

DNV·GL

SAFEMASS

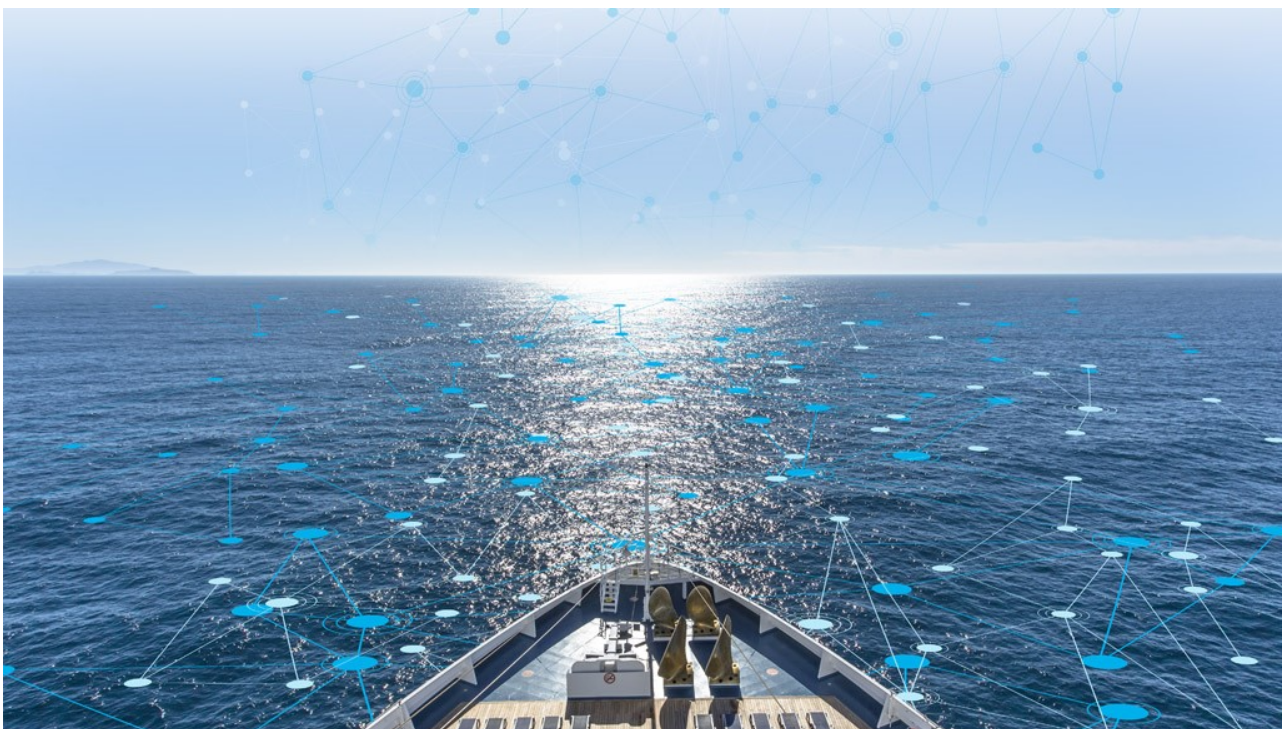
Study of the risks and regulatory issues of specific cases of MASS – Part 2

European Maritime Safety Agency (EMSA)

Report No.: 2019-0805, Rev. 0

Document No.: 11FSQ7AF-2

Date: 2020-03-25



Project name: SAFEMASS
Report title: Study of the risks and regulatory issues of specific cases of MASS – Part 2
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.: 10158635
Organisation unit: Safety, Risk & Reliability
Report No.: 2019-0805, Rev. 0
Document No.: 11FSQ7AF-2
Applicable contract(s) governing the provision of this Report: Contract Number 2019/EMSA/OP/4/2019

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 2 (out of 2) addresses the emerging risk associated with three similar unmanned vessels being designed and remotely operated according to the A2-B0 level of autonomy and control. The study includes a hazard identification (HAZID), fault tree analysis (FTA), 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:

Verified by:

Approved by:

Sondre Øie
Principal Consultant

Øystein Engelhardtzen
Senior Researcher

Peter Hoffmann
Head of Section Safety Risk & Reliability

Erlend Norstein
Consultant

Hans Jørgen Johnsrud
Senior Consultant

Copyright © DNV GL 2020. All rights reserved. Unless otherwise agreed in writing: (i) This publication or parts thereof may not be copied, reproduced or transmitted in any form, or by any means, whether digitally or otherwise; (ii) The content of this publication shall be kept confidential by the customer; (iii) No third party may rely on its contents; and (iv) DNV GL undertakes no duty of care toward any third party. Reference to part of this publication which may lead to misinterpretation is prohibited. DNV GL and the Horizon Graphic are trademarks of DNV GL AS.

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, remote control, hazard, hazard identification, HAZID, safety, risk, risk analysis, risk control options, 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	ERLOR	OYSTE	
B	2020-03-09	Final draft issued for review	SONDO	OYSTE	
0	2020-03-25	Final report	SONDO	OYSTE	PHOFF

Table of contents

EXECUTIVE SUMMARY	1
DEFINITIONS.....	6
1 PROBLEM DEFINITION	7
2 BACKGROUND INFORMATION	8
3 METHOD OF WORK	9
3.1 Meeting and work sessions	9
3.2 Expertise involved	9
3.3 Limitations	10
4 A2-B0 SHIP CONCEPT DESCRIPTIONS (TASK 2. A)	11
4.1 A2-B0 level of autonomy and control	11
4.2 Identification and breakdown of generic A2-B0 functions	15
4.3 Ship description and operational context	21
4.4 Remote Control Centre (RCC)	23
5 HAZID OF THE A2-B0 MASS CATEGORY (TASK 2. B)	26
5.1 Focus areas	26
5.2 HAZID approach	26
5.3 HAZID output	31
6 FAULT TREE ANALYSIS (TASK 2. C)	33
6.1 TOP event: MASS fails in collision avoidance	35
6.2 Emerging risks associated with collision scenario	42
7 RISK CONTROL OPTIONS (TASK 2. D)	45
7.1 RCO #1 – Ensure sufficient reliability of systems performing navigation functions	45
7.2 RCO #2 – Ensure sufficient reliability of RCC operators’ response actions to system failures	48
7.3 RCO #3 – Ensure sufficient supervision capacity and availability of RCC	50
7.4 RCO #4 – Ensure sufficient capability for MASS fleet to enter minimum risk conditions	52
8 CONCLUDING REMARKS	53
9 REFERENCES	55
APPENDIX A – SAFEMASS PARTICIPANTS (PART 2)	56
APPENDIX B – HAZID LOG	58
APPENDIX C – GUIDEWORDS	71
APPENDIX D – FTA AND RCM TABLE	73

List of figures

Figure 1 – The concept of normal operations, abnormal situations and MRCs	13
Figure 2 – The “how” and “why” logic behind function hierarchies	16
Figure 3 – Functions under analysis for A2-B0 ship.....	17
Figure 4 – Navigation & Manoeuvring.....	18
Figure 5 – Condition detection	19
Figure 6 – Condition analysis.....	19
Figure 7 – Action planning and control	20
Figure 8 – Route Gothenburg – Frederikshavn	22
Figure 9 – Traffic situation around Gothenburg	23
Figure 10 – “Control Room operator response” columns in the HAZID log sheet	27
Figure 11 – “Hazard identification” columns in the HAZID log sheet.....	27
Figure 12 – Fault tree branches for TOP event ID 0.0 (collision avoidance failure).....	35
Figure 13 – Fault tree branches for intermediate event ID 1.0.....	36
Figure 14 – Fault tree branches for intermediate event ID 2.0.....	37
Figure 15 – Fault tree branches for intermediate event ID 3.0.....	38
Figure 16 – Fault tree branches for intermediate event ID 4.0.....	39
Figure 17 – Fault tree branches for intermediate event ID 5.0.....	40
Figure 18 – Fault tree branches for intermediate event ID 5.1.1	41
Figure 19 – Fault tree branches for intermediate event ID 5.1.2	42
Figure 20 – Allocation of A2-B0 MASS navigation functions in normal operations	53
Figure 21 – Allocation of A2-B0 MASS navigation functions in case of analysis failure	53
Figure 22 – Analysis and planning functions allocated to the human operator	54



List of tables

Table 1 - MSC 100/5/6 proposal for level of autonomy and control.....	7
Table 2 - A2 and A3 level of autonomy and control as proposed in MSC 100/5/6.....	12
Table 3 - Ship dimensions	21
Table 4 - Manning of RCC.....	25
Table 5 - Functions initially selected for hazard identification	29
Table 6 - Scenarios used to aid hazard identification	29
Table 7 - Fault tree analysis symbols.....	33
Table 8 - RCMs associated with RCO #1 targeting the reliability of navigation systems.....	46
Table 9 - RCMs associated with RCO #2 targeting the reliability of RCC operators' actions	48
Table 10 - RCMs associated with RCO #3 targeting RCC supervision capacity and availability	50
Table 11 - RCMs associated with RCO # 4 targeting the MASS fleet's capability to enter MRCs	52
Table 12 - HAZID guidewords based on the SHERPA taxonomy /6/	71

EXECUTIVE SUMMARY

This report documents Part 2 of the SAFEMASS study and addresses emerging risks associated with the A2-B0 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 unmanned vessels operated with a relatively high level of automation, combined with supervision by human operators located in a Remote-Control Centre (RCC).


For Part 2 of SAFEMASS, risks emerging from the following topics were of particular interest:

- Capacities and abilities required to supervise multiple vessels in various operational modes, incl. in case of abnormal situations and emergencies.
- Human-machine interfaces (HMI) and other visual displays required for successful acquisition and analysis of information, decision-making and implementation of control actions.
- Threats to operator vigilance induced by human factors such as boredom or *underload* during quiet and normal operations, as well as stress and other negative factors present during periods with high workload.
- Influence from challenges with communication link, such as latency and connectivity.
- Operators' diminished ship sense from being remotely located (onshore), e.g. reduced or altered perceptions of stability, speed, heading and environmental conditions.
- Challenges related to not being physically present to fix problems, e.g. in case of maintenance, equipment failures or rescue operations.

As a basis for risk analysis, descriptions of a generic MASS fleet and RCC designed and operated according to the A2-B0 MASS category were developed. The concept included operation of three identical MASS performed by one bridge and one engine operator located in the RCC. A set of automated navigation functions was selected from the MASS concept description and used as study nodes in a hazard identification (HAZID) process. By combining these with tasks performed by the RCC operators to supervise or assist the MASS, 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 A2-B0 MASS concept. This resulted in a list of hazards used as a basis for constructing a fault tree analysis (FTA) model suitable for further examination of the causal relationship between events occurring in a ship collision scenario. The study identified several risks emerging from the A2-B0 MASS category's combined use of remotely controlled and unmanned operations. The main risks are summarized in the following four paragraphs.

A major concern is when navigation failures are not alerted to, or goes undetected by, the RCC operator(s). In case the MASS system is unaware of not detecting an object, it will also not issue an alarm to attract the RCC operator's attention. As such there is no guarantee that the RCC operator will detect the object because his or her attention is shared between multiple vessels (here: three). The same risk can be applied to the remainder of navigation functions (analysis, planning and action). However, while this also can be critical, because collision avoidance depends on objects being detected successfully, it can be argued that the reliability of this function is particularly important. For failures which are successfully detected by the MASS system, there is still a risk that RCC operator will fail to notice or acknowledge the alarm with the correct response. Poor alarm prioritization and categorization can cause



events to drown in alarm floods or reduce operators' vigilance due to experiencing alarm fatigue. Other influencing factors could be that the operators are occupied with tasks of higher priority, or that they are not physically present in the RCC and available to observe the alarm.

Another emerging risk is that the RCC operator's response to navigational failures is not made feasible, even when successfully alerted and detected. As with automated systems in general, being left with the task to resolve automation failures or shortcomings can represent challenging tasks for the operators. For object detection and classification, the failure may stem from limitations in the systems capabilities, or degraded systems (e.g. sensors). Being remotely located, and to a large extent relying on the same input data as the control system, the operator's chance of success is relative to the system's capabilities, or lack thereof. That is, for the operator to reliably perform object detection and classification, he or she must be presented with information they are capable of interpreting (but the system is not).

When it comes to responding to failures in analysis, planning and execution of actions, such scenarios often involve having limited time available to respond, combined with potentially little knowledge about previous occurrences ("out-of-the-loop" issues). Because the RCC operators does not have capacity to continuously monitor all the MASS, he or she then relies on the availability of information required to obtain enough situational awareness for sound decision making and safe implementation of manoeuvring actions. If not having thought through such scenarios when developing human-machine interfaces and other displays or controls, the RCC operator may struggle to override and intervene correctly. Another threat to successful operator responses is not optimizing routines for active supervision according to the parts of the voyage when the MASS is expected to require the most assistance.

The final emerging risk stems from hazards threatening the RCCs supervision capability. These can be technical failures such as loss of communication link and power outage, but also absence of operator presence due abnormal events such as acute illness. Other hazards include excessive workload or routines and procedures not supporting operator vigilance.

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 Risk Control Options (RCO) categories. 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

RCM #1 includes RCMs intended to ensure sufficient reliability of systems performing navigation functions. While having reliable systems in itself will lower the likelihood of collisions, it will also reduce the need for operator interventions, hence also limiting the opportunities for human error. Recommendations therefore include (list not exhaustive):

- Ensure reliability and redundancy by use of several and different types of object detection systems, independent of each other (redundant).
- Choose a combination of object detection systems based on careful consideration about each technology's relative capabilities, as well as how they support RCC operators' ability to assist in object detection.
- Select object detection systems which are capable of testing and confirming their functionality through self-diagnostics.

- Define criteria (to set notifications/ alarms) for when assistance from RCC operators is required to maintain normal operations.
- Use sensors and cameras designed to withstand possible impairments due to environmental conditions (snow, salt, rain etc.).
- Verify that the navigation system can comply with relevant parts of COLREG.
- Perform comprehensive testing of software to confirm reliability both as part of commissioning (e.g. hardware-in-the loop testing) as well as after updates, to verify functionality and absence of failures.

RCC #2

RCC #2 was to ensure that the RCC operators can reliably act as an additional layer of defence against collisions in cases where a MASS in automation mode performs navigation failures. This is done by allowing the RCC operators to predict and prevent navigation failures through active supervision, or by responding to (detected) system failures. To support this strategy, the following RCMs are proposed:

- Equip the RCC with a layout and human-machine interfaces which enables supervision of the entire MASS fleet, also while performing attention-demanding tasks on individual vessels.
- Design a user-friendly alarm system, incl. clear visual and audible alarm presentation, enabled by alarm categorization and prioritization.
- Provide RCC operators with sufficient training in MASS automation capabilities and limitations, including when and how to supervise operations and take manual control.

RCC #3

RCC #3 aims at ensuring that the RCC is available and has the capacity required to maintain supervision of the MASS fleet. This is a pre-requisite for both reliable system and human performance in performing navigation functions. As such, both technical and organisational RCMs were identified, with the former consisting of recommendations to:

- Ensure sufficient redundancy, reliability and availability of both the RCC/ MASS power supplies and communication link to avoid loss of MASS monitoring and control due to single failures.
- Have a backup RCC workstation in an alternative geographical location and/or a portable device available for essential control of MASS fleet, incl. the possibility to have MASS enter an MRC.

Equally important, the organisational RCMs consist of:

- Clear procedures and routines for ensuring continuous presence of operators on watch in RCC, for all operational modes, and for all parts of MASS' voyages.
- Implement strict and clear procedures for how many MASS can be operated in manual mode simultaneously, and when.
- Have an off-duty RCC operator available on-call in case of on-duty RCC operators becoming incapacitated (e.g. sick/ injured), or in case of increase in workload.

- Provide RCC operators with a minimum amount of cross-competency to handle critical tasks, such as enabling the RCC engine operator to supervise navigation of a MASS in case the RCC bridge operator is absent or occupied with other tasks.
- Design tasks and work shifts in ways which supports operator vigilance and prevents boredom.

