Risk control measures		
FTA ID	Event description	Causes	Accident scenario/ sequence of events	RCM ID	Topics	RCM descriptions
1.3.2.1.2	Poor/ inadequate communication by MASS system (not understood by other vessels)	i. Poor quality of message provided by the communication system, e.g.; - Sound - Language, phrases used ii. Other vessels not familiar with MASS ways of communicating	-> 1.3.2.1 Unsuccessful automated communication by MASS system with other vessel(s) *AND* -> 1.3.2.2 MASS operator fails successfully to communicate with other vessels --> 1.3.2 Unsuccessful communication by MASS with other vessels ---> 1.3 Unsuccessful communication between vessels involved ----> 1.0 Navigation error by vessels involved causes limited room for manoeuvrability *AND* ----> 2.0 Two or more vessels involved fails to perform collision avoidance manoeuvring -----> 0.0 Collision between MASS and other vessel(s)	**RCM-10**	MASS system to be able to communicate with other vessels.	COLREG rules for avoiding collisions are not depending on verbal communication between the crews of the different vessels, in order to avoid collisions. As such, same as: - RCM-04 a) to c) - and in addition; a) MASS system to communicate with other vessels in due time by distributing and transmitting VHF messages according to the standard Marine Communication Phrases (SMCP). b) The MASS systems should be able to relay incoming radio traffic (VHF) to a MASS operator (if part of operation), and allow for human-human communication with other vessels. c) MASS operators to be notified when MASS system initiates communication with vessels. d) Provide means so that it is easy for MASS operator to listen in on communication from other locations than the bridge.

	Fault tree analysis			Risk control measures		
FTA ID	Event description	Causes	Accident scenario/ sequence of events	RCM ID	Topics	RCM descriptions
1.3.2.2.1.1	MASS operator(s) intentionally do not muster on bridge.	i. Over-reliance in automation by MASS operator(s). ii. High workload/ crew shortage. iii. Event not perceived as critical - MASS operators prioritize other tasks.	-> 1.3.2.2.1 MASS operator fails to muster on bridge --> 1.3.2.2 MASS operator fails successfully to communicate with other vessels *AND* --> 1.3.2.1 Unsuccessful automated communication by MASS system with other vessel(s) ---> 1.3.2 Unsuccessful communication by MASS with other vessels ----> 1.3 Unsuccessful communication between vessels involved -----> 1.0 Navigation error by vessels involved causes limited room for manoeuvrability *AND* -----> 2.0 Two or more vessels involved fails to perform collision avoidance manoeuvring ------> 0.0 Collision between MASS and other vessel(s)	**RCM-11**	Ensure availability of MASS operator to supervise and (if necessary) control MASS operations.	Same as: - RCM-10 d) - and in addition; a) Clear routines and procedures for when to muster/ be in proximity of/ or present on bridge. Criteria for presence can be traffic density, failures or limitations in the automation system, weather conditions and visibility, water depth, width of passage, and availability of infrastructure. b) Portable alarm system to indicate event criticality. c) Limit number of alarms/ notifications given to operator to avoid "alarm fatigue". d) The system should escalate alarms and possibly go into a minimum risk condition (MRC) if the operator is not mustering on the bridge within a given time (see also RCM-12 c)).

	Fault tree analysis			Risk control measures		
FTA ID	Event description	Causes	Accident scenario/ sequence of events	RCM ID	Topics	RCM descriptions
1.3.2.2.1.2.1	MASS operator(s) not informed event.	i. MASS operator 1 does not observe alarm on portable device (does not carry alarm, noisy environments, technical failure etc.) AND; ii. MASS operator 2 being unavailable (multiple causes e.g. asleep, sick)	-> 1.3.2.2.1.2 MASS operator unintentionally does not muster on bridge --> 1.3.2.2.1 MASS operator fails to muster on bridge ---> 1.3.2.2 MASS operator fails successfully to communicate with other vessels *AND* ---> 1.3.2.1 Unsuccessful automated communication by MASS system with other vessel(s) ----> 1.3.2 Unsuccessful communication by MASS with other vessels -----> 1.3 Unsuccessful communication between vessels involved ------> 1.0 Navigation error by vessels involved causes limited room for manoeuvrability *AND* ------> 2.0 Two or more vessels involved fails to perform collision avoidance manoeuvring -------> 0.0 Collision between MASS and other vessel(s)	**RCM-12**	Ensure that MASS operators are informed about unsuccessful communication or failure in communication system.	a) Ensure high reliability and availability of portable alarm device, e.g. by; - routine to always carry device - securely attachment of device - sufficient light and audio signal - good quality and sufficient IP rating - good signals in areas visited by operators - off-duty operator to be notified if alarm is not acknowledged b) Clear routines for how to act in case 1 / 2 operators are indisposed. c) The MASS should at all times have the possibility to enter at least one pre-defined minimum risk condition (MRC) in the case of operator inaction within time criteria pre-defined for critical events and failures.

	Fault tree analysis			Risk control measures		
FTA ID	Event description	Causes	Accident scenario/ sequence of events	RCM ID	Topics	RCM descriptions
1.3.2.2.1.2.2	MASS operator(s) are informed about event but prevented from mustering on bridge (in time).	i. MASS operator 1 is located too far away from bridge (unclear routines, poor handover etc.) AND; ii. MASS operator 2 being unavailable (multiple causes e.g. asleep, sick)	-> 1.3.2.2.1.2 MASS operator unintentionally does not muster on bridge --> 1.3.2.2.1 MASS operator fails to muster on bridge ---> 1.3.2.2 MASS operator fails successfully to communicate with other vessels *AND* ---> 1.3.2.1 Unsuccessful automated communication by MASS system with other vessel(s) ----> 1.3.2 Unsuccessful communication by MASS with other vessels -----> 1.3 Unsuccessful communication between vessels involved ------> 1.0 Navigation error by vessels involved causes limited room for manoeuvrability *AND* ------> 2.0 Two or more vessels involved fails to perform collision avoidance manoeuvring -------> 0.0 Collision between MASS and other vessel(s)	**RCM-13**	Ensure that MASS operators are made available to muster to the bridge in due time.	Same as: - RCM-11 a) to d) - RCM-12 c) - and in addition; a) Time until warning and/ or alarms should be defined by how far away from the bridge (or other control station) the operator is located. b) Communication equipment combined with displays showing navigational information located in an location additional to the bridge.