RCO #4

A fourth RCO is to ensure that all the vessels in a MASS fleet at any given time has the opportunity to enter so called "minimum risk conditions" (MRC). An MRC is a safe (as possible) state for one or several MASS to enter in case of technical failures and/or human error prevents the vessel from maintaining normal operations. This can be a necessary measure in response to reduction or loss of RCC supervision capabilities. RCMs targeting MRCs include:

- MRCs to be defined for all critical system failures and external events which can potentially escalate to cause unacceptable impact on the MASS's or other involved vessels' safety, or to the environment, if not dealt with
- Critical events on one MASS automatically triggers the other vessels to also enter an MRC.
- MASS fleet to enter MRC in case RCC becomes unavailable, e.g. due to a blackout.
- Having an emergency stop button in the RCC which puts the entire MASS fleet into an MRC state.

The study concludes that the need for supervision is directly related to the degree of system reliability (or *unreliability*). A less reliable system requires more active supervision and frequent intervention. The demands put on RCC operator in various operational modes and scenarios must be taken into consideration when making decisions about how functions are to be allocated between the system and human operator in a best possible way. Such efforts should be made already early in the design stage when defining the MASS Concept of Operations (ConOps). This allows for developing fit-for-purpose automation, which subsequently can be optimized with additional non-technical solutions, such as those introduced via manning and organisation of work staff, procedures, routines and training.

ACRONYMS

AIS	Automatic Identification System
BAM	Bridge Alert Management
CCTV	Closed-Circuit Television
COLREG	International Regulations for Preventing Collisions at Sea
CRO	Control Room Operator
DP	Dynamic Positioning
ECDIS	Electronic Chart Display and Information System
EMSA	European Maritime Safety Agency
FSA	Formal Safety Assessment
FTA	Fault Tree Analysis
HAZID	Hazard Identification
HMI	Human Machine Interface
IAS	Integrated Automation System
IMO	International Maritime Organisation
ISM	International Safety Management
LIDAR	Light Detection and Ranging
MASS	Maritime Autonomous Surface Ships
MFD	Multi function displays
MRC	Minimum Risk Condition
NMA	Norwegian Maritime Authority
PMS	Power Management System
RCC	Remote Control Centre
RCM	Risk Control Measures
RCO	Risk Control Options
SAR	Search and Rescue
SMCP	Standard Marine Communication Phrases

DEFINITIONS

Anticipated failure	Failure expected to occur (e.g. >once a year) that should not prevent normal operation of the vessel.
A2-B0	Vessel with an A2 level of autonomy (autonomous) with no qualified operators onboard but available in a remote location.
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) A2-B0 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 A2-B0 level of autonomy and control.
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.
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.
Operator	Human operator who is located in the remote-control centre (RCC), responsible for the supervision, monitoring and control of either bridge/deck functions (Bridge Operator) or engine functions (Engine Operator). Also referred to as RCC 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.
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.

1 PROBLEM DEFINITION

Part 2 of the SAFEMASS study addresses the emerging risk associated with *autoremove* /2/ operations of multiple vessels designed according to the A2-B0 category (Table 1). While part 1 of the study described three different vessels involved in different functions, this study describes three identical vessels in relation to the navigation function.

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

Similar to part 1 of the study the need for human intervention and system redundancy is investigated. However, this study will address the human elements in an autoremove context, including issues related to latency, connectivity and human-machine interface (HMI).

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 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 /2/*. Being too futuristic can invalidate the results and create a sense of unrealism. A balance between feasibility and future opportunities has therefore been strived for when developing the study basis. The focus in this study is therefore on 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 /2/*. The guideline's overall objective is to provide a framework which ensures that application of novel concepts and technologies result in a safety level equivalent to (as good as 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 a sample ship description for the A2-B0 category, as well as recommendations for risk analysis.

3 METHOD OF WORK

The Study on the A2-B0 combination, MASS without qualified seafarers onboard being supervised by a qualified operator.

- Task 2.a: Provide a description of a generic A2-B0 ship and its enablers
- Task 2.b: Perform HAZID for the A2-B0 combination
- Task 2.c: Develop analytical fault tree models
- Task 2.d: 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 Meeting 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 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 15th and 16th of October 2019. The purpose was to identify and discuss emerging risks as a result from applying A2-B0 level of autonomy and control to the three identical vessels developed in Part 2.
- **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 A2-B0 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 today's current situation.

4 A2-B0 SHIP CONCEPT DESCRIPTIONS (TASK 2. A)

Part 2 of SAFEMASS studies emerging risks associated with operating three identical A2-B0 MASS designed and operated according to the concept description outlined in this chapter. Sub-chapter 4.1 provides an interpretation of the A2-B0 level of autonomy and control. This is further operationalized in sub-chapter 4.2 by describing the *Navigation & Manoeuvring* functions, which is also the main focus area in this study. This includes the description of a generic automation system based on principles from DNVGL-CG-0264 Autonomous and remotely operated ships /2/, but adapted to fit a A2-B0 MASS concept. Sub-chapter 4.3 includes information about the vessels' physical characteristics, capabilities and operational environment, followed by a description of the Remote-Control Centre.

4.1 A2-B0 level of autonomy and control

The definition proposed in MSC 100/5/6 (see Table 1 and Table 2) provides an overall framework and some directions about how to develop a A2-B0 MASS concept. However, for the purpose of this study, the definition requires some additional details and further maturation. To do so, the principle of "minimum risk conditions" and how they are relevant for A2-B0 MASS is first explained in sub-chapter 4.1.1. This is followed by an interpretation of the A2-B0 level of autonomy and control in sub-chapter 4.1.2. Lastly, a generic description MASS navigation functions is outlined in chapter 4.2, together with a set of assumptions considered to be applicable for this study's A2-B0 concept.

4.1.1 "Minimum risk conditions" applied to the A2-B0 MASS category

The A2-B0 MASS category is defined in Table 2. As can be read, compared to the A3-B1 ships described in Part 1 of SAFEMASS, the operator is always informed of all decisions taken by the system. Furthermore, it is stated that the qualified operator can override the system at any stage.

Table 2 – A2 and A3 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	<p style="text-align: center;">Supervised</p> <p>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.</p>	A2-B0	A2-B1
	A3	<p style="text-align: center;">Autonomous</p> <p>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".</p>	A3-B0	A3-B1

To fully grasp the concept behind the A2 level of autonomy, it is in the context of this study considered useful to have an idea of *when* it is beneficial for the operator to override the system. One way to do this is by applying the concept of *Minimum Risk Conditions* (MRC) [2].

MRC provide a framework and set of definitions for how to design and operate a MASS in case of disruptions to the normal operational state. 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.

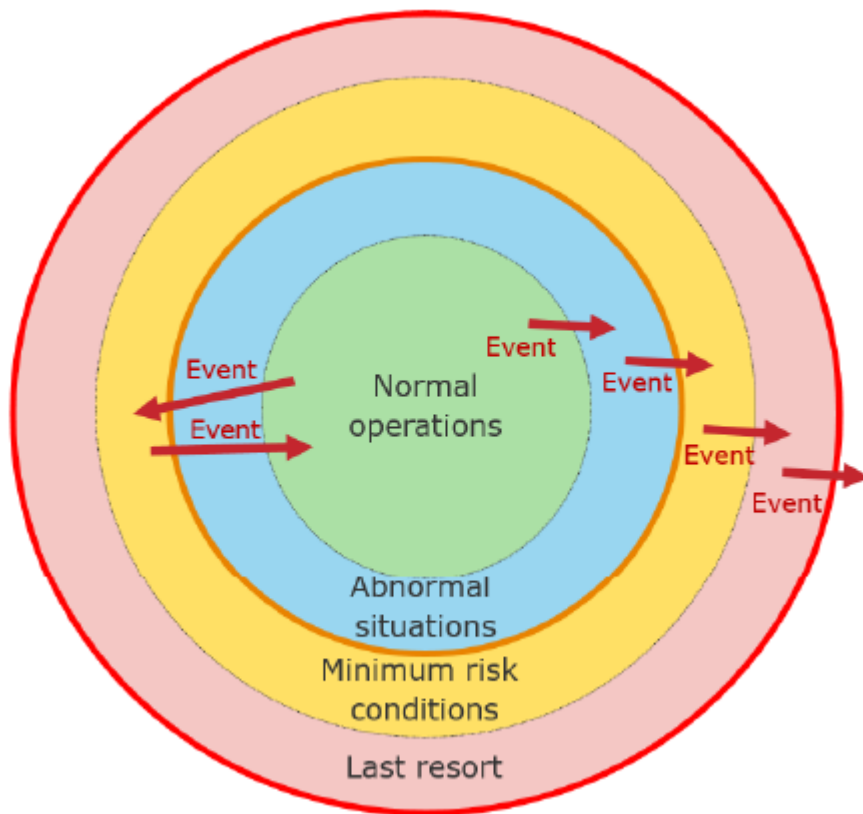


Figure 1 – The concept of normal operations, abnormal situations and MRCs

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 /2/:

- 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) /2/.
- 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 A2-B0 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* /2/.

4.1.2 Interpretation of the A2-B0 level of autonomy and control


To better understand the practical implications of applying the A2-B0 MASS category to a ship concepts, the definition was broken down and interpreted as described in the following sections.

It is assumed that the various autonomy levels can partly be interpreted based on what distinguishes them from the next level up or down. As such, the interpretation is to a large degree driven by how it compares to the A3 level studied in Part 1 of SAFEMASS.

Compared to the A3-B1 combination, a A2-B0 MASS appears to require a higher level of human involvement, specifically with regards to supervising decisions and actions taken by the MASS. The first part of the definition states that:

“The qualified operator is always informed of all decisions taken by the system [...]”.

While Part 1 of SAFEMASS assumes that the A3-B1 MASS operator is *only* informed when the MASS exceeds its operational boundaries, the A2-B0 definition indicates that the operator performs more active monitoring and supervision. However, there are two arguments for why “always” can be interpreted as the operator always having *access* to information, instead of performing constant monitoring of all vessels. First, even operators on conventional vessels are not informed of *all* actions performed by automated systems. Second, considering that



this study's concept involves supervision of three identical MASS, the remote operator will not be able to simultaneously monitor and process all decisions taken all three vessels. Consequently, the following assumptions have been made:

- As with A3-B1, the A2-B0 concept also involves pre-defining a set of parameters for what is considered *normal operations* (Figure 1) and for when the remote human operator is requested to devote attention towards a specific ship and situation.
- Only the most essential information is continuously displayed in the Remote-Control Centre (RCC). This can be information presented on a large screen display (LSD).
- The remote operator has access to and can obtain more information about the ship if he or she actively navigates through human-machine interfaces and other displays.

Next, the A2-B0 category states:

“Permission of the qualified operator is not required for the ship system to execute functions, decisions and actions; [...]”.

This part of the definition has a similar wording to that of the A3 level. Nevertheless, it is here argued that the A2 level has certain limitations compared to A3. It is assumed that an A2 MASS is not as proficient as an A3 MASS to recognize its own limitations and predict future challenges. This includes a more limited capability of aggregating data from several different data sources and sub-systems to perform predicative analysis about future states.

Examples can be to analyse complex traffic situations to take early collision avoidance actions, or to determine how different equipment failures combined can influence the vessels overall condition and performance. For an A2 MASS such tasks are to a larger degree allocated to the operator, than what is the case with A3 category vessels. The assumption is based on how the A2 level implies an increased demand to keep the operator informed (than A3).

The above-mentioned assumption is further supported by the final part of the definition. Compared to A3 where the qualified operator overrides the ship system when operating *outside* defined parameters, with an A2:

“[...] the qualified operator can override the system at any stage.”.

This implies that an A2 MASS is not always capable of sound judgement regarding whether to enter an MRC or to continue with an operation in case of abnormalities. As such, there can be a demand for the operator to intervene, both to *prevent* abnormal situations as well as to ensure that the MASS safely enters an MRC.

In summary, an A2 level MASS is less advanced in its automated capabilities compared to those designed and operated according A3. As a result, they require more active supervision, decision-support and intervention from operators both to stay within boundaries of normal operations, and to reliably enter MRCs.

4.2 Identification and breakdown of generic A2-B0 functions

Being able to identify risks emerging as a result of adopting the A2-B0 level of autonomy and control requires that the functions expected to be performed by the MASS are identified. The first step in this process is to perform a function analysis by breaking down (decomposing) the MASS main functions into hierarchy of sub-functions. This function hierarchy (or “tree”) helps to further define how the A2-B0 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, justification for the identified sub-functions or tasks can be found by asking “why” they are required.

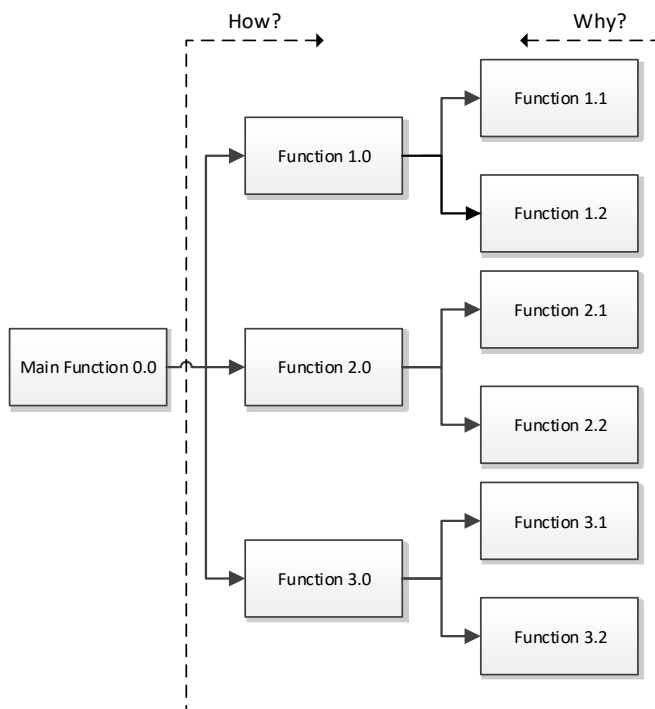


Figure 2 – The “how” and “why” logic behind function hierarchies

A generic function tree was developed which included a complete list of functions expected to be performed by the study’s three A2-B0 MASS vessels. The main functions are listed in Figure 2, while the next level of sub-functions is described in the following subsequent chapters

In contrast to the functions analysed in part 1 of the study the A2-B0 ship analysis is restricted to the functions highlighted in Blue in Figure 3. More specifically the sub-function *Navigation & Manoeuvring during transit* was the main focus of the workshop. In addition, the abnormal situations subfunctions related to Fire, Search and Rescue (SAR) and damage control was discussed.