	Fault tree analysis			Risk control measures		
FTA ID	**Event description**	**Causes**	**Accident scenario/ sequence of events**	**RCM ID**	**Topics**	**RCM descriptions**
1.3.2.2.2	MASS operator musters on bridge but fails to successfully communicate with other vessel(s)	i. Skill degradation e.g. caused by; - inadequate training - limited experience due to automation ii. Communication equipment (incl. Information displays) not suitable for task; - complex to use - information unavailable, e.g. requires time consuming navigation between images on HMI displays	-> 1.3.2.2 MASS operator fails successfully to communicate with other vessels *AND* -> 1.3.2.1 Unsuccessful automated communication by MASS system with other vessel(s) --> 1.3.2 Unsuccessful communication by MASS with other vessels ---> 1.3 Unsuccessful communication between vessels involved ----> 1.0 Navigation error by vessels involved causes limited room for manoeuvrability *AND* ----> 2.0 Two or more vessels involved fails to perform collision avoidance manoeuvring -----> 0.0 Collision between MASS and other vessel(s)	**RCM-14**	Provide the MASS operators with sufficient competence in how to communicate with other vessels, incl. use of equipment.	a) Combined use of training and actual field experience with communication equipment. b) Ensure high degree of usability on communication equipment and associated human-machine interfaces (see standards such as ISO 11064, ISO 9241-110 and ISO 9241-210).
2.1	Other vessel(s) fails to perform collision avoidance manoeuvring.	Risk as today/ not an emerging risk.	*AND* -> 2.2 MASS fails to perform «last minute» collision avoidance manoeuvring --> 2.0 Two or more vessels involved fails to perform collision avoidance manoeuvring *AND* --> 1.0 Navigation error by vessels involved causes limited room for manoeuvrability ---> 0.0 Collision between MASS and other vessel(s)	**RCM-15**	Ensure MASS safety by defining MRCs.	Same as: - RCM-01 a) - and in addition: a) Define (as part of design) MRCs for when the MASS system recognizes it is not able to re-enter a normal operational state (i.e. comply with COLREG).

	Fault tree analysis			Risk control measures		
FTA ID	Event description	Causes	Accident scenario/ sequence of events	RCM ID	Topics	RCM descriptions
2.2.1.1.1	MASS navigational system failure (e.g. software design).	i. Faulty software design ii. Incorrect software coding iii. Poor object detection e.g. due to sensor failures, environmental conditions. iv. System state deteriorated but not detected, e.g. actuator failure not detected	-> 2.2.1.1 MASS system performs incorrect manoeuvring --> 2.2.1 MASS commits «last minute» manoeuvring error (responsible for collision) *AND* --> 2.2.2 MASS fails to perform «last minute» collision avoidance manoeuvring ---> 2.2 MASS fails to perform «last minute» collision avoidance manoeuvring ----> 2.0 Two or more vessels involved fails to perform collision avoidance manoeuvring *AND* ----> 1.0 Navigation error by vessels involved causes limited room for manoeuvrability -----> 0.0 Collision between MASS and other vessel(s)	**RCM-16**	Ensure sufficient control system reliability.	Same as: - RCM-05 b) e) and d)

	Fault tree analysis			Risk control measures		
FTA ID	Event description	Causes	Accident scenario/ sequence of events	RCM ID	Topics	RCM descriptions
2.2.1.1.2.1	Incorrect navigation input provided by MASS operator	i. Insufficient competence ii. Inadequate procedures/ routines iii. Useability of software/ interfaces	-> 2.2.1.1.2 Incorrect navigation parameters in MASS system --> 2.2.1.1 MASS system performs incorrect manoeuvring ---> 2.2.1 MASS commits «last minute» manoeuvring error (responsible for collision) *AND* ---> 2.2.2 MASS fails to perform «last minute» collision avoidance manoeuvring ----> 2.2 MASS fails to perform «last minute» collision avoidance manoeuvring -----> 2.0 Two or more vessels involved fails to perform collision avoidance manoeuvring *AND* -----> 1.0 Navigation error by vessels involved causes limited room for manoeuvrability ------> 0.0 Collision between MASS and other vessel(s)	**RCM-17**	Implement measures to prevent human error when working on navigation software.	Same as: - RCM-06 a) to d)

	Fault tree analysis			Risk control measures		
FTA ID	Event description	Causes	Accident scenario/ sequence of events	RCM ID	Topics	RCM descriptions
2.2.1.1.2.2	Incorrect configuration/ set-up provided by shore parties	i. Insufficient competence ii. Inadequate procedures/ routines iii. Useability of software/ interfaces	-> 2.2.1.1.2 Incorrect navigation parameters in MASS system --> 2.2.1.1 MASS system performs incorrect manoeuvring ---> 2.2.1 MASS commits «last minute» manoeuvring error (responsible for collision) *AND* ---> 2.2.2 MASS fails to perform «last minute» collision avoidance manoeuvring ----> 2.2 MASS fails to perform «last minute» collision avoidance manoeuvring -----> 2.0 Two or more vessels involved fails to perform collision avoidance manoeuvring *AND* -----> 1.0 Navigation error by vessels involved causes limited room for manoeuvrability ------> 0.0 Collision between MASS and other vessel(s)	**RCM-18**	Implement measures to prevent human error when working on navigation software.	Same as: - RCM-06 a) to d) - RCM-07 a)
2.2.1.2	Operator incorrectly intervenes with successful MASS performance (overrides system).	i. Operator distrusts decisions/actions made by MASS. ii. Operator misinterprets decisions/ actions made by MASS (mode confusion).	-> 2.2.1 MASS commits «last minute» manoeuvring error (responsible for collision) *AND* -> 2.2.2 MASS fails to perform «last minute» collision avoidance manoeuvring --> 2.2 MASS fails to perform «last minute» collision avoidance manoeuvring ---> 2.0 Two or more vessels involved fails to perform collision avoidance manoeuvring *AND* ---> 1.0 Navigation error by vessels involved causes limited room for manoeuvrability ----> 0.0 Collision between MASS and other vessel(s)	**RCM-19**	Prevent mode confusion and distrust in automation among MASS operators.	a) Provide MASS operator with sufficient training in MASS system automation, incl.; - system diagnostics in time critical situations - share experiences about more and less reliable functions, and relevant mitigations - regular simulator training similar to BRM, courses. b) The MASS system should be designed according to principles of "closed loop dynamics" (include operator in the loop by interaction with automation and information flows creating situational awareness).

	Fault tree analysis			Risk control measures		
FTA ID	Event description	Causes	Accident scenario/ sequence of events	RCM ID	Topics	RCM descriptions
2.2.2.1	MASS system fails to regain normal operational state (due to limitations in navigational capability).	i. Limitations in MASS navigational capability by design. Failures in MASS automation system covered by 2.2.1.1.1.	*AND* -> 2.2.2.2 MASS system fails to enter MRC when exceeding navigational capabilities (independently from operator) *AND* -> 2.2.2.3 MASS operator fail to take corrective action/ maintains collision course --> 2.2.2 MASS fails to perform «last minute» collision avoidance manoeuvring *AND* --> 2.2.1 MASS commits «last minute» manoeuvring error (responsible for collision) ---> 2.2 MASS fails to perform «last minute» collision avoidance manoeuvring ----> 2.0 Two or more vessels involved fails to perform collision avoidance manoeuvring *AND* ----> 1.0 Navigation error by vessels involved causes limited room for manoeuvrability -----> 0.0 Collision between MASS and other vessel(s)	**RCM-20**	Ensure MASS safety by defining MRCs.	Same as: - RCM-15 a)

	Fault tree analysis			Risk control measures		
FTA ID	Event description	Causes	Accident scenario/ sequence of events	RCM ID	Topics	RCM descriptions
2.2.2.2	MASS system fails to enter MRC when exceeding navigational capabilities (independent from/ without intervention from operator).	i. Limitations in MASS navigational capability by design. ii. MRC not defined during design stage of MASS.	*AND* -> 2.2.2.1 MASS system fails to regain normal operational state (due to limitations in navigational capability) *AND* -> 2.2.2.3 MASS operator fail to take corrective action/ maintains collision course --> 2.2.2 MASS fails to perform «last minute» collision avoidance manoeuvring *AND* --> 2.2.1 MASS commits «last minute» manoeuvring error (responsible for collision) ---> 2.2 MASS fails to perform «last minute» collision avoidance manoeuvring ----> 2.0 Two or more vessels involved fails to perform collision avoidance manoeuvring *AND* ----> 1.0 Navigation error by vessels involved causes limited room for manoeuvrability -----> 0.0 Collision between MASS and other vessel(s)	**RCM-21**	Ensure MASS safety by defining MRCs.	a) There should at all times be more than one MRC available. b) Ensure that system responsible for taking the MASS into an MRC is independent of the MASS navigational system. c) For each identified MRC, consider whether it is feasible for the MASS operator to aid the MASS system and/or function as a back-up in a reliable manner. d) Test and verify that the MASS system is able to detect all scenarios where MRC should be initiated.

	Fault tree analysis			Risk control measures		
FTA ID	Event description	Causes	Accident scenario/ sequence of events	RCM ID	Topics	RCM descriptions
2.2.2.3.1.1	MASS operator(s) intentionally do not muster on bridge.	i. Over-reliance in automation by MASS operator(s). may have frequently observed that the MASS system successfully avoids collisions. ii. High workload/ crew shortage. iii. Event not perceived as critical - MASS operators prioritize other tasks.	-> 2.2.2.3.1 MASS operator(s) fail to muster on bridge --> 2.2.2.3 MASS operator fail to take corrective action/ maintains collision course *AND* --> 2.2.2.2 MASS system fails to enter MRC when exceeding navigational capabilities *(*independently from operator*)* *AND* --> 2.2.2.1 MASS system fails to regain normal operational state *(*due to limitations in navigational capability*)* ---> 2.2.2 MASS fails to perform «last minute» collision avoidance manoeuvring *AND* ---> 2.2.1 MASS commits «last minute» manoeuvring error *(*responsible for collision*)* ----> 2.2 MASS fails to perform «last minute» collision avoidance manoeuvring -----> 2.0 Two or more vessels involved fails to perform collision avoidance manoeuvring *AND* -----> 1.0 Navigation error by vessels involved causes limited room for manoeuvrability ------> 0.0 Collision between MASS and other vessel*(s)*	**RCM-22**	Ensure availability of MASS operator to supervise and (if necessary) control MASS operations.	Same as: - RCM-11 a) b) and d) - RCM-10 d)

	Fault tree analysis			Risk control measures		
FTA ID	Event description	Causes	Accident scenario/ sequence of events	RCM ID	Topics	RCM descriptions
2.2.2.3.1.2.1	MASS operator(s) not informed event.	i. MASS operator 1 does not observe alarm on portable device (does not carry alarm, noisy environments, technical failure etc.) AND; ii. MASS operator 2 being unavailable (multiple causes e.g. asleep, sick)	-> 2.2.2.3.1.2 MASS operator unintentionally does not muster on bridge --> 2.2.2.3.1 MASS operator(s) fail to muster on bridge ---> 2.2.2.3 MASS operator fail to take corrective action/ maintains collision course *AND* ---> 2.2.2.2 MASS system fails to enter MRC when exceeding navigational capabilities *(*independently from operator*)* *AND* ---> 2.2.2.1 MASS system fails to regain normal operational state *(*due to limitations in navigational capability*)* ----> 2.2.2 MASS fails to perform «last minute» collision avoidance manoeuvring *AND* ----> 2.2.1 MASS commits «last minute» manoeuvring error *(*responsible for collision*)* -----> 2.2 MASS fails to perform «last minute» collision avoidance manoeuvring ------> 2.0 Two or more vessels involved fails to perform collision avoidance manoeuvring *AND* ------> 1.0 Navigation error by vessels involved causes limited room for manoeuvrability -------> 0.0 Collision between MASS and other vessel*(s)*	**RCM-23**	Ensure that MASS operators are informed about unsuccessful navigation.	Same as: - RCM-12 a) b) and c)

	Fault tree analysis			Risk control measures		
FTA ID	Event description	Causes	Accident scenario/ sequence of events	RCM ID	Topics	RCM descriptions
2.2.2.3.1.2.2	MASS operator(s) are informed about event but prevented from mustering on bridge.	i. MASS operator 1 is located too far away from bridge (unclear routines, poor handover etc.) AND; ii. MASS operator 2 being unavailable (multiple causes e.g. asleep, sick)	-> 2.2.2.3.1.2 MASS operator unintentionally does not muster on bridge --> 2.2.2.3.1 MASS operator(s) fail to muster on bridge ---> 2.2.2.3 MASS operator fail to take corrective action/ maintains collision course *AND* ---> 2.2.2.2 MASS system fails to enter MRC when exceeding navigational capabilities *(*independently from operator*)* *AND* ---> 2.2.2.1 MASS system fails to regain normal operational state *(*due to limitations in navigational capability*)* ----> 2.2.2 MASS fails to perform «last minute» collision avoidance manoeuvring *AND* ----> 2.2.1 MASS commits «last minute» manoeuvring error *(*responsible for collision*)* -----> 2.2 MASS fails to perform «last minute» collision avoidance manoeuvring ------> 2.0 Two or more vessels involved fails to perform collision avoidance manoeuvring *AND* ------> 1.0 Navigation error by vessels involved causes limited room for manoeuvrability -------> 0.0 Collision between MASS and other vessel*(s)*	**RCM-24**	Ensure that MASS operators are made available to muster to the bridge in due time.	Same as: - RCM-11 a) - RCM-12 b) and c) - RCM 13 a).