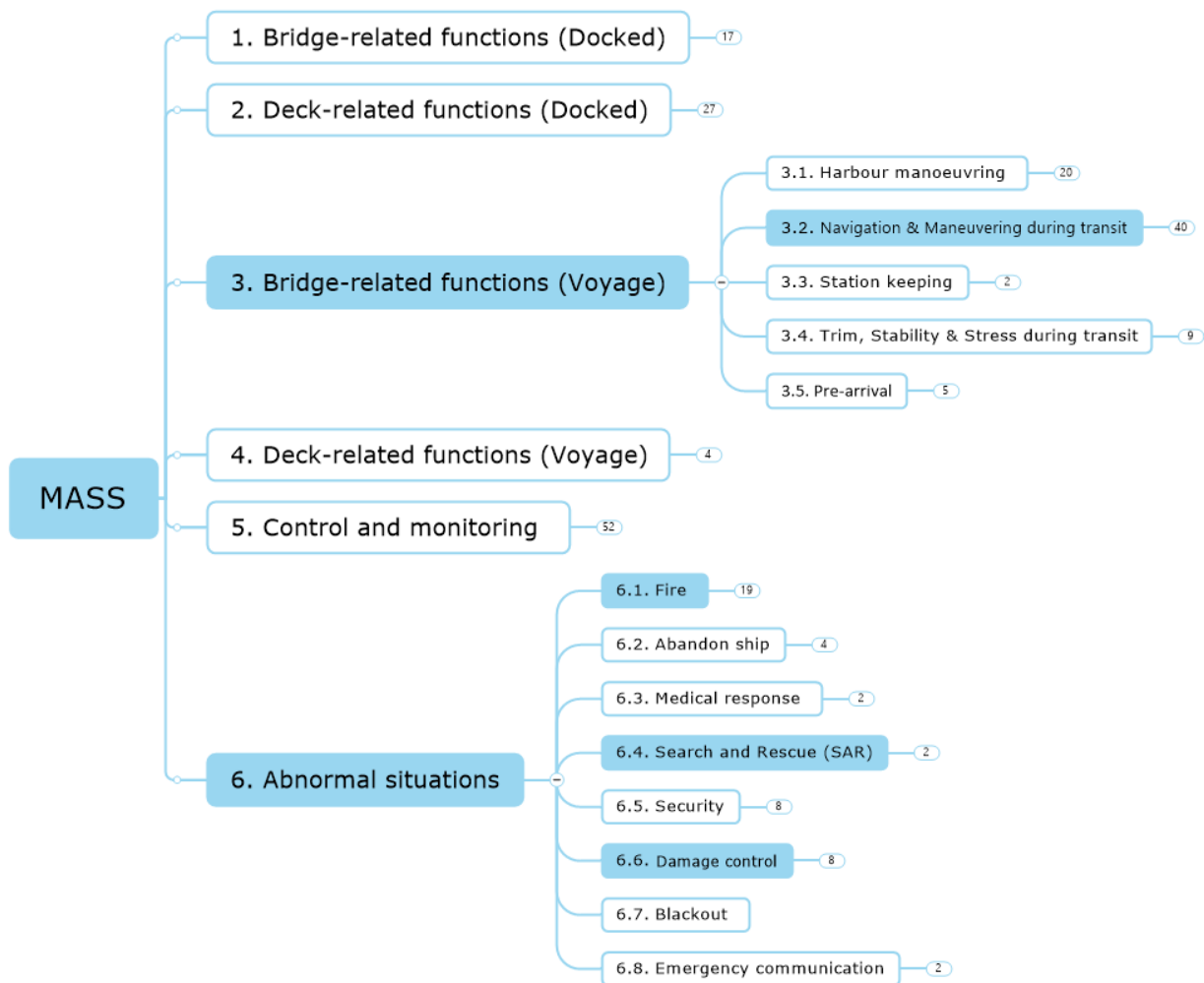


Figure 3 – Functions under analysis for A2-B0 ship

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 functions in the engine department on a MASS is largely independent of operational mode. For this reason, the Bridge/Deck functions was divided in to 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 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* to the 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 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 /3/.

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).

Figure 4 illustrates the function *Navigation & manoeuvring during transit* which was under focus in the part 2 HAZID workshop. The following subchapters will explain each of the subfunctions illustrated in Figure 4 in more details.

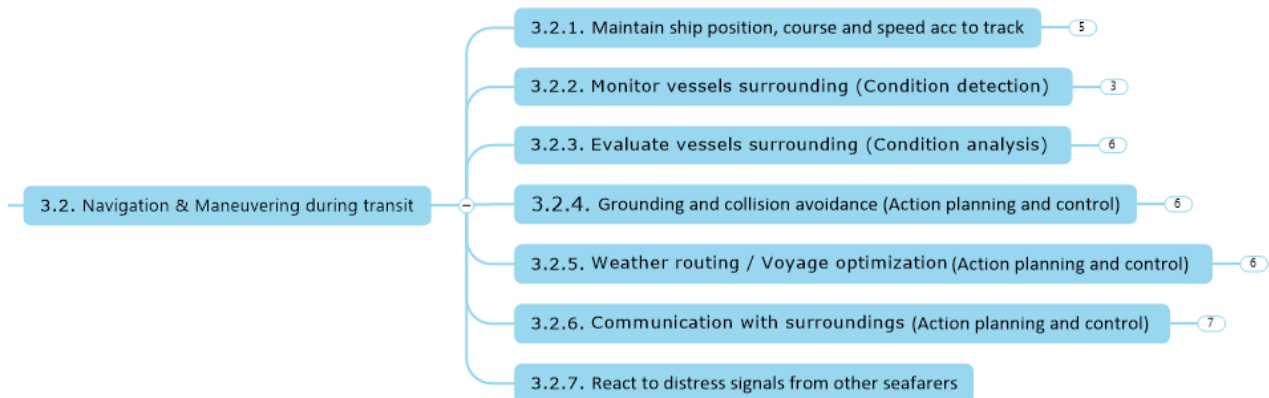


Figure 4 – Navigation & Manoeuvring

4.2.1 Maintain ship position, course and speed according to track

The function of maintaining the ship position, course and speed according to track can be performed by existing heading and track control systems. However, most track control systems require an active supervision and confirmations by a human operator. A more autonomous system is assumed for the A2-B0 ships under analysis in this study. More autonomous in respect that the system will alter speed and heading by itself without notifying any human operator. Furthermore, the system deviates from the existing systems by having the ability to adjust the route during transit while current systems will strictly follow the track approved by the operator before departure. It is assumed that the A2-B0 system has the ability to adjust the track during transit by considering external factors as described in in the following sub-chapters (4.2.2, 4.2.3, 4.2.4, 4.2.5, 4.2.6, 4.2.7). Consequently, the system is assumed to be able to conduct the route autonomously without notifying the operator when operating within pre-defined parameters of what constitutes normal operations.

4.2.2 Monitor vessel surroundings (Condition detection)

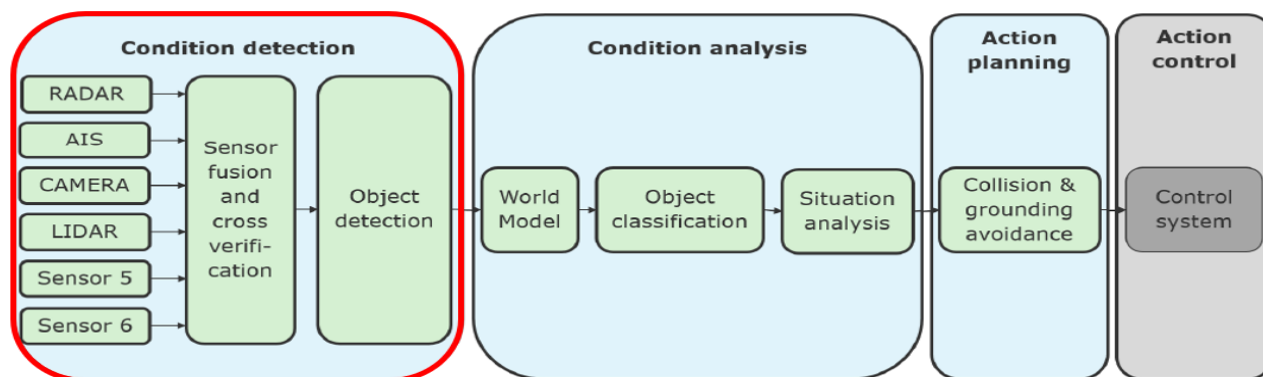


Figure 5 – Condition detection

The navigation functionality for the A2-B0 vessels in this study is based on DNV GL class guidelines for autonomous and remotely operated ships /2/ illustrated in Figure 5. For the *Condition detection* function, it is assumed that the vessel has the following instruments available: RADAR, LIDAR, AIS, Camera and sound reception systems. In addition, it is assumed that the ship is equipped with wind and tidal current sensors as well as wave radar to detect the local environmental conditions. Furthermore, it is assumed that the system will in this phase be able to detect and record all external communications attempts conducted by other vessels or personnel to an equal degree as a human operator. Including communication conducted verbally, over radio or by light and sound signals. Finally, it is assumed that all instruments are interfaced to a central system for cross verification.

4.2.3 Evaluate vessel surroundings (Condition analysis)

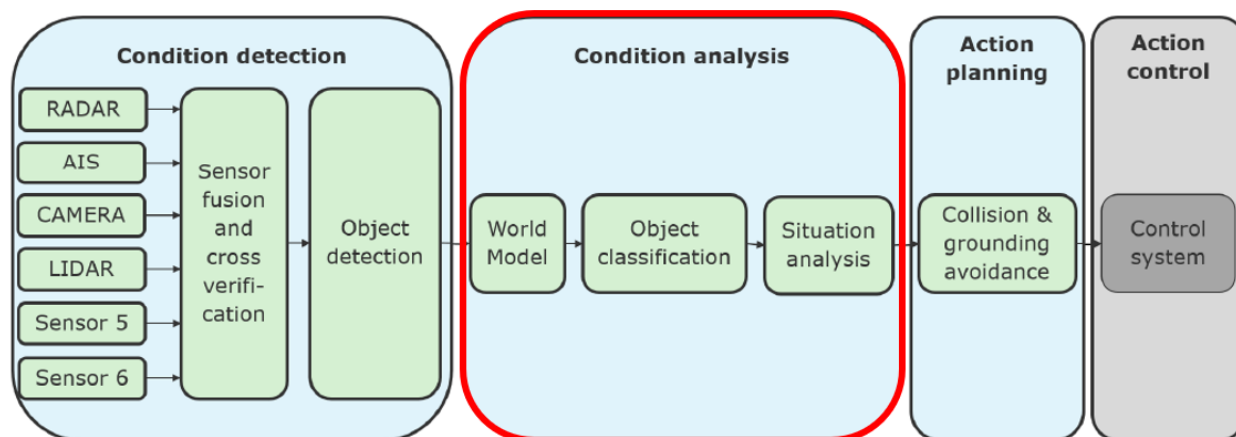


Figure 6 – Condition analysis

The data received in the previous phase is analysed as illustrated in Figure 6. Initially the data is analysed to identify the class of the object. It is in this phase assumed that the system is capable of classifying most categories of vessels, navigational marks and other floating or fixed objects. If the system is not able to classify the object to a certain percentage of probability the human operator in the RCC is alerted.

Once the object is classified the situation analysis commences. It is in this phase assumed that the system considers the objects speed and course to predict further movements and

estimate if there are any potential conflicts compared to the vessel's own plan. To aid this process, it is assumed that the probable movement and manoeuvre capability is predicted based on a profile database linked to the classified object as well as the COLREG regulations. Similar as to the classification phase the human operator in the RCC is alerted if a classified object, deemed to be in potential conflict with own plan, deviates significantly from the expected movements or otherwise operates in an unpredictable manner.

Furthermore, the local environmental data collected in the previous phase is analysed and compared to the forecasted weather. By weighing the actual weather against the forecasted, it is assumed that the system is able to predict the future environmental conditions to an equal degree as a human operator.

Likewise, the external communication data from the previous phase is analysed against the IMO's Standard Marine Communication Phrases (SMCP) or similar standard communication guidelines to anticipate the vessels intentions and need for reply. In this A2-B0 ship concept, it is not expected that the system is able to understand and conduct all external communication independently. Instead, the human operator in the RCC is alerted if uncertainties occurs.

4.2.4 Grounding and collision avoidance (Action planning and control)

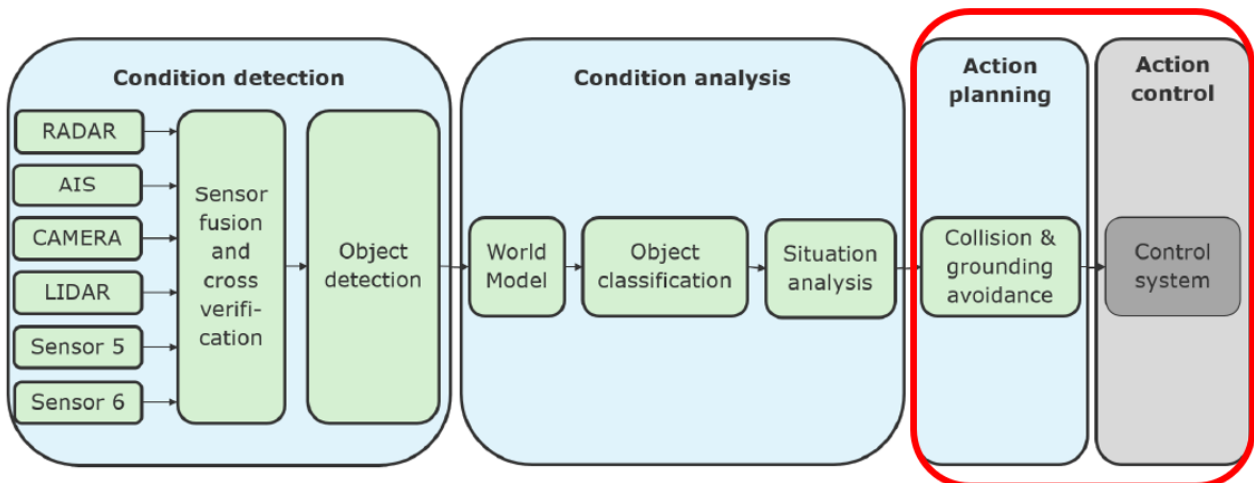


Figure 7 – Action planning and control

The collision and grounding avoidance function is conducted in the final phase of the model as illustrated in Figure 7. During this phase the system estimates the most optimal action to avoid collision or grounding. It is assumed that the system will to some degree recognize emerging hazards related to the chosen route and will communicate this to the remote operator if exceeding pre-set risk parameters. However, in contrast to the A3-B1 vessels described in Part 1, it is not assumed that the system always will have the capability to stop operation or enter an MRC without relying on operator intervention.

4.2.5 Weather routing and Voyage optimization (Action planning and control)

It is assumed that the A2-B0 ship is able to conduct weather routing and voyage optimization during transit. Similar to *the previous function*, the *weather routing and voyage optimization* is included in the action planning and control phase as illustrated in Figure 7. Based on the results from the condition analysis, the system will estimate the most optimal route to avoid

weather damage and reduce transit time. In addition, it is assumed that the planned route is evaluated against the risk of grounding and collision avoidance.

4.2.6 Communication with surroundings (Action planning and control)

The *communication with surroundings* function is also considered a part of the action planning and control phase illustrated in Figure 7. Based on the condition analysis of communication it is assumed that the MASS system can provide a reply on basis requests such as “*What is your present course / heading?*”. However, as mentioned above it is not expected that this A2-B0 ship will conduct all communication. If any out of the ordinary communication occurs the RCC operator will be alerted.

4.2.7 React to distress signals from other seafarers (Action planning and control)

Similar as to the previous (Action planning and control) functions, the *React to distress signals from other seafarers* function rely on the condition detection and analysis process discussed above (4.2.2, 4.2.3). It is assumed that all objects classified as distress signals will result in the MASS system alerting the RCC operator.

4.3 Ship description and operational context

Part 2 of the study follows a similar methodology as for Part 1 by describing vessel’s operational profile and context to structure further discussion. This concept provides a description of three identical MASS vessels designed according to the A2-B0 MASS category which operates on the same shipping route between Gothenburg – Frederikshavn. The vessels are designed to operate with no seafarers onboard but are being supervised by qualified operators from a Remote-Control Centre (RCC) located in Gothenburg.

Table 3 – Ship dimensions

Parameter	Measure
LOA:	80.00m
Beam:	15.00m
Draught:	5.00m
GT:	3000
DWT:	3000
Speed:	10kn
Capacity	100 TEU

4.3.1 Ship power generation and propulsion:

MV Auto is equipped with four 2000kW diesel generators to power two 1200KW azimuth pods for main propulsion and two 700KW tunnel thrusters for harbour manoeuvring. While the normal service profile includes all thrusters, the vessel will be able to operate with only one of the azimuth pods and tunnel thrusters powered by one of the generators. Thus, providing a redundancy of the propulsion and manoeuvre capability. In addition, a backup diesel generator will be present to provide a redundancy for critical equipment in case of emergency.