	Fault tree analysis			Risk control measures		
FTA ID	Event description	Causes	Accident scenario/ sequence of events	RCM ID	Topics	RCM descriptions
2.2.2.3.2	MASS operator musters on bridge but fails to successfully intervene.	i. Skill degradation/ insufficient manoeuvring skills e.g. caused by; - inadequate training - limited experience due to automation/ rare scenario. ii. Decision-making impacted by stressful situation/ limited time available. iii. MASS operator trusts automation over own skill set (over-reliance). iv. Navigational equipment (incl. information displays) not suitable for task; - complex to use - information unavailable, e.g. requires time consuming navigation between images on HMI displays	-> 2.2.2.3 MASS operator fail to take corrective action/ maintains collision course *AND* -> 2.2.2.2 MASS system fails to enter MRC when exceeding navigational capabilities (independently from operator) *AND* -> 2.2.2.1 MASS system fails to regain normal operational state (due to limitations in navigational capability) --> 2.2.2 MASS fails to perform «last minute» collision avoidance manoeuvring *AND* --> 2.2.1 MASS commits «last minute» manoeuvring error (responsible for collision) ---> 2.2 MASS fails to perform «last minute» collision avoidance manoeuvring ----> 2.0 Two or more vessels involved fails to perform collision avoidance manoeuvring *AND* ----> 1.0 Navigation error by vessels involved causes limited room for manoeuvrability -----> 0.0 Collision between MASS and other vessel(s)	**RCM-25**	Provide the MASS operators with sufficient competence in how to communicate with other vessels, incl. use of equipment.	Same as: - RCM-12 c) - and in addition; a) Use of Bridge Resource Management (BRM) simulator training combined with routines to perform navigational and manoeuvring tasks manually at a regular basis during normal operations. b) Ensure high degree of usability on navigational control panels and associated human-machine interfaces (see standards such as ISO 11064, ISO 9241-110 and ISO 9241-210).
0.0	**TOP event: Loss of stability/ buoyancy**					
1.1.1	MASS system performs incorrect pre-departure stability calculation	i. MASS system does not register correct weight of cargo. Ii. Wrong input to stability calculation iii. System does not detect deviation between calculated and actual loading condition	-> 1.1 Incorrect pre-departure stability condition --> 1.0 Stability failure *AND* --> 2.0 Water ingress *AND* --> 3.0 MASS and operator jointly takes incorrect damage stability contingency	**RCM-26**	Ensure correct stability calculation by cross-checking data.	a) The MASS (automation) system should be able to crosscheck weights on loading manifest. b) MASS system should be able to crosscheck loading condition, e.g. by checking against draft marks. c) Sub-systems should report status to a master-system which keeps track of the aggregated state of the vessel (including all relevant sub-systems) and initiates transition

	Fault tree analysis			Risk control measures		
FTA ID	Event description	Causes	Accident scenario/ sequence of events	RCM ID	Topics	RCM descriptions
			---> 0.0 Loss of stability/ buoyancy during voyage			to a minimum risk condition (MRC) when needed.
1.1.2.1	MASS system fails to inform operator about stability calculation failure	i. MASS operator 1 does not observe alarm on portable device (does not carry alarm, noisy environments, technical failure etc.) AND; ii. MASS operator 2 being unavailable (multiple causes e.g. asleep, sick)	-> 1.1.2 Stability calculation failure not corrected --> 1.1 Incorrect pre-departure stability condition ---> 1.0 Stability failure *AND* ---> 2.0 Water ingress *AND* ---> 3.0 MASS and operator jointly takes incorrect damage stability contingency ----> 0.0 Loss of stability/ buoyancy during voyage	**RCM-27**	Ensure that MASS operators are informed about stability calculation failures.	Same as: - RCM-12 a) b) and c)

	Fault tree analysis			Risk control measures		
FTA ID	Event description	Causes	Accident scenario/ sequence of events	RCM ID	Topics	RCM descriptions
1.1.2.2	MASS operator fails to correct stability calculation failure	i. Skill degradation/ insufficient stability calculation knowledge/ proficiency e.g. caused by; - inadequate training - limited experience/ task unfamiliarity due to automation ii. High workload/ reduced manning iii. Presence of other tasks competing for prioritization/ commercial pressures to leave port iv. Alarm criticality not clearly communicated/ poorly designed alarm system v. Loading computer equipment (incl. information displays) not suitable for task; - complex to use - information unavailable, e.g. requires time consuming navigation between images on HMI displays	-> 1.1.2 Stability calculation failure not corrected --> 1.1 Incorrect pre-departure stability condition ---> 1.0 Stability failure *AND* ---> 2.0 Water ingress *AND* ---> 3.0 MASS and operator jointly takes incorrect damage stability contingency ----> 0.0 Loss of stability/ buoyancy during voyage	RCM-28	Ensure that MASS operator can correct stability failure.	a) MASS operator to perform automated functions manually at regular intervals to ensure task and system familiarity. Support with checklists and procedures. b) Ensure that routines/ shift schedules are optimized to reduce workload so that all necessary system checks can be performed in a reliable manner. c) Ensure that alarms are categorized and prioritized to avoid alarm flood, and that alarm presentation (text, sequence and availability) is based on the criticality of individual and combined alarms. d) Ensure high degree of usability on navigational control panels and associated human-machine interfaces (see standards such as ISO 11064, ISO 9241-110 and ISO 9241-210).
1.2.1	MASS system performs incorrect transfer of internal liquid loads	i. Sensor failure/ error resulting in incorrect ballast transfer (e.g. sensor showing incorrect heel angle). Ii. Wrong input to stability calculation	-> 1.2 Incorrect transfer of internal liquid loads during voyage (e.g ballast water, fuel, fresh water etc.) --> 1.0 Stability failure *AND* --> 2.0 Water ingress *AND* --> 3.0 MASS and operator jointly takes incorrect damage stability contingency ---> 0.0 Loss of stability/ buoyancy during voyage	RCM-29	Ensure correct transfer of internal liquid load.	Same as: - RCM-26 c) - and in addition; a) The MASS system should include self-check and diagnostics functions able to detect failures in e.g. sensors. b) The MASS system should inform the operator about the intensions/ expected result of an operation before the operation is commenced. c) The MASS system should provide the operator with enough information to enable the operator to validate the correctness of the operation in question.