4.3.2 Manoeuvre and navigation capability

It is assumed that the autonomous system can provide the same level of manoeuvrability as if manoeuvred by humans. Consequently, the vessels can to some degree maintain position keeping by adjusting the heading towards the wind/current with the use of azimuth propellers and bow thrusters. 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. Furthermore, it is expected that all vessels are equipped with a navigation system capable of adhering to COLREG within its predefined operational limitations, meaning that the system is able to navigate and manoeuvre according the regulations which does not open for undefinable options such as "good seamanship" /5/.

4.3.3 Operational area

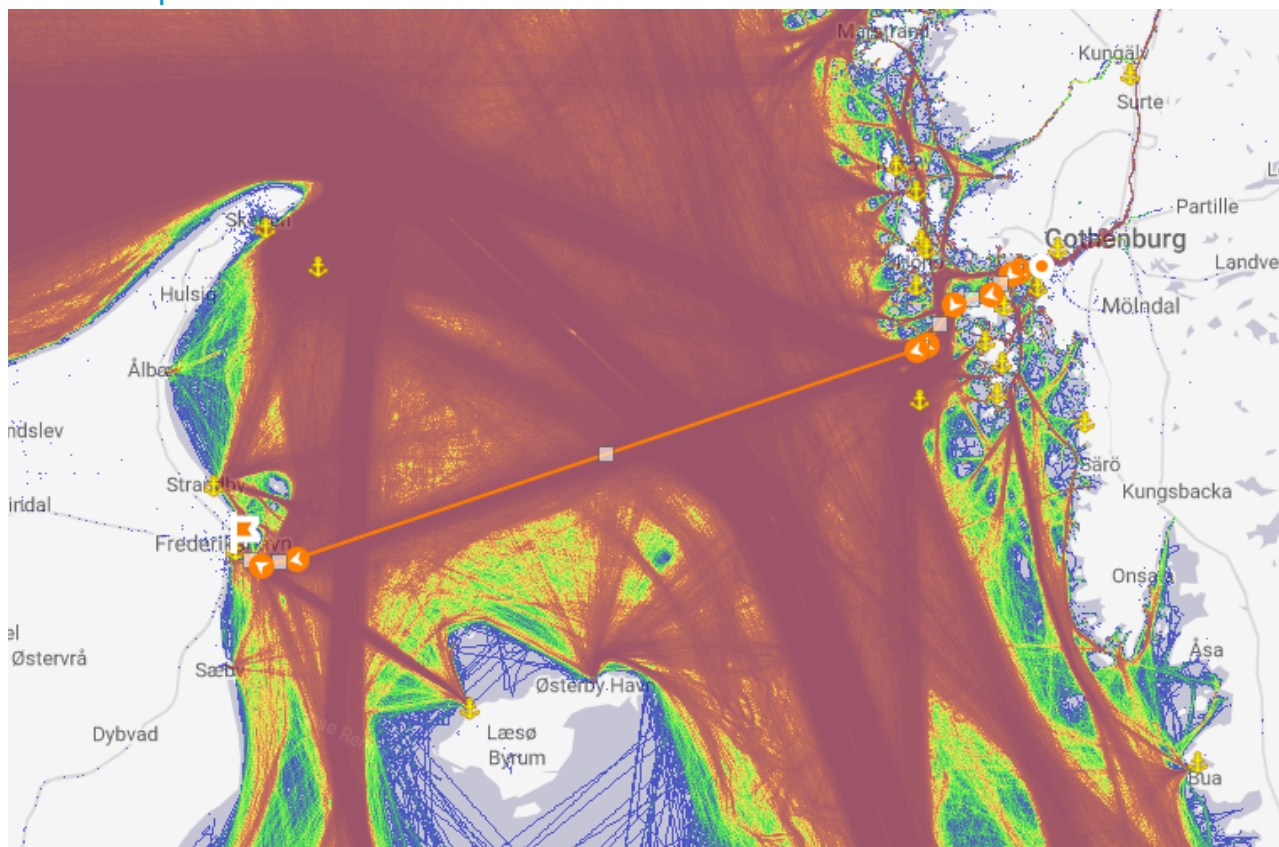


Figure 8 – Route Gothenburg – Frederikshavn

The route between Gothenburg (Sweden) and Frederikshavn (Denmark) is crossing the Kattegat sea area inside both the Swedish and Danish sector. With a total distance of 50Nm the voyage is expected to last for around 5 hours.

Figure 8 illustrates the Kattegat sea area which has a high-density traffic profile as it is the main open sea water route from the North Sea to the Baltic sea. In addition, the port of Gothenburg shown in figure 2, is Scandinavia's largest port and is also considered to be highly trafficked. Frederikshavn receive less vessels but is still considered to have a high density of traffic.

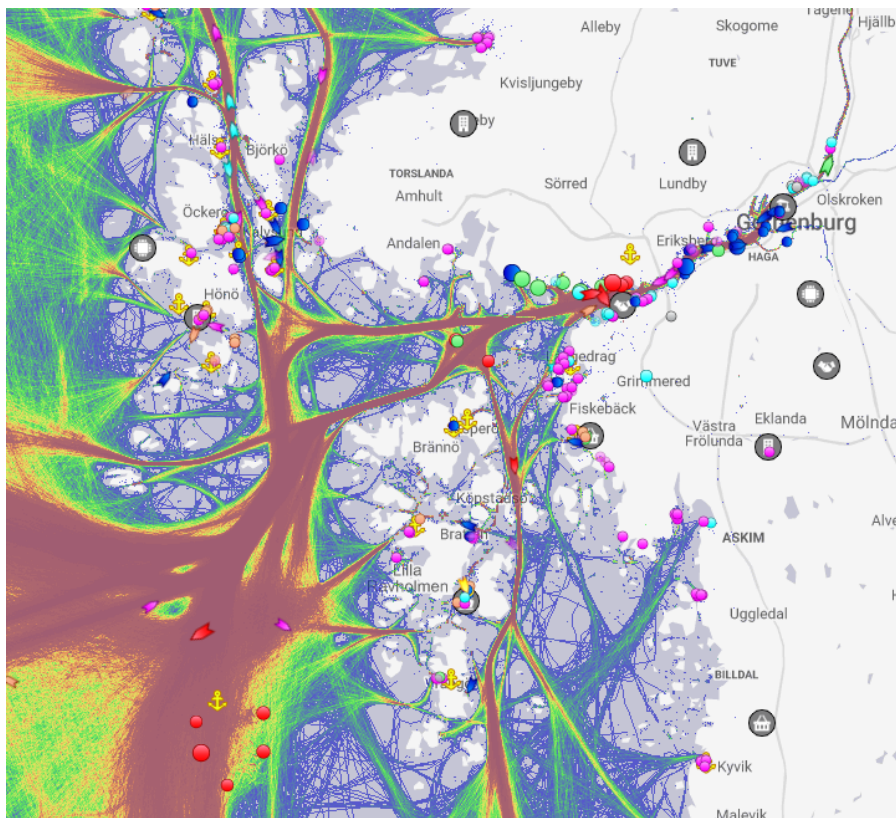


Figure 9 – Traffic situation around Gothenburg

4.3.4 Weather and sea-state limitations


Kattegat sheltered from the North Sea and is therefore not normally exposed to high waves. Still, the vessel route is passing a relatively open sea area which occasionally can receive heavy weather.

4.4 Remote Control Centre (RCC)

An RCC is in this case established in Gothenburg in a location protected from physical and electrical harm. Furthermore, all essential equipment is configured with redundancy to prevent a system breakdown caused by any single point failure. In addition, the equipment is connected to UPS and an emergency generator providing redundancy in case of power outage.

4.4.1 RCC workstations

The RCC consists of a Bridge and ECR workstation designed to provide equivalent function and interface as if the operation was conducted onboard the vessel. Thus, interfacing data from the same instruments as found on the Bridge and ECR such as: ECDIS, AIS, RADAR, LIDAR, echo sounder, Loading computer, IAS, PMS etc. In addition, high quality camera provides a live view from the Bridge to monitor traffic and navigational hazards. Likewise, CCTV are covering the entire vessel and interfaces to displays in the RCC. Furthermore, the instruments for each vessel are displayed on multi-function displays (MFD), enabling each screen to show



vessel data for all three vessels. In addition, a larger screen display is provided to give a visual overview of the more critical issues that may occur (e.g. navigational data and status and performance of main ship functions).

4.4.2 Watchkeeping and alarm notification

While the vessels are designed to operate independently, some tasks require human assistance from the RCC. In such cases it is assumed that the RCC operator will be alerted in form of a visual and/or audial alarm in a similar manner as would be the case for a conventional bridge system. Furthermore, the more critical alarms will be displayed on the focus display where some basic information will be provided to the operator regarding the issue and type of assistance required.

The functionality of the Bridge Alert Management system (BAM) will be equivalent to what is required onboard. Hence, corresponding with system BAM MSC.302(87), but adapted to RCC operations for multiple MASS vessels. To avoid the operator being overloaded with information, only the alarms rated with the highest criticality will be displayed on the focus screen.

Unlike what was the case for the A3-B1 MASS category in Part 1, the vessels are not equipped with an alarm system capable of always identifying when parameters for pre-defined boundary conditions are breached. I.e. the vessels are not always able to detect and diagnose when its autonomous system performance is degraded, uncertain or fails. Instead it will continue with its autonomous operations unless interrupted by the RCC operators. As such, alarms will primarily be provided for isolated function failures or external threats, and not for diagnostics performed by the MASS system based on a combination of segregated input data.

4.4.3 Communication between RCC and MASS

As most of the transit occurs in open waters away from shore, there is limited cellular network coverage in the area. It is therefore assumed that all communication transferred between ship to shore is sent over satellite system which have full coverage in the Kattegat sea area. It is recognized that current satellite systems would have limitations regarding the data transfer this MASS case requires. However, it is in this case assumed that a future satellite coverage is established to provide a stable high-speed connection.

4.4.4 RCC manning

All vessels are designed according to level A2-B0 autonomy which does not requires qualified operators onboard. However, the registered ISM technical management company will operate from the RCC and will therefore have full responsibility of the vessel's operation. Operators will still supervise the operation from the RCC and interfere if the vessel system is outside defined parameters. Consequently, the operators require maritime competence to understand the functions executed by the system. Hence, maritime competence from both Bridge/Deck and Engine department. This competence is already defined by the STCW conventions and serves as a basic competence requirement for RCC operators. In addition, more specialised competence regarding autonomous system is required.

Table 4 – Manning of RCC

Department	Title	No.	STCW	Responsibility
Bridge & Deck	Bridge Operator	1	II/2 II/5	- Navigational supervision - Supervise all Bridge equipment - Supervise all Deck equipment - Supervise cargo handling (Load/Discharging, securing) - Supervise vessels stability, integrity and ballast mgt.
Engine	Engine Operator	1	III/2 III/5 III/6	- Machinery supervision - Supervise all Engine machinery and equipment - Supervise all electrical equipment
Total		2		

Table 2 illustrates the proposed manning of the RCC according to level A2-B0 autonomy. The manning consists of one Bridge operator and one Engine operator with maritime competence according to the STCW convention. Furthermore, two additional operators would be required for 24h operation.

5 HAZID OF THE A2-B0 MASS CATEGORY (TASK 2. B)

This chapter documents Task 2.b in Part 2 of the SAFEMASS study; a hazard identification (HAZID) of the A2-B0 MASS concept developed in Task 2. a. The HAZID is documented in Appendix B.

5.1 Focus areas

Building on the problem definition of SAFEMASS Part 2 (see chapter 1) the HAZID's focus is primarily on challenges associated with remote supervision of MASS performance and not having qualified crew onboard. Thus, for this HAZID it was of specific interest to examine potential vulnerabilities associated with remote supervision and control by human operators.

5.1.1 RCC supervision

Regarding RCC supervision, the HAZID aimed to explore the following topics:

- Capacities and abilities required to supervise multiple vessels in various operational modes, incl. in case of abnormal situations and emergencies.
- Presentation of information on human-machine interfaces (HMI) and other visual displays required for successful acquisition and analysis of information, decision-making and implementation of control actions.
- Threats to operator vigilance induced by human factors such as boredom during quiet, normal operations, and stress during periods with high workload.
- Influence from challenges with communication link, such as latency and connectivity.

5.1.2 Unmanned operations

Regarding unmanned operations, the HAZID aimed to explore the following topics:

- Operators' diminished ship sense from being remotely located (onshore), e.g. reduced or altered perceptions of stability, speed, heading and environmental conditions.
- Challenges related to not being physically present to fix problems, e.g. in case of maintenance, equipment failures or rescue operations.

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 sheet (Appendix B) was developed specifically to meet the objectives and address the focus areas of SAFEMASS Part 2. As can be seen in Figure 10 and Figure 11, the log sheet consisted of two main parts; a) Control room operator response, and b) the Hazard identification.

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

Control Room Operator response			
ID	Operator presence	Tasks	Information required
3.0 Bridge-related functions (Voyage)			
3.2 Navigation & Maneuvering during transit			
1	From discontinuous monitoring (RM2) to full monitoring (RM3)	- Acknowledge collision warning alarm on MASS 1, obtain situational awareness and monitor system performance	- Alarm (visual and sound) - Closest Point of Approach (CPA) - Time to Closest Point of Approach (TCPA) - ECDIS, radar, camera, etc.

Figure 10 – “Control Room operator response” columns in the HAZID log sheet

Hazard Identification (What if....?)					
Guideword	Hazardous event	Cause	Consequence	Top event (worst case)	Safety measures
C1: Check omitted	Operator (Bridge) asleep, does not acknowledge collision alarm	-Task/ job factors (physical working environment, procedures, etc.) - Individual/ person factors (work overload/underload, fatigue, motivation) - Organisation factors (work pressures, manning level, organisational or safety culture, psychosocial working environment, etc.	- Lack of time to analysis and take correct action. - Escalation of situation → increased likelihood of major accident event (collision)	Major accident event: Ship collision → With potential for loss of life	Ensure: - Always more than 1 operator present in room - Sound alarm (collision warning) - Navigational Watch Alarm System (BNWAS), motion sensor system - Sufficient procedures, HMI and "Fit for duty" operator self-assessment - Last resort by ship systems → Minimum Risk Condition (MRC) to be defined for all expected scenarios - Alarm escalation path are defined.

Figure 11 – “Hazard identification” columns in the HAZID log sheet.

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

- a) **Control room operator response** (Figure 10), consisting of four columns for collecting the following data:
 - i. *ID*; Hazard identification number.
 - ii. *Operator presence*; location and mode of the operator (see separate definitions below).
 - iii. *Tasks*; Actions required by human operator.
 - iv. *Information required*; Information required by the human operator to conduct the task.

b) **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 – Guidewords).
- ii. *Hazardous event*; event associated with MASS performance and/ or RCCs ability to supervise operations.
- iii. *Cause*; Factors which could cause the hazardous event to occur. In this study the human-related hazards listed in the FSA guideline /4/ (MSC-MEPC.2/Circ.12/Rev.2) 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. *Safety measures*; 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 were identified, these were noted as input for further considerations.

The definition of **operator presence** was based on the classification provided in ISO 23860 /4/ (with some custom modifications):

- *RM0 – No remote monitoring*: There are no operator to monitor the autonomous ship system, nor to take control in case of warning or alert from the system.
- *RM1 - Available remote monitoring*: The operator is available in the control room, ready in case of warning or alert from the ship automation system, but they may be not at the control station. There will be a longer latency before the operator can have full situational awareness.
- *RM2 - Discontinuous monitoring*: The autonomous ship system is monitored and controlled by the control room operator. Monitoring and control may be discontinuous during a short period. The operator is always available at or near the control station, ready in case of warning or alert from the system. The operator control latency is relatively short.
- *RM3 - Full monitoring*: The autonomous ship system is actively monitored and controlled at any time by the control room operator. The operator control latency is close to zero.

5.2.2 HAZID nodes

The *Control Room Operator Response* columns in the HAZID log sheet includes operator presence, tasks and information required to perform functions identified as critical and relevant in the function breakdown (chapter 4.2). This makes up the HAZID's main study nodes, i.e. items subject to analysis and are listed in Table 5.