	Fault tree analysis			Risk control measures		
FTA ID	**Event description**	**Causes**	**Accident scenario/ sequence of events**	**RCM ID**	**Topics**	**RCM descriptions**
1.2.2.1	MASS system fails to inform operator about liquid load transfer failure	i. MASS operator 1 does not observe alarm on portable device (does not carry alarm, noisy environments, technical failure etc.) AND; ii. MASS operator 2 being unavailable (multiple causes e.g. asleep, sick)	-> 1.2.2 Liquid load transfer failure not corrected --> 1.2 Incorrect transfer of internal liquid loads during voyage (e.g. ballast water, fuel, fresh water etc.) ---> 1.0 Stability failure AND ---> 2.0 Water ingress AND ---> 3.0 MASS and operator jointly takes incorrect damage stability contingency ----> 0.0 Loss of stability/ buoyancy during voyage	**RCM-30**	Ensure that MASS operators are informed about liquid load transfer failure.	Same as: - RCM-12 a) b) and c) - and in addition; a) The MASS system should always have the possibility to enter at least one pre-defined minimum risk condition (MRC) when required operator-input is not received.
1.2.2.2	MASS operator fails to correct liquid load transfer failure	i. Skill degradation/ insufficient stability calculation knowledge/ proficiency e.g. caused by; - inadequate training - limited experience/ task unfamiliarity due to automation ii. High workload/ reduced manning iii. Presence of other tasks competing for prioritization/ commercial pressures to leave port iv. Alarm criticality not clearly communicated/ poorly designed alarm system vi. Integrated Automation System (IAS) /ballast transfer system (incl. information displays) not suitable for task; - complex to use - information unavailable, e.g. requires time consuming	-> 1.2.2 Liquid load transfer failure not corrected --> 1.2 Incorrect transfer of internal liquid loads during voyage (e.g ballast water, fuel, fresh water etc.) ---> 1.0 Stability failure *AND* ---> 2.0 Water ingress *AND* ---> 3.0 MASS and operator jointly takes incorrect damage stability contingency ----> 0.0 Loss of stability/ buoyancy during voyage	**RCM-31**	Ensure that MASS operator is able to correct liquid load transfer failure.	Same as: - RCM-28 a) to d)

	Fault tree analysis			Risk control measures		
FTA ID	Event description	Causes	Accident scenario/ sequence of events	RCM ID	Topics	RCM descriptions
		navigation between images on HMI displays				
1.3.1	MASS system fails to secure cargo	i. Cargo securing system not suitable for cargo type. ii: Unable to secure cargo due to cargo irregularity (e.g. not expected type, shape, weight) iii. Cargo securing equipment failure	*AND* -> 1.3.2 Cargo securing failure not corrected *AND* -> 1.3.3 Excessive movement of vessel (wind, heave etc.). ->1.3 Cargo shifts during voyage (depends on ship type) --> 1.0 Stability failure *AND* --> 2.0 Water ingress *AND* --> 3.0 MASS and operator jointly takes incorrect damage stability contingency ---> 0.0 Loss of stability/ buoyancy during voyage	**RCM-32**	Secure cargo sufficiently prior to departure.	Same as: - RCM-26 c) - RCM-29 a) to c) - and in addition; a) Ensure that the MASS always has a cargo securing system which is compatible with the actual cargo being loaded.
1.3.2.1	MASS system fails to inform operator about cargo securing failure	i. MASS operator 1 does not observe alarm on portable device (does not carry alarm, noisy environments, technical failure etc.) AND; ii. MASS operator 2 being unavailable (multiple causes e.g. asleep, sick)	-> 1.3.2 Cargo securing failure not corrected *AND* -> 1.3.1 MASS system fails to secure cargo *AND* -> 1.3.3 Excessive movement of vessel (wind, heave etc.). ->1.3 Cargo shifts during voyage (depends on ship type) --> 1.0 Stability failure *AND* --> 2.0 Water ingress *AND* --> 3.0 MASS and operator jointly takes incorrect damage stability contingency ---> 0.0 Loss of stability/ buoyancy during voyage	**RCM-33**	Ensure that MASS operators are informed about cargo securing failure.	Same as: - RCM-12 a) b) and c)

	Fault tree analysis			Risk control measures		
FTA ID	Event description	Causes	Accident scenario/ sequence of events	RCM ID	Topics	RCM descriptions
1.3.2.2	MASS operator fails to secure cargo	i. Skill degradation/ insufficient stability calculation knowledge/ proficiency e.g. caused by; - inadequate training - limited experience/ task unfamiliarity due to automation ii. High workload/ reduced manning iii. Presence of other tasks competing for prioritization/ commercial pressures to leave port iv. Alarm criticality not clearly communicated/ poorly designed alarm system vi. Cargo securing system (incl. information displays) not suitable for task; - complex to use - information unavailable, e.g. requires time consuming navigation between images on HMI displays	-> 1.3.2 Cargo securing failure not corrected *AND* -> 1.3.1 MASS system fails to secure cargo *AND* -> 1.3.3 Excessive movement of vessel (wind, heave etc.). ->1.3 Cargo shifts during voyage (depends on ship type) --> 1.0 Stability failure *AND* --> 2.0 Water ingress *AND* --> 3.0 MASS and operator jointly takes incorrect damage stability contingency ---> 0.0 Loss of stability/ buoyancy during voyage	**RCM-34**	Ensure that MASS operator is able to correct cargo securing failure.	Same as: - RCM 28 a) to d)
1.3.3	Excessive movement of vessel	i. vessel exposed to wind, heave etc. due to incorrect voyage planning, weather routing etc.	*AND* -> 1.3.2 Cargo securing failure not corrected *AND* -> 1.3.3 Excessive movement of vessel (wind, heave etc.). ->1.3 Cargo shifts during voyage (depends on ship type) --> 1.0 Stability failure *AND* --> 2.0 Water ingress *AND* --> 3.0 MASS and operator jointly takes	**RCM-35**	MASS system to avoid heavy weather areas.	a) The MASS system should diagnose and compare forecasted weather from different MET data sources. b) The MASS system should retrieve and consider all applicable route and reporting information (ships routing). c) The MASS system should be able to retrieve and evaluate all info for the route in ENC, such as IHO and IALA info. d) The MASS operator should be obligated to review and approve the voyage plan prior to departure. e) The MASS system should provide the MASS operator with input on what considerations it