Hazards associated with other functions and scenarios were logged as they emerged naturally from the workshop discussions, or from being prompted by HAZID guidewords.

Table 5 – Functions initially selected for hazard identification

ID	Function
---	<i>Bridge-related functions (voyage)</i>
3.2	Navigation & manoeuvring during transit
3.2.1	Maintain ship position, course and speed according to track
3.2.2	Monitor vessels surrounding (condition detection)
3.2.3	Evaluate vessels surrounding (condition analysis)
3.2.4	Grounding and collision avoidance (action planning and control)
3.2.5	Weather routing / Voyage optimization (action planning and control)
3.2.6	Communication with surroundings (action planning and control)
3.2.7	React to distress signals from other seafarers (action planning and control)
---	<i>Abnormal situations</i>
6.1	Fire
6.4	Search and Rescue (SAR)
6.6	Damage control

A majority of the functions listed in Table 5 were related to a navigation. The same scenarios used in SAFEMASS Part 1 were applied to provide a context for discussing navigational hazards during the HAZID workshop (see Table 6).

Table 6 – Scenarios used to aid hazard identification

ID	Scenario description	Graphic illustration
1	<p>COLREG Crossing situation</p> <ul style="list-style-type: none"> - First phase of scenario 1 describes a crossing situation where vessel B is on crossing course with MASS vessel 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 maneuvering according to COLREG Reg.17. 	

ID	Scenario description	Graphic illustration
2 COLREG Crossing situation	<p>- Other ship B on 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.</p>	
3 High density traffic situation - regatta	<p>- Scenario 3 describes a high-density traffic situation where the MASS vessel encounters several sailboats attempting to cross (regatta). - Due to the complexity of the situation the system is not able to analyze (predict next movements).</p>	
4 High density traffic situation - pleasure crafts	<p>- 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.</p>	
5 COLREG Crossing situation	<p>- 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.</p>	

5.2.3 HAZID process

The HAZID workshop was performed at DNV GLs offices in Høvik on the 15th and 16th of October, 2019. Representatives from EMSA, NMA, Wilhelmsen and Norwegian Shipowners Association were participating collectively with DNV GL consultants.

- 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)
- 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

A more detailed description of the participants profile can be read in Appendix A.

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 operator presence, tasks, information required and navigation functions (i.e. the HAZID study nodes).

Three specific measures were made to ensure that the participants had a 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 A2-B0 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 as 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 50 rows with unique ID numbers. Hazards/ hazardous events, causes and consequences from 45 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. The remaining 5 rows were all grouped under HAZID node *Abnormal situations* and includes risks associated with responding to various emergencies. These are marked with light "orange" coloured IDs and are summarized below. All the hazards reflect limitations associated with the operators being remotely located, instead of physically present onboard the MASS:

- HAZID ID #45: Limited ability to physically observe (sense vibration, noise, perform checks) severity of damage/ compartments caused by grounding. Although being supported by instrumented systems monitored and controlled from the RCC, the response may become more complex and time consuming (depending on the design).
- HAZID ID #46: Limited ability to confirm severity of potential impacts with smaller objects (kayak, rib, sailboat), such as people in the water or being injured. This may result in Search and Rescue (SAR) or other emergency response services not being called for, which in turn could increase the risk of fatalities, e.g. due to drowning.

- 
- HAZID ID #47: In case of detecting people in distress, e.g. due to a collision, an unmanned MASS will face challenges when it comes to rescuing people either from the water or sinking vessels. Remotely operated SAR functions will have to be defined, or alternatively, rules and legal aspects regarding responsibilities will have to be reviewed.
 - HAZID ID #48 and #49: Having no people physically onboard can also cause challenges when it comes to confirming onset of fires and performing firefighting. Depending on where the fire occurs, and what the available means are for firefighting, being solely dependent on fire detection systems can cause unnecessary downtime or escalation. To compensate for having no one onboard, small fires may have to be extinguished with full scale firefighting systems (e.g. sprinkler), instead of a firefighting team extinguishing the fire locally. Alternatively, small fires may go undetected and escalate in case of insufficient fire detection coverage.

6 FAULT TREE ANALYSIS (TASK 2. C)

This chapter documents Task 2.c in Part 2 of the SAFEMASS study; a fault tree analysis (FTA) of potential accident scenarios related to the A2-B0 MASS concepts developed in Task 2.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 /4/. Fault tree symbols are explained in Table 7.

Table 7 – 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.



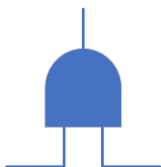
Basic event symbol: The basic event symbol indicates what are considered the most detailed level of causes to be examined, as determined by the purpose of the analysis and availability of data.



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 the main TOP event:

- MASS fails in collision avoidance

The TOP event was selected to reflect the problem definition of SAFEMASS Part 2, namely to examine emerging risks associated with the navigation function of A2-B0 MASS. Hazards not included as part of the fault trees, but still considered relevant, are discussed in chapter 5.3.

The FTA adopts the HAZIDs focus on challenges associated with RCC supervision and unmanned operations. This implies that efforts were made to include and examine events representing vulnerabilities related supervision of multiple vessels, not having personnel



onboard, as well as the functionality and availability of the communication link. Exceptions can be other types of events which are primarily included to provide an overall understanding of the risk picture. Such events are not examined in detail due to mainly reflecting hazards already associated with conventional shipping (i.e. not emerging risks associated with A2-B0). 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 model 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).
- **RCC operator:** RCC 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 /4/ 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 is provided in sub-chapters 6.2.

6.1 TOP event: MASS fails in collision avoidance

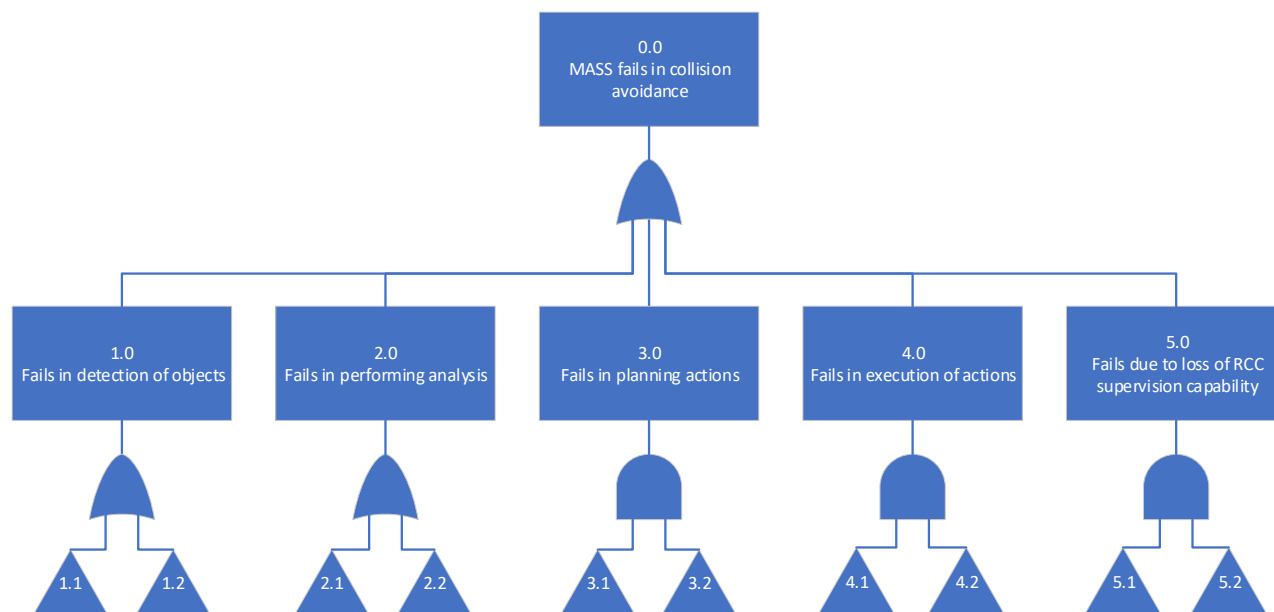


Figure 12 – Fault tree branches for TOP event ID 0.0 (collision avoidance failure)

The *TOP* event selected for the FTA in Part 2 is that the MASS fails in avoiding collision with another vessel or floating object (Figure 12). In contrast to the specific COLREG scenarios examined in Part 1 of SAFEMASS, this FTA applies a more general approach where the actions of external vessels are not specified in detail. Instead the FTA analyse the failure of performing collision avoidance by examining causal factors behind the intermediate events:

- 1.0 MASS fails in detection of objects
- 2.0 MASS fails in performing analysis
- 3.0 MASS fails in planning actions
- 4.0 MASS fails in execution of actions
- 5.0 MASS fails due to loss of RCC supervision capability

The navigation functions of object detection, situation analysis, planning and executing manoeuvring actions can be considered an iterated sequence of actions required to avoid collision with objects. An object or vessel is detected, its behaviour and intentions are analysed, a plan for how to avoid collision is generated, and finally the plan is put into action. As the performance of each subsequent function depends on the former (i.e. they are dependent), a failure at each step of the sequence could result in a collision.

Lastly, failure of the RCC to perform supervision is identified as a separate hazard as it has the potential to cause a global navigation failure (i.e. it causes all functions to fail).

6.1.1 MASS fails in detection of objects

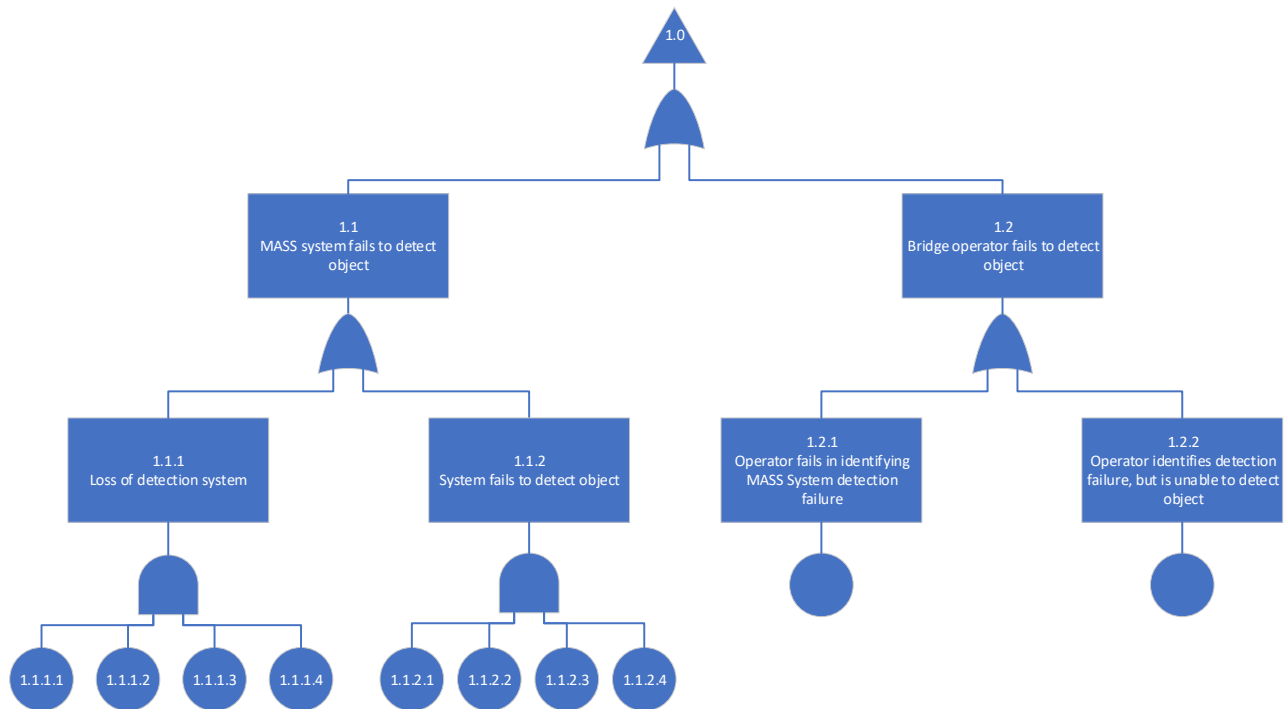


Figure 13 – Fault tree branches for intermediate event ID 1.0

Both the MASS system and the RCC operator can fail in detecting a hazardous object (Figure 13). Depending on the type and number of detection systems the MASS has available, their overlap in capability, range and sector; a loss of one detection system can potentially compromise the whole detection capability. Likewise, specific detection systems could have limitations that prevents it from detecting certain objects. Nevertheless, it is assumed that a MASS approved for operation will utilize more than one detection system. Hence, if a camera has reduced detection capability due to e.g. snow, other systems such as RADAR or LIDAR are available to provide heterogenous redundancy to compensate for the loss of object detection via cameras.

Furthermore, the RCC operator's opportunity to detect an object depends on him or her being notified, e.g. via an alarm system. As the RCC operator in this A2-B0 MASS concept is responsible for monitoring several (three) vessels, the operator's attention capacity will be devoted towards where it is the most required. The MASS system's ability to recognize its own failure and alert the operator is therefore considered a vulnerable part of the overall system.

However, even if the RCC operator is alerted there is still a risk that he or she is not capable of detecting the object, e.g. due to environmental factors such as snow, fog etc., creating poor visibility, or poor image projection. Moreover, the operators' vigilance and detection skills also rely on individual skill sets and being provided with sufficient training and procedures.

6.1.2 MASS fails in performing analysis

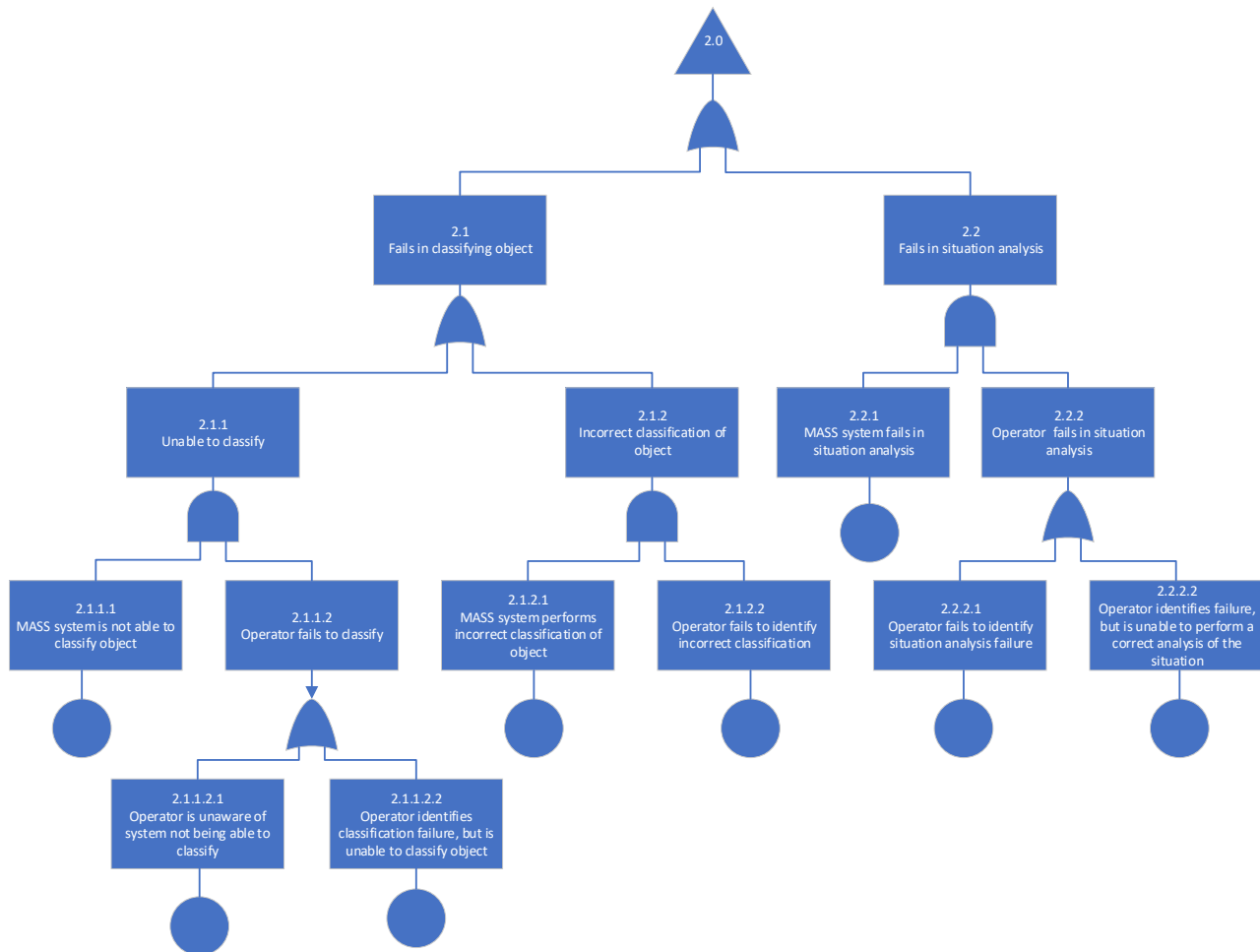


Figure 14 – Fault tree branches for intermediate event ID 2.0

The intermediate events illustrated in Figure 14 concerns the analysis and classification of data obtained from the detection systems. Consequently, it is assumed that successful object detection has occurred. It is then necessary to classify and analyse the object to establish situational awareness. This forms the basis for interpreting the object(s) intentions and future actions.