	Fault tree analysis			Risk control measures		
FTA ID	Event description	Causes	Accident scenario/ sequence of events	RCM ID	Topics	RCM descriptions
			incorrect damage stability contingency ---> 0.0 Loss of stability/ buoyancy during voyage			has based its choice on. f) The MASS system to be able to detect local NAV conditions when planning the voyage. g) The MASS system should be able to detect deviations between actual and forecasted weather conditions. h) The MASS system's parameters for heavy weather damage should always be prioritized over voyage optimization.
2.1.1.1.1	MASS fails to sufficiently secure cargo hatch	i. Malfunction of cargo hatch securing system ii. Not able to secure cargo hatch due to physical blockage. Iii. Not able to detect unsecured cargo hatch due to sensor error/failure	*AND* -> 2.1.1.1.2 Unsecured cargo hatch not corrected --> 2.1.1.1 Unsecured cargo hatch --->2.1.1 Loss of watertight integrity of cargo hatch ---->2.1 Loss of watertight integrity *AND* ----> 2.2 Green seas on deck -----> 2.0 Water ingress *AND* -----> 1.0 Stability failure *AND* -----> 3.0 MASS and operator jointly takes incorrect damage stability contingency ------> 0.0 Loss of stability/ buoyancy during voyage	**RCM-36**	Ensure reliable securing of cargo hatches.	Same as: - RCM-29 a) and c) - RCM-26 c)

	Fault tree analysis			Risk control measures		
FTA ID	**Event description**	**Causes**	**Accident scenario/ sequence of events**	**RCM ID**	**Topics**	**RCM descriptions**
2.1.1.1.2.1	MASS fails to inform operator about unsecured cargo hatch	i. MASS operator 1 does not observe alarm on portable device (does not carry alarm, noisy environments, technical failure etc.) AND; ii. MASS operator 2 being unavailable (multiple causes e.g. asleep, sick)	-> 2.1.1.1.1 MASS fails to sufficiently secure cargo hatch *AND* -> 2.1.1.1.2 Unsecured cargo hatch not corrected --> 2.1.1.1 Unsecured cargo hatch --->2.1.1 Loss of watertight integrity of cargo hatch ---->2.1 Loss of watertight integrity *AND* ----> 2.2 Green seas on deck -----> 2.0 Water ingress *AND* -----> 1.0 Stability failure *AND* -----> 3.0 MASS and operator jointly takes incorrect damage stability contingency ------> 0.0 Loss of stability/ buoyancy during voyage	**RCM-37**	Ensure that MASS operators are informed.	Same as: - RCM-12 a) b) and c)
2.1.1.1.2.2	Operator fails to secure cargo hatch	i. Skill degradation/ insufficient stability calculation knowledge/ proficiency e.g. caused by; - inadequate training - limited experience/ task unfamiliarity due to automation ii. High workload/ reduced manning iii. Presence of other tasks competing for prioritization/ commercial pressures to leave port iv. Alarm criticality not clearly communicated/ poorly designed alarm system vi. Cargo hatch securing system (incl. information displays) not suitable for task;	-> 2.1.1.1.1 MASS fails to sufficiently secure cargo hatch *AND* -> 2.1.1.1.2 Unsecured cargo hatch not corrected --> 2.1.1.1 Unsecured cargo hatch --->2.1.1 Loss of watertight integrity of cargo hatch ---->2.1 Loss of watertight integrity *AND* ----> 2.2 Green seas on deck -----> 2.0 Water ingress *AND* -----> 1.0 Stability failure *AND* -----> 3.0 MASS and operator jointly takes incorrect damage stability contingency ------> 0.0 Loss of stability/ buoyancy during voyage	**RCM-38**	Ensure that MASS operator is able to correct cargo hatch securing failure.	Same as: - RCM-28 a) to d)

	Fault tree analysis			Risk control measures		
FTA ID	Event description	Causes	Accident scenario/ sequence of events	RCM ID	Topics	RCM descriptions
		- complex to use - information unavailable, e.g. requires time consuming navigation between images on HMI displays				
2.1.1.2.1.1.1	MASS system fails to sea-fasten loose object	i. Loose objects left unsecured during port stay, e.g. by third party ii. Loose objects not detected iii. Loose objects not properly secured due to securing equipment/system capability	*AND* -> 2.1.1.2.1.1.2 Unsecured loose object not corrected --> 2.1.1.2.1.1 Cargo hatch damaged from objects with insufficient sea fastening ---> 2.1.1.2.1 Cargo hatch damaged By external force *AND* ---> 2.1.1.2.2 Damaged cargo hatch not corrected ----> 2.1.1.2 Damaged cargo hatch ----->2.1.1 Loss of watertight integrity of cargo hatch ------>2.1 Loss of watertight integrity *AND* ------> 2.2 Green seas on deck -------> 2.0 Water ingress *AND* -------> 1.0 Stability failure *AND* -------> 3.0 MASS and operator jointly takes incorrect damage stability contingency --------> 0.0 Loss of stability/ buoyancy during voyage	**RCM-39**	Ensure that all loose objects are secured before departure.	Same as: - RCM-26 c) - and in addition; a) All personnel to be aware of the importance of securing all equipment and loose objects when working on MASS (incl. third party personnel providing service during port stay) b) MASS system to be able to monitor, detect and inspect potential loose objects. c) MASS system to be able to secure or remove loose objects. d) Human operator to be alerted if a potential loose object is left unsecured.

	Fault tree analysis			Risk control measures		
FTA ID	Event description	Causes	Accident scenario/ sequence of events	RCM ID	Topics	RCM descriptions
2.1.1.2.1.1.2.1	MASS fails to inform operator about unsecured object	i. MASS operator 1 does not observe alarm on portable device (does not carry alarm, noisy environments, technical failure etc.) AND; ii. MASS operator 2 being unavailable (multiple causes e.g. asleep, sick)	-> 2.1.1.2.1.1.2 Unsecured loose object not corrected *AND* -> 2.1.1.2.1.1.1 MASS system fails to sea fasten loose object --> 2.1.1.2.1.1 Cargo hatch damaged from objects with insufficient sea fastening ---> 2.1.1.2.1 Cargo hatch damaged By external force *AND* ---> 2.1.1.2.2 Damaged cargo hatch not corrected ----> 2.1.1.2 Damaged cargo hatch ----->2.1.1 Loss of watertight integrity of cargo hatch ------>2.1 Loss of watertight integrity *AND* ------> 2.2 Green seas on deck -------> 2.0 Water ingress *AND* -------> 1.0 Stability failure *AND* -------> 3.0 MASS and operator jointly takes incorrect damage stability contingency --------> 0.0 Loss of stability/ buoyancy during voyage	**RCM-40**	Ensure that MASS operators are informed.	Same as: - RCM-12 a) b) and c)

	Fault tree analysis			Risk control measures		
FTA ID	Event description	Causes	Accident scenario/ sequence of events	RCM ID	Topics	RCM descriptions
2.1.1.2.1.1.2.2	Operator fails to secure loose object.	i. Skill degradation/ insufficient stability calculation knowledge/proficiency e.g. caused by; - inadequate training - limited experience/ task unfamiliarity due to automation ii. High workload/ reduced manning iii. Presence of other tasks competing for prioritization/ commercial pressures to leave port iv. Alarm criticality not clearly communicated/ poorly designed alarm system v. loose object securing equipment / system (incl. information displays) not suitable for task; - complex to use - information unavailable, e.g. requires time consuming navigation between images on HMI displays	-> 2.1.1.2.1.1.2 Unsecured loose object not corrected *AND* -> 2.1.1.2.1.1.1 MASS system fails to sea fasten loose object --> 2.1.1.2.1.1 Cargo hatch damaged from objects with insufficient sea fastening ---> 2.1.1.2.1 Cargo hatch damaged By external force *AND* ---> 2.1.1.2.2 Damaged cargo hatch not corrected ----> 2.1.1.2 Damaged cargo hatch ----->2.1.1 Loss of watertight integrity of cargo hatch ------>2.1 Loss of watertight integrity *AND* ------> 2.2 Green seas on deck -------> 2.0 Water ingress *AND* -------> 1.0 Stability failure *AND* -------> 3.0 MASS and operator jointly takes incorrect damage stability contingency --------> 0.0 Loss of stability/ buoyancy during voyage	**RCM-41**	Ensure that MASS operator is able to secure loose object.	Same as: - RCM-28 a) to d)
2.1.1.2.1.2	Cargo hatch damaged directly from wave impact	i. High seas/ swells	-> 2.1.1.2.1 Cargo hatch damaged by external force *AND* -> 2.1.1.2.2 Damaged cargo hatch not corrected --> 2.1.1.2 Damaged cargo hatch --->2.1.1 Loss of watertight integrity of cargo hatch ---->2.1 Loss of watertight integrity *AND* ----> 2.2 Green seas on deck -----> 2.0 Water ingress	**RCM-42**	No RCMs identified (similar to conventional shipping).	No RCMs identified (similar to conventional shipping).

	Fault tree analysis			Risk control measures		
FTA ID	Event description	Causes	Accident scenario/ sequence of events	RCM ID	Topics	RCM descriptions
			AND -----> 1.0 Stability failure *AND* -----> 3.0 MASS and operator jointly takes incorrect damage stability contingency ------> 0.0 Loss of stability/ buoyancy during voyage			
2.1.1.2.2.1	MASS fails to inform operator about damaged cargo hatch	i. MASS operator 1 does not observe alarm on portable device (does not carry alarm, noisy environments, technical failure etc.) AND; ii. MASS operator 2 being unavailable (multiple causes e.g. asleep, sick)	-> 2.1.1.2.2 Damaged cargo hatch not corrected *AND* -> 2.1.1.2.1 Cargo hatch damaged by external force --> 2.1.1.2 Damaged cargo hatch --->2.1.1 Loss of watertight integrity of cargo hatch ---->2.1 Loss of watertight integrity *AND* ----> 2.2 Green seas on deck -----> 2.0 Water ingress *AND* -----> 1.0 Stability failure *AND* -----> 3.0 MASS and operator jointly takes incorrect damage stability contingency ------> 0.0 Loss of stability/ buoyancy during voyage	**RCM-43**	Ensure that MASS operators are informed.	Same as: - RCM-12 a) b) and c)

	Fault tree analysis			Risk control measures		
FTA ID	Event description	Causes	Accident scenario/ sequence of events	RCM ID	Topics	RCM descriptions
2.1.1.2.2.2	Operator fails to correct damaged cargo hatch	i. Skill degradation/ insufficient stability calculation knowledge/proficiency e.g. caused by; - inadequate training - limited experience/ task unfamiliarity due to automation ii. High workload/ reduced manning iii. Presence of other tasks competing for prioritization/ commercial pressures to leave port iv. Alarm criticality not clearly communicated/ poorly designed alarm system v. system for correcting damaged cargo hatch (incl. information displays) not suitable for task; - complex to use - information unavailable, e.g. requires time consuming navigation between images on HMI displays	-> 2.1.1.2.2 Damaged cargo hatch not corrected *AND* -> 2.1.1.2.1 Cargo hatch damaged by external force --> 2.1.1.2 Damaged cargo hatch --->2.1.1 Loss of watertight integrity of cargo hatch ---->2.1 Loss of watertight integrity *AND* ----> 2.2 Green seas on deck -----> 2.0 Water ingress *AND* -----> 1.0 Stability failure *AND* -----> 3.0 MASS and operator jointly takes incorrect damage stability contingency ------> 0.0 Loss of stability/ buoyancy during voyage	**RCM-44**	Ensure that MASS operator is able to correct damaged cargo hatch.	Same as: - RCM-28 a) to d)
2.2.1.1	MASS system performs incorrect voyage planning	i. System does not consider correct forecasted weather data for the planed route ii. System does not consider traffic systems and reporting regulations in voyage plan iii. 'System does not detect and evaluate chart nav hazards for the voyage	-> 2.2.1 Green seas on deck due to Incorrect voyage planning --> 2.2 Green seas on deck *AND* -->2.1 Loss of watertight integrity ---> 2.0 Water ingress *AND* ---> 1.0 Stability failure *AND* ---> 3.0 MASS and operator jointly takes incorrect damage stability contingency	**RCM-45**	Ensure that relevant data is used and compared during voyage planning.	Same as: - RCM-26 c) - RCM-35 a) to h)