Part of this function consist of identifying the object to be of a pre-defined class of objects, e.g. motor driven vessel. As such, the MASS system may fail at situation analysis by not being able to classify an object with sufficient confidence. Similar to object detection, the RCC operator will not be able to support the MASS system in performing classification, unless he or she is notified to do so.

Furthermore, the MASS system may also fail at situation analysis in case of performing incorrect classification of an object. For instance, a vessel engaged in fishing could be mistaken as an on-route cargo vessel. Such a failure may potentially be more critical than (knowingly) not being able to classify at all, as the both the MASS system and RCC operator will not be made aware of the mistake and its implications. Moreover, due to the dependency between the functions, subsequent situation analysis will be performed using incorrect data.

Lastly, the MASS system could fail at performing analysis despite being provided with correct data. In a traffic scenario the MASS system is programmed to assume that the other vessels are COLREG compliant and interpret their future intentions accordingly. For most vessel types, including the MASS in this concept, a vast number of complex traffic situations can occur. It is considered reasonable to believe that the MASS system occasionally will experience limitations in its capabilities, and therefore require assistance from the RCC operator to analyse situations. Again, as with object detection and classification, successful human intervention requires an alarm or notification to be issued. If the traffic situation at this stage is already challenging to analyse for the MASS system, the RCC operator may have limited time available to gain the situational awareness required for planning and deciding on how to act.

6.1.3 MASS fails in planning actions

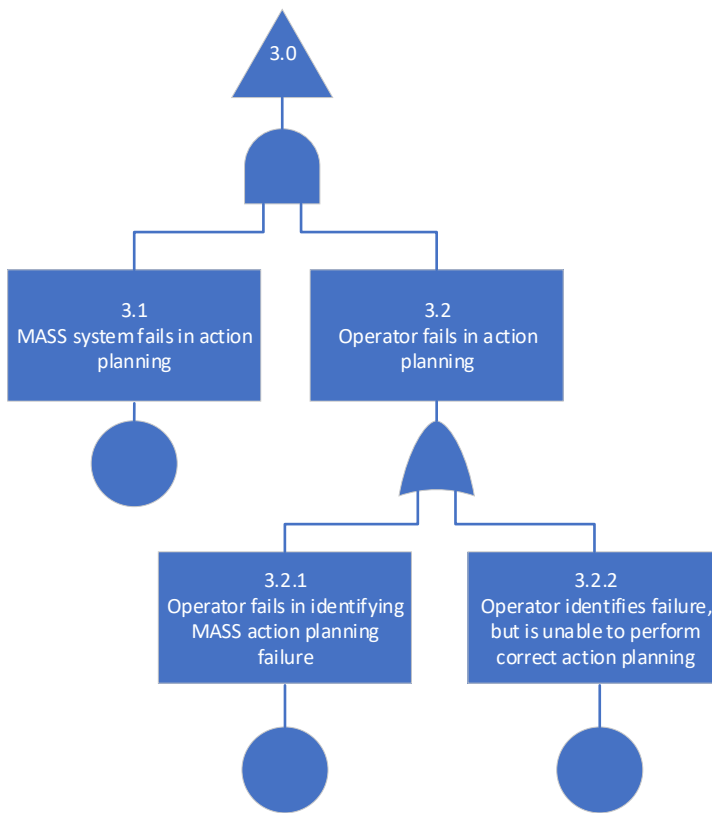


Figure 15 – Fault tree branches for intermediate event ID 3.0

After having analysed the situation, the MASS system’s next step is to plan which actions to execute (Figure 15). When applied to a traffic scenario, after having interpreted the other vessels’ intentions the MASS then (iteratively) estimates how its own movements can aid in preventing a collision. This study’s concept assumes that COLREG will serve as a basis to calculate the MASS’ preferred manoeuvres. That being said, COLREG rules cannot be transformed directly into a set of quantitative rules and are therefore subject for interpretation. To experience conflicts between rules must therefore be expected, also when applied to automation algorithms. In collision avoidance scenarios, it is here argued that the MASS system will weight its options against an estimated degree of compliancy with the different rules. Consequently, there is a risk that the MASS system fails due to incorrect weighting of the rules. Furthermore, the underlying interpretation COLREG used as basis for

programming automated decision-making may be faulty, due to the vast number and combinations of navigational situations it is intended to cover.

The RCC operator is meant to be alerted if the actions planned for are to some degree in conflict with parts of COLREG or other pre-set parameters. Because it may be challenging to define parameters for when to request assistance from the RCC operator to resolve various COLREG scenarios, there is a risk that notifications and alarms are issued too late. This may cause a situation where the MASS already is in a close traffic scenario. As for the other navigation functions, a delay or failure to alert the operators will reduce the time available to enter the automation-loop, and thus increase the risk of human error.

6.1.4 MASS fails in execution of actions

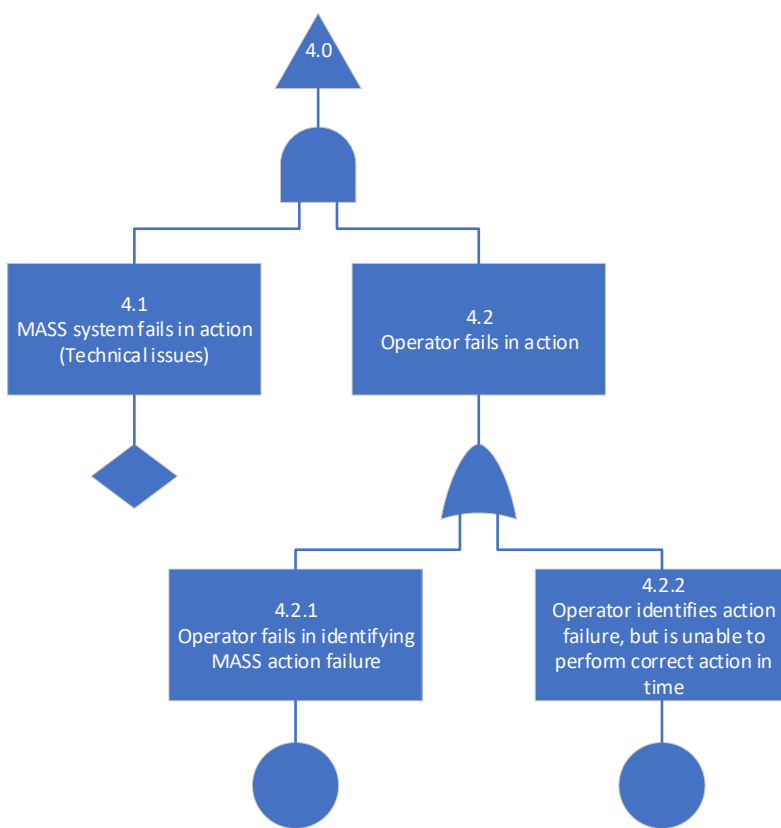


Figure 16 – Fault tree branches for intermediate event ID 4.0

The execution of planned actions is the final step of a collision avoidance sequence (Figure 16). Assuming that all of the previously mentioned functions (detection, analysis, planning) are performed correctly, this step consists of the actions required to physically alter the behaviour of the MASS. As with the other functions, the operator is alerted in case of failing to perform the intended actions, or if there are any critical malfunctions with technical equipment. At this point it is particularly critical if the MASS system fails or is delayed in alarming the operator. The available response time for the operator is likely to be even more marginal during the action phase as it is the final part of attempting to avoid collision.

6.1.5 MASS fails due to loss of RCC supervision

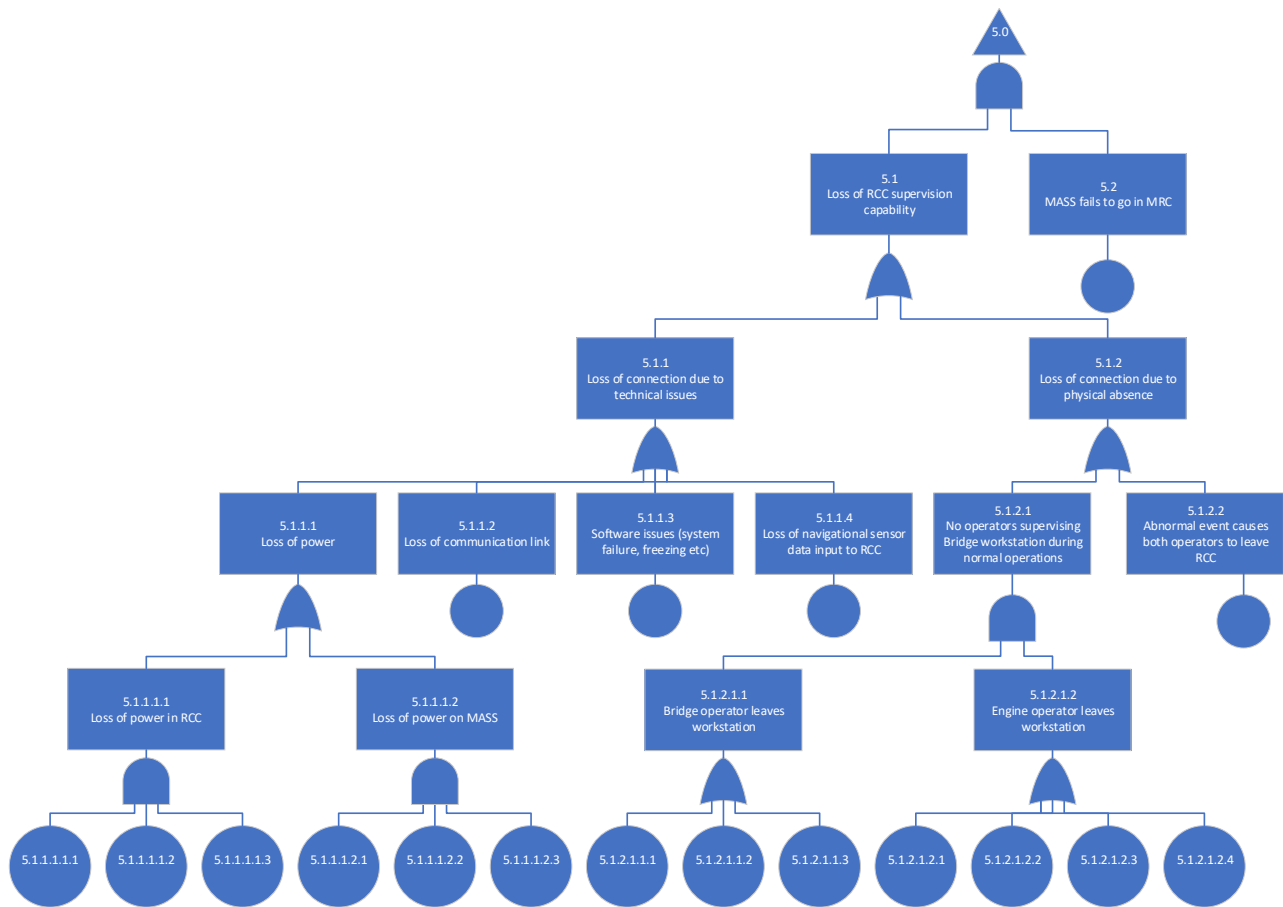


Figure 17 – Fault tree branches for intermediate event ID 5.0

The loss of RCC supervision capability (Figure 17) is assumed to affect all of the previous mentioned phases and is therefore grouped into a separate task. If for some reason the RCC is unsupervised, the operator's role in the detection, analysis, planning and action phase can be discarded. The remaining contingency will then be the systems capability to solve the issue or enter an MRC.

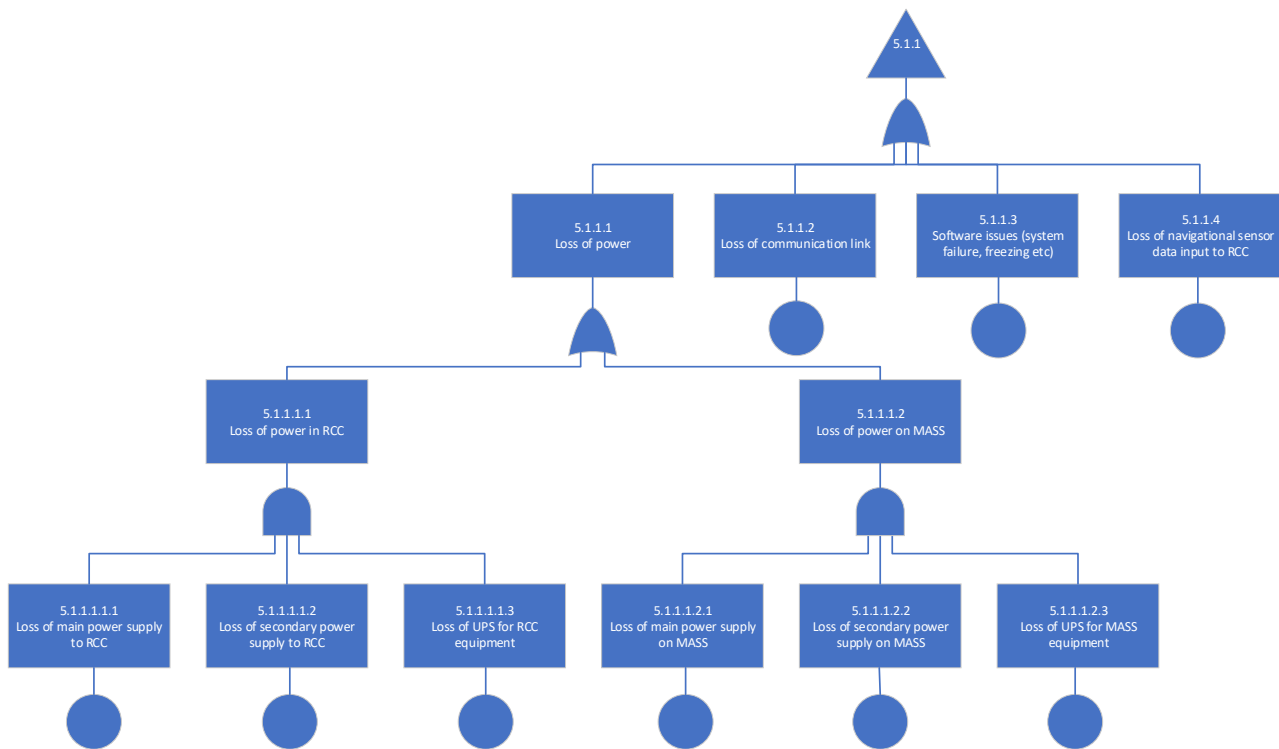


Figure 18 – Fault tree branches for intermediate event ID 5.1.1

Loss of RCC supervision capability can mainly be traced back to either technical issues or physical absence of operators (Figure 18). Furthermore, the technical issues can be divided into several failure types such as loss of power, communication or navigational sensor data, as well as software issues. Of these, a full loss of power in the MASS or RCC can be considered to more serious failure events. However, the MASS and RCC utilized in the concept of this study includes a full redundancy (secondary power supply and UPS) which reduces the probability for a full blackout to last for a longer period.

Another serious event is losing the communication link between the MASS and RCC. While a stable satellite connection is part of the study's concept, such a failure is considered realistic in future projects involving highly automated vessels. If the main communication link is lost, the RCC operator will not have any possibility to operate the MASS and have to rely completely on the MASS system's ability to enter and maintain a as safe as possible state. Another scenario is losing the connection due to software issues. If for example the system "freezes" or shuts down, it could result in a partial or fully loss of supervision capability. Such software errors could be that the ECDIS used for supervision stops responding and requires a reboot. Other failures could be the loss of navigational sensor data input to RCC such as RADAR or camera. The severity of the failure would then depend on the remaining sensors and current situation.

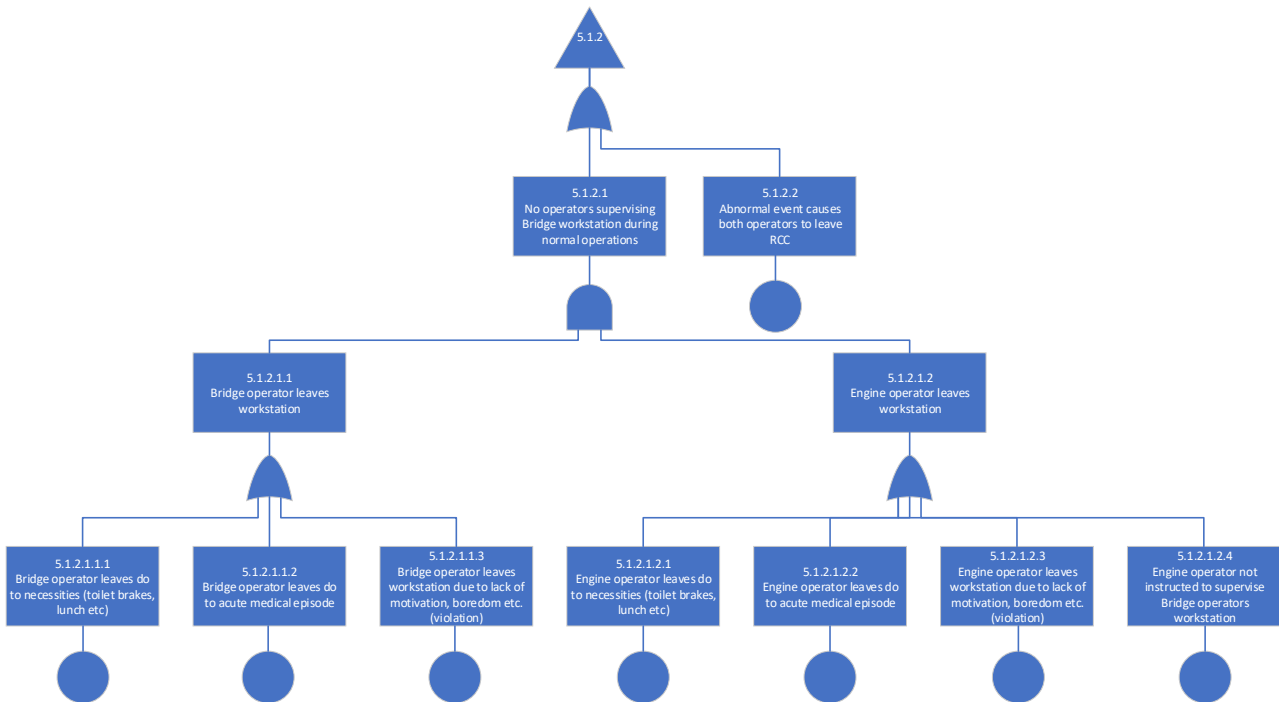


Figure 19 – Fault tree branches for intermediate event ID 5.1.2


Regarding lack of operator presence (Figure 19) the most serious hazard is considered to be that the operators needs to evacuate due to an abnormal event such as fire, injuries, terror etc. In such events the RCC operators would lose all control of the MASS if no backup operator stations are available at other locations. These abnormal scenarios are however considered to be low probability events. Unless regulated, situations where the RCC operators temporarily leave the workstation for more mundane reasons is considered to be far more likely. The operator needs to leave the workstations during the watch for various necessities such as toilet brakes, lunch etc. Moreover, the operator might encounter some acute medical issues that requires him or her to leave the workstation immediately. In such cases only one operator will remain in the RCC to supervise both the bridge and engine workstations. This can be considered a difficult task if the operator has limited cross competence, or if the HMI has limitations when it comes to supervising multiple systems and vessels. Other threats are incidents where one of the RCC operators leaves the workstation without sufficiently instructing the other operator about how to perform substitutional supervision.

6.2 Emerging risks associated with collision scenario

The HAZID and FTA uncovered several emerging risks related to the concept of A2-B0 MASS operations. A summary of the main concerns is presented in the following sub-chapters.

6.2.1 Navigation failures not alerted to, or undetected by, RCC operator

Several of the identified risks relate to navigation failures not being communicated to the RCC operator, e.g. by use of alarms or other notifications. If the MASS system is not aware of its own failures the RCC operator(s) will also not receive a cue about what is wrong. Then the only way for the operator to notice the failure is to actively monitor the systems, at all times. This does not however appear to be a feasible solution with the study's concept of only two RCC operators (engine and bridge) being responsible for supervising three MASS in simultaneous operations.



If, for example, a smaller pleasure craft for some reason is left undetected by the system, the RCC operator may not have sufficient attention span or capacity to focus on this specific area. Consequently, he or she may fail to implement compensating interventions. A similar situation may occur in cases where the MASS system has classified or analysed an object's intention incorrectly. The MASS system may, for example, confuse vessels types or navigational marks without notifying the RCC operator. Similarly, it may interpret a traffic operation incorrectly due to inadequate algorithms. While the operator might recognize the error if he or she is made aware of it, it will be difficult to identify if no cue is provided.

6.2.2 RCC operator's response to navigational failures not made feasible


Other risks emerged regarding the RCC operators' role in responding to failures in the navigational functions. This refers to the situations where the MASS system recognizes its own limitations and/or failures and successfully requests assistance from the RCC operator(s), e.g. via an alarm. Even if the operator directs all his/her attention to the task, risks associated with all the navigation functions (detection, analysis, planning and action) have been found.

The analysis revealed some concerns related to the detection instruments' potential limitations when it comes to observing smaller objects. Especially, detecting leisure craft or objects such as submerged containers or fishing gear may not always be successfully detected by RADAR, LIDAR and AIS. A scenario could be that the MASS has registered a weak echo target in high seas which later disappeared. The RCC operator would then be left with camera data to locate an unidentified object in a relatively large area, a task possibly made even more challenging in case of rough seas.

Likewise, the RCC operator is presented with a similar challenge when having to assist in object classification. Considering the available technology for classifying objects, cameras currently seem the most suitable to aid the operator in the classification process. Consequently, the operator relies on a single instrument to classify an object, such as having to distinguish a fishing buoy from a person in the water. Compared to the detection function, however, with classification the RCC operator knows the location of the object which helps reduce the complexity and criticality of the task.

When it comes to responding to failures in the navigation analysis function, risks emerged from the RCC operator(s) potentially having limited knowledge of previous occurrences ("out-of-the-loop" issues). This is due to the RCC operators being required to supervise several MASS at the same time. In comparison, on a conventional vessel the navigator will continuously observe situational cues over time. As such, an RCC operator will have to obtain situational awareness in a much more limited time. This would be particularly challenging in complex traffic situations with close vicinity of several other vessels. Moreover, if the situation requires an immediate action by the RCC operator, the available time would be even more limited.

For navigation analysis, similarities can be seen in a situation where a Captain on a conventional vessel is alerted to the bridge to assist the navigator in assessing a complex traffic situation. However, in such a scenario the Captain would have the navigator available for assistance. The navigator could explain his/hers view of the situation and previous occurrences that might have led to the event. For remote MASS operations, the RCC operator will have to rely on the information available at the moment, or, if part of the concept, use playback functions and logs to examine previous events. The cause(s) of the automated analysis failure, and the reason for why the RCC operator's attention was called for, could be a



further complicating factor. If the cause is a limitation in the MASS capabilities, which the RCC operator is familiar with, this could make the situation more predictable and easier to handle. If the cause is rarer and more difficult to interpret, it could potentially cause the RCC operator to fail in doing the analysis, e.g. if information is unavailable or contains errors.

One of the most critical scenarios is where an action (manoeuvring) failure occurs after object detection and situation analysis have performed successfully by the MASS system. If the MASS is situated in close vicinity to other vessels, the RCC operator(s) finds him or herself in a situation with the least time available, but also the most tasks to do. The RCC operator(s) will then have to detect and classify all the surrounding objects, analyse their intentions and movements, and finally plan and execute the actions required to avoid collision.

Furthermore, it is uncertain how the RCC operator will be performing the direct manoeuvring of the MASS. If the failure is caused by technical/ mechanical issues, the RCC operator may be faced with the similar challenges the MASS system encountered. As such, in many cases, for the operator to take control an override must be made technically possible, e.g. by use of a redundant system for emergency steering. Including this redundancy as part of the automated system could also add another layer of defence.

6.2.3 Limitations in RCCs capabilities to perform supervision

A more 'global' risk emerges from how direct control of one MASS limits the supervision of other parts of the fleet under operation. Being fully or partially occupied with controlling one MASS will demand much of the RCC operator(s) attention until the situation is resolved. During this period, it is uncertain how much supervision is required for the other MASS. This will depend largely on the situation each MASS is in. If 1/3 MASS is experiencing a critical equipment failure, while the two others both are in traffic dense areas, it may not be safe to continue with automated operations. If not properly supported by routines and procedures, in cases where several MASS require simultaneous supervision, the RCC operators are forced to prioritise where monitoring and control is needed the most. Considering that there are only two RCC operators on duty in this study's concept, the capacity limited to one MASS at the time. Consequently, in a worst-case scenario where several MASS require direct control, the RCC operator's capacity would be exceeded.

7 RISK CONTROL OPTIONS (TASK 2. D)

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 sufficient reliability of systems performing navigation functions
- RCO #2 – Ensure sufficient reliability of operator response actions to system failures
- RCO #3 – Ensure sufficient supervision capacity and availability of RCC
- RCO #4 – Ensure sufficient capability for MASS fleet to enter minimum risk conditions

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.

7.1 RCO #1 – Ensure sufficient reliability of systems performing navigation functions

The FTA identified several emerging risks associated with potential unreliability of navigation functions. As discussed in chapter 6.2.1, one of the main risks was scenarios where the MASS system is unaware of having failed to perform a function (e.g. detect an object). While this hazard alone can cause a MASS in automation mode to collide with an object, it also inhibits the RCC operators from responding to system failures by not being provided with a cue (e.g. alarm) to supervise the operation and/or take manual control.

Because successful situation analysis, planning and manoeuvring actions all rely on successful object detection, this function can be considered particularly critical. As long as the object detection function is reliable, or capable of notifying the RCC operators about failures or impaired functionality, the MASS system can either enter an MRC or request manual assistance through human intervention.

Another implication of unreliable functions are the effects it has on the RCCs supervision capacity (see also RCO #3). A higher number of failures will require more active supervision by the RCC operators as a prevention strategy or increase their workload when having to respond to alarms. This will in turn reduce the RCCs capacity to monitor other MASS.

As such, an important RCO is to ensure that the systems performing navigation functions are highly reliable, by RCMs such as:

- Ensure reliability and redundancy by use of several and different types of object detection systems, independent of each other (redundant).
- Choose a combination of object detection systems based on;
 - careful consideration about each technology’s relative capabilities, and
 - how they support RCC operators’ ability to assist in object detection.
- Define criteria (to set notifications/ alarms) for when assistance from RCC operators is required to maintain normal operations.
- Select object detection systems which;
 - are capable of testing and confirming their functionality through self-diagnostics, and
 - have sensors and cameras designed to withstand possible impairments due to environmental conditions (snow, salt, rain etc.).
- Implement principles of “defences-in-depth” to avoid failed navigation due to cyber security breaches.
- Verify that the navigation system can comply with relevant parts of COLREG (see RCM-19).
- Introduce strict protocols and routine for software updates, maintenance and access.
- Perform comprehensive testing of software to confirm reliability both as part of commissioning (e.g. hardware-in-the loop testing) as well as after updates, to verify functionality and absence of failures.

A complete list of RCMs associated with RCO #1 is provided in Table 8.

Table 8 – RCMs associated with RCO #1 targeting the reliability of navigation systems

ID no.	Risk control measures
RCM-01	a) Multiple independent detection systems (e.g. RADAR, LIDAR, AIS, Camera) should be used to provide redundancy and reliable object detection.
	b) Decisions about type and number of detection systems (e.g. RADAR, LIDAR, AIS, Camera) should take into account the effects from failure modes, such as the RCC operator being able to respond to alarms, and/or successfully entering an MRC.
	c) Availability and reliability of object detection systems should be determined based on their relative capabilities, also in case of failures.
	d) Define criteria for when navigation systems is considered to have failed in performing their respective functions (object detection/ classification, situation analysis, planning or action), and for which single or combination of failures manual support from the RCC operators is required (see RCM-09 a) and RCM-18 c) about alarm system).
	e) Define criteria for which object detection system(s) combined with monitoring by RCC operators is sufficient to maintain normal MASS operations (see also RCM-01 d)).

ID no.	Risk control measures
	<p>f) Regular and preventive maintenance of object detection systems (both soft- and hardware).</p> <p>g) Apply a "defenses-in-depth" approach with multiple layers of defense mechanisms to hinder, detect and limit the damage from cyber security breaches. The infrastructure of network components, servers, operator workstations and other endpoints both on board and in the RCC should be hardened to reduce the risk associated with cyber threats. It may also be relevant to assess the cyber security of IT service providers, telecom providers, hosting services, external servers, relay stations, satellites, etc., depending on scope of the project.</p>
RCM-05	<p>a) Each object detection system should be capable of identifying detection failures by comparing the accuracy of weighted object detection measurements performed by other object detection systems.</p> <p>b) Each object detection system should be able to confirm its functionality by performing self-diagnostics.</p>
RCM-10	<p>a) A minimum of two systems shall (separately) have the capability to present information of sufficient quality for the operator to successfully perform object detection and classification in due time (quality may refer to resolution, color depth, framerate, coverage etc.).</p> <p>d) Design of sensors and cameras to take into account possible impairments due to environmental conditions (snow, salt, rain etc.).</p>
RCM-11	<p>a) Perform testing and verification of object classification system's capabilities prior to deployment.</p>
RCM-14	<p>a) The object classification system should be able to automatically generate reliable/verified confidence scores indicating accuracy of object classification.</p>
RCM-16	<p>a) MASS system to be able to comprehend the navigational situation based on a combined evaluation of the object classification data and observations of external environment (wind, current, depth, vessels location, heading and speed etc.). Comprehension includes predicting movements of other vessels to identify potential future dangers to navigation.</p> <p>b) MASS system for situation analysis should incorporate suitable safety margins for any given conditions, including its own capabilities combined with uncertainty estimates for all input data.</p>
RCM-18	<p>a) Define criteria for what is considered successful and failed situational analysis by the MASS system (covered more in detail by RCM-01 d)).</p>
RCM-19	<p>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.</p> <p>b) 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.</p>

ID no.	Risk control measures
RCM-32	a) Strict protocol and routine for software updates, maintenance and access.
	b) Comprehensive testing of software to confirm reliability both as part of commissioning (e.g. hardware-in-the loop testing) as well as after updates, to verify functionality and absence of failures.