	Fault tree analysis			Risk control measures		
FTA ID	Event description	Causes	Accident scenario/ sequence of events	RCM ID	Topics	RCM descriptions
			----> 0.0 Loss of stability/ buoyancy during voyage			
2.2.1.2.1	MASS system fails to inform operator about incorrect voyage plan	i. MASS operator 1 does not observe alarm on portable device (does not carry alarm, noisy environments, technical failure etc.) AND; ii. MASS operator 2 being unavailable (multiple causes e.g. asleep, sick)	-> 2.2.1.2 Voyage plan failure not corrected *AND* -> 2.2.1.1 MASS system performs Incorrect voyage planning --> 2.2.1 Green seas on deck due to Incorrect voyage planning ---> 2.2 Green seas on deck *AND* --->2.1 Loss of watertight integrity ----> 2.0 Water ingress *AND* ----> 1.0 Stability failure *AND* ----> 3.0 MASS and operator jointly takes incorrect damage stability contingency -----> 0.0 Loss of stability/ buoyancy during voyage	**RCM-46**	Ensure that MASS operators are informed.	Same as: - RCM-12 a) b) and c)

	Fault tree analysis			Risk control measures		
FTA ID	Event description	Causes	Accident scenario/ sequence of events	RCM ID	Topics	RCM descriptions
2.2.1.2.2	MASS operator fails to correct voyage plan	i. Skill degradation/ insufficient stability calculation knowledge/proficiency e.g. caused by; - inadequate training - limited experience/ task unfamiliarity due to automation ii. High workload/ reduced manning iii. Presence of other tasks competing for prioritization/ commercial pressures to leave port iv. Alarm criticality not clearly communicated/ poorly designed alarm system V. voyage planning system (incl. information displays) not suitable for task; - complex to use - information unavailable, e.g. requires time consuming navigation between images on HMI displays	-> 2.2.1.2 Voyage plan failure not corrected *AND* -> 2.2.1.1 MASS system performs Incorrect voyage planning --> 2.2.1 Green seas on deck due to Incorrect voyage planning ---> 2.2 Green seas on deck *AND* --->2.1 Loss of watertight integrity ----> 2.0 Water ingress *AND* ----> 1.0 Stability failure *AND* ----> 3.0 MASS and operator jointly takes incorrect damage stability contingency -----> 0.0 Loss of stability/ buoyancy during voyage	**RCM-47**	Ensure that MASS operator is able to correct voyage plan.	Same as: - RCM-28 a) to d)
2.2.2.1	MASS system performs incorrect weather routing / voyage optimization during transit	i. 'System does not detect and evaluates local nav hazards ii. System does not recognize the deviation between actual and forecasted weather condition iii. MASS system parameters weight voyage optimization over risk for heavy weather damage	-> 2.2.2 Green seas on deck due to route adjustments during transit --> 2.2 Green seas on deck *AND* -->2.1 Loss of watertight integrity ---> 2.0 Water ingress *AND* ---> 1.0 Stability failure *AND* ---> 3.0 MASS and operator jointly takes incorrect damage stability contingency ----> 0.0 Loss of stability/ buoyancy during voyage	**RCM-48**	MASS system to avoid heavy weather damage.	Same as: - RCM-26 c) - RCM-35 a) to h)

	Fault tree analysis			Risk control measures		
FTA ID	Event description	Causes	Accident scenario/ sequence of events	RCM ID	Topics	RCM descriptions
2.2.2.2.1	MASS System fails to inform operator about Incorrect weather routing / voyage optimization	i. MASS operator 1 does not observe alarm on portable device (does not carry alarm, noisy environments, technical failure etc.) AND; ii. MASS operator 2 being unavailable (multiple causes e.g. asleep, sick)	-> 2.2.2.2 Weather routing / voyage optimization failure not corrected *AND* -> 2.2.2.1 MASS system performs Incorrect weather routing / voyage optimization during transit --> 2.2.2 Green seas on deck due to route adjustments during transit ---> 2.2 Green seas on deck *AND* --->2.1 Loss of watertight integrity ----> 2.0 Water ingress *AND* ----> 1.0 Stability failure *AND* ----> 3.0 MASS and operator jointly takes incorrect damage stability contingency -----> 0.0 Loss of stability/ buoyancy during voyage	**RCM-49**	Ensure that MASS operators are informed.	Same as: - RCM-12 a) b) and c)

	Fault tree analysis			Risk control measures		
FTA ID	Event description	Causes	Accident scenario/ sequence of events	RCM ID	Topics	RCM descriptions
2.2.2.2.2	MASS operator fails to correct weather routing / voyage optimization failure	i. Skill degradation/ insufficient stability calculation knowledge/proficiency e.g. caused by; - inadequate training - limited experience/ task unfamiliarity due to automation ii. High workload/ reduced manning iii. Presence of other tasks competing for prioritization/ commercial pressures to leave port iv. Alarm criticality not clearly communicated/ poorly designed alarm system V. Weather routing / voyage optimization equipment/system (incl. information displays) not suitable for task; - complex to use - information unavailable, e.g. requires time consuming navigation between images on HMI displays	-> 2.2.2.2 Weather routing / voyage optimization failure not corrected *AND* -> 2.2.2.1 MASS system performs Incorrect weather routing / voyage optimization during transit --> 2.2.2 Green seas on deck due to route adjustments during transit ---> 2.2 Green seas on deck *AND* --->2.1 Loss of watertight integrity ----> 2.0 Water ingress *AND* ----> 1.0 Stability failure *AND* ----> 3.0 MASS and operator jointly takes incorrect damage stability contingency -----> 0.0 Loss of stability/ buoyancy during voyage	**RCM-50**	Ensure that MASS operator is able to correct weather routing / voyage optimization failure.	Same as: - RCM-28 a) to d)
3.0	MASS and operator jointly take incorrect damage stability contingency	Undeveloped event.	*AND* -> 1.0 Stability failure *AND* -> 2.0 Water ingress --> 0.0 Loss of stability/ buoyancy during voyage	**RCM-51**	--	--

THIS PAGE IS INTENTIONALLY LEFT BLANK

About DNV GL

DNV GL is a global quality assurance and risk management company. Driven by our purpose of safeguarding life, property and the environment, we enable our customers to advance the safety and sustainability of their business. We provide classification, technical assurance, software and independent expert advisory services to the maritime, oil & gas, power and renewables industries. We also provide certification, supply chain and data management services to customers across a wide range of industries. Operating in more than 100 countries, our experts are dedicated to helping customers make the world safer, smarter and greener.