7.2 RCO #2 – Ensure sufficient reliability of RCC operators’ response actions to system failures

In cases where a MASS in automation mode performs a navigation failure, the RCC operators provide an additional layer of defence against collisions. This is done by predicting and preventing navigation failures through active supervision, or by responding to (detected) system failures. The FTA identified several emerging risks associated with human failure when performing such tasks (see chapter 6.2.2).

Causes of human error can be found in individual or contextual factors influencing human performance, such as the time available to perform tasks, their complexity, degradation of operators’ skills due to increased automation, confusion about MASS operating modes, or poor quality of training, procedures and routines. As such a second important RCO was to ensure sufficient human reliability by introducing RCMs aimed at the following:

- Equip the RCC with a layout and human-machine interfaces which enable supervision of the entire MASS fleet, also while performing attention-demanding tasks on individual vessels. Interface design (i.e. images) should support the RCC operators in quick comprehension of navigational situations, incl. wind, current, water depths, vessels type, location, heading and speed etc. MASSs which are under manual control should be clearly indicated at all times. Information about key decisions or intentions of MASS in automation mode should be available in due time before they are executed.
- Design a user-friendly alarm system, incl. clear visual and audible alarm presentation, enabled by alarm categorization and prioritization. Notifications and alarms must be tied to thought-through criteria about when human intervention is required, so that the RCC operators are informed in due time and made capable of gaining the situational awareness which is necessary to take action.
- Provide RCC operators with sufficient training in MASS automation capabilities and limitations, including when and how to supervise operations and take manual control. Demanding tasks which are not regularly performed as part of normal operations should be supplemented with realistic training (e.g. by use of simulators) at frequent enough intervals to prevent skill-degradation.

A complete list of RCMs associated with RCO #2 is provided in Table 9.

Table 9 – RCMs associated with RCO #2 targeting the reliability of RCC operators’ actions

ID no.	Risk control measures
RCM-09	a) Ensure a clear visual and audible alarm presentation of system failures, including alarm categorization and prioritization.

ID no.	Risk control measures
	e) Provide RCC operators with training to gain sufficient knowledge about MASS automated capabilities (and limitations).
RCM-10	b) Provide the RCC operators with training in how to perform object detection, classification, situation analysis, planning and implementation of action in case of failures in the various navigation systems (see also RCM-09 e), RCM-15 b) and RCM-24 b)).
	c) Establish routine for the RCC operators to check and confirm presence of other vessels via radio communication in case of degraded object detection and classification systems.
	e) Clear procedures and routines for RCC operators' tasks, roles and responsibilities in case of responding to system failures/ unavailability.
RCM-15	a) Objects should be visually presented (e.g. on HMI) to the operator in a manner which supports human recognition, i.e. clear and unambiguous images or visualizations combined with information about distances.
	b) Provide RCC operator(s) with training in how and when to expect incorrect classification by the system (i.e. knowledge about system limitations and capabilities).
	c) Establish routines and cues (e.g. on HMI) for when the RCC operator(s) is required to actively supervise and assist in object detection, classification, situation analysis and action planning. For object detection and classification this can be aided by a system-generated score of accuracy and machine learning.
RCM-18	b) MASS system to notify RCC operator in due time when its detection, classification, situational analysis, planning and action capabilities have been exceeded (use limits/ levels for notifications, warnings and alarms as cues).
	c) The design of HMI and other visual display units (e.g. camera images) should support RCC operators in quick comprehension of situation, incl. wind, current, water depths, vessels type, location, heading and speed etc. A combination of overview (e.g. AIS) and camera images could be used.
	d) HMI to clearly indicate which situation, and for which MASS, analysis, planning and/ or action has failed.
RCM-21	a) MASS to always inform RCC operator about key decisions/ intentions in due time before they are executed (part of A2-B0 concept).
RCM-24	a) RCC operator to have certified competence as a navigator according to STCW.
	b) Ensure frequent enough training in how to manually control MASS from a remote location as means to prevent skill deterioration and out-of-the-loop task unfamiliarity. Could be by use of simulators for training in how to respond to automation failures, but also by taking manual control during normal operations at scheduled intervals.
	e) HMI to clearly indicate which MASS is being controlled.

7.3 RCO #3 – Ensure sufficient supervision capacity and availability of RCC

The FTA revealed emerging risks at a more systemic level, both with regards to organisational as well as technological aspects. Closely related to the reliability of systems (RCO #1) and operator tasks (RCO #2), is the RCCs availability and capacity to maintain supervision of the MASS fleet. Technological risks included loss of the communication link between the RCC and MASS, insufficient monitoring devices (e.g. displays), and events making the RCC unavailable, such as power outage or fires. Organisational risks included poor routines and procedures for continuous presence of operators in the RCC, manning levels not sufficient to meet demanding peaks in workload, and operator vigilance threatened by longer periods with boredom. A third important RCO is therefore to ensure sufficient supervision capacity and availability of the RCC by introducing RCMs such as:

- Clear procedures and routines for ensuring continuous presence of operators on watch in RCC, for all operational modes, and for all parts of MASS’ voyages.
- Implement strict and clear procedures for how many MASS can be operated in manual mode simultaneously, and when.
- Have an off-duty RCC operator available on-call in case of on-duty RCC operators becoming incapacitated (e.g. sick/ injured), or in case of increase in workload.
- Have a backup RCC workstation in an alternative geographical location and/or a portable device available for essential control of MASS fleet, incl. the possibility to have MASS enter an MRC.
- Design tasks and work shifts in ways which supports operator vigilance and prevents boredom.
- Ensure sufficient redundancy, reliability and availability of both the RCC/ MASS power supplies and communication link to avoid loss of MASS monitoring and control due to single failures.
- Provide RCC operators with a minimum amount of cross-competency to handle critical tasks, such as enabling the RCC engine operator to supervise navigation of a MASS in case the RCC bridge operator is absent or occupied with other tasks.

A complete list of RCMs associated with RCO #3 is provided in Table 10.

Table 10 – RCMs associated with RCO #3 targeting RCC supervision capacity and availability

ID no.	Risk control measures
RCM-09	b) Clear procedures and routines for ensuring continuous presence of operators on watch in RCC, for all operational modes, and for all parts of MASS’ voyages. Consider planning the MASS fleet’s logistics and voyages (incl. speed) in ways which minimize the RCC operators’ workload, and, which in case something should happen, provides enough time to gain sufficient situational awareness – e.g. avoid having several MASS doing port maneuvering at the same time.
	c) Bridge Navigational Watch Alarm System (BNWAS) motion sensor system in RCC to sound an alarm if the watch officer on the bridge of a ship falls asleep, becomes otherwise incapacitated, or is absent for too long a time.

ID no.	Risk control measures
	d) Task design and work shift arrangements to support RCC operator vigilance and "fitness for duty" - e.g. avoid long and/or boring periods (work <i>underload</i>).
RCM-15	d) Provide RCC operator(s) with enough visual display surface area (e.g. a large screen) to simultaneously monitor MASS fleet movements while at the same time support the individual MASS with specific challenges or failures, such as classification of specific objects.
RCM-18	e) MASS system to clearly indicate when information is in-/out of sync, e.g. following a loss of, or delays (latency) in the communication link.
RCM-24	<p>c) Implement strict and clear procedures for how many MASS can be operated in manual mode simultaneously, and when. The allowed number of automated vs. manually operated MASS should be based on;</p> <ul style="list-style-type: none"> - Capacity and workload of RCC operators - MASS capabilities in various operational modes - External conditions, such as environment and traffic density - RCC setup with regards to monitoring capabilities (size/ number of visual displays)
RCM-25	a) Ensure sufficient redundancy, reliability and availability of RCC power supply to avoid loss of MASS monitoring and control due to single failures.
RCM-28	a) Ensure sufficient redundancy, reliability and availability of MASS power supply to avoid loss of MASS monitoring and control due to single failures.
RCM-31	a) Ensure sufficient redundancy, reliability and availability of communication link between MASS and RCC to prevent loss of MASS monitoring and control due to single failures.
RCM-35	b) RCC operators to have valid health certificates to prevent incidents of acute illness while on-duty in RCC.
	c) Off-duty RCC operators to be on-call and in relatively close proximity of RCC as back-up in case assistance is required on a short notice.
RCM-41	a) Have a backup RCC workstation in an alternative geographical location for essential control of MASS fleet, incl. the possibility to have MASS enter an MRC.
	b) Have a portable system available to provide essential control of MASS fleet from outside RCC, incl. the possibility to make a MASS enter an MRC.
RCM-34	a) Operators to have a portable alarm or radio in case having to temporarily leave RCC so he or she quickly be notified to support the operator on watch.
	b) Consider providing (bridge and engine) RCC operators with minimum amount of cross-competency to handle critical tasks, such as enabling the engine operator to supervise navigation of a MASS in case the bridge operator is absent or occupied with other tasks (e.g. manual control over another MASS).

7.4 RCO #4 – Ensure sufficient capability for MASS fleet to enter minimum risk conditions

In case the RCC's supervision capabilities are diminished, it is important that all vessels in the MASS fleet remains in a as safe as possible state. As part of the concept, this is achieved through incorporating the principle of minimum risk conditions (MRC) as part of the design and operational concept (see chapter 4.1.1). The FTA identified several emerging risks which could potentially threaten MASS ability to successfully enter MRCs. This was particularly associated with the RCC being responsible for a number of vessels larger than the number of operators. For example, in case of an incident on one MASS the RCC operator(s) are likely to be pre-occupied with supervising and assisting the affected MASS in entering an MRC. This leaves the other MASS in the fleet partly or fully unsupervised until all operations are restored back to normal, somewhat depending on the actual routines and technology being applied. As such, a fourth important RCO is to ensure sufficient capability for the MASS fleet to enter MRCs, with RCMs such as:

- MRCs to be defined for all critical system failures and external events which can potentially escalate to cause unacceptable impact on the MASS's or other involved vessels' safety, or to the environment, if not dealt with
- Critical events on one MASS automatically triggers the other vessels to also enter an MRC.
- MASS fleet to enter MRC in case RCC becomes unavailable, e.g. due to a blackout.
- Having an emergency stop button in the RCC which puts the entire MASS fleet into an MRC state.

A complete list of RCMs associated with RCO #3 is provided in Table 11.

Table 11 – RCMs associated with RCO # 4 targeting the MASS fleet's capability to enter MRCs

ID no.	Risk control measures
RCM-24	d) Consider whether other MASS in automated mode should enter MRC in case of the RCC operators being occupied with manual operations on another MASS. E.g. a MASS in automated mode may not be allowed to sail unsupervised through areas with high traffic density.
RCM-31	b) All MASS to enter MRC in case of losing communication link or communication of critical information.
RCM-35	a) Consider having a MASS fleet emergency stop button which causes all vessels controlled from RCC to enter an MRC state.
RCM-42	a) MRCs to be defined for all critical system failures and external events which can potentially escalate to cause unacceptable impact on the MASS's or other involved vessels' safety, or to the environment, if not dealt with. Careful considerations should be made regarding MASS dependency on support from RCC operators to enter MRCs. Last Resort MRCs should in principle not solely depend on operator actions to be successful.

8 CONCLUDING REMARKS

Part 2 of the SAFEMASS study highlights the importance of understanding of how functions are allocated between the automated system and the human operator. Figure 20 illustrates how the A2-B0 MASS category performs navigation functions in a normal operating state. The automated system, indicated with blue (full) boxes, performs all functions while the human operator, indicated by half orange/ half grey boxes, performs supervision activities across several vessels.

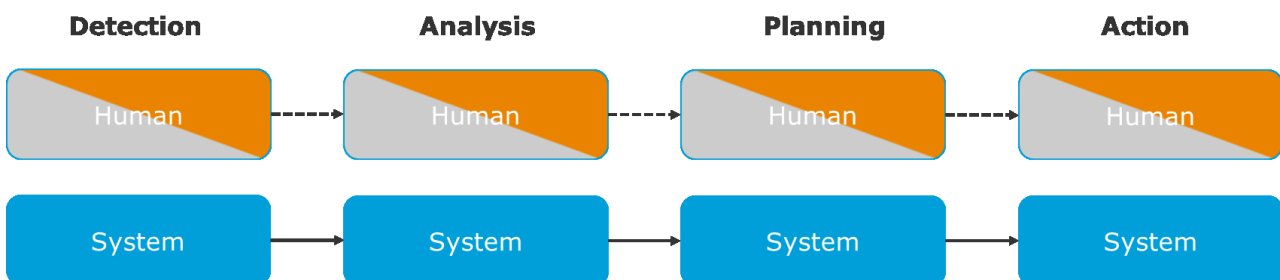


Figure 20 – Allocation of A2-B0 MASS navigation functions in normal operations

One of the rationales behind supervision is the degree of system *unreliability*. Figure 21 illustrates a situation where the automated system has failed in performing an *analysis* to the extent where the human operator intervenes and performs the analysis, before again activating automation mode for the system to carry on with planning and actions. On a MASS, this could be a situation where the identified objects and/ or vessels behaves in a way which exceeds the system’s capability to interpret navigational situations allowing safe planning of further actions. In principle, similar scenarios could be illustrated for failures in all the different functions. A minimum pre-requisite for successful human intervention is that the operator is provided with a cue (e.g. an alarm) which directs his or her attention towards the vessel requiring assistance. If not, the outcome depends on the human operator supervising the affected vessel at the time of the event, possibly by chance, seeing how he or she is responsible for more than one vessel (here: three).

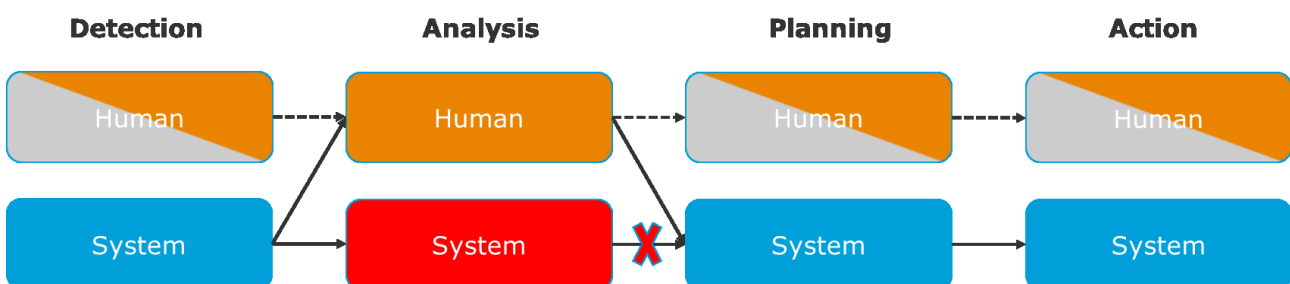


Figure 21 – Allocation of A2-B0 MASS navigation functions in case of analysis failure

The study also argues that the degree and need for reliability and other system properties (e.g. capability and availability) may vary across navigational phases and situations, such as transit, port manoeuvring or abnormal events. This largely depends contextual factors, such as traffic density and environmental conditions (e.g. wind or currents), but also partly on more systemic characteristics such as logistics, routes and voyage planning. For example, if all vessels in a MASS fleet are constantly situated in traffic dense waters, solutions for more continuous supervision of all vessels may be required. In comparison, if most of the voyages consist of transit through areas with little traffic, supervision capacities may be directed towards the vessels requiring the most assistance. As such, an argument can be made that a

MASS design can rarely be better than the Concept of Operations (ConOps) it is based on. For example, during system engineering it may be concluded that the MASS system's capabilities for reliable situation analysis and planning during port manoeuvring are limited, and therefore require operator intervention (see Figure 22). To achieve an optimal design, allocation of functions between the operator and automated system should, to the extent possible, be defined and implemented *a priori* to match operational demands, instead of manifesting itself as ungrateful trouble-shooting tasks for the human to solve during the operational phase.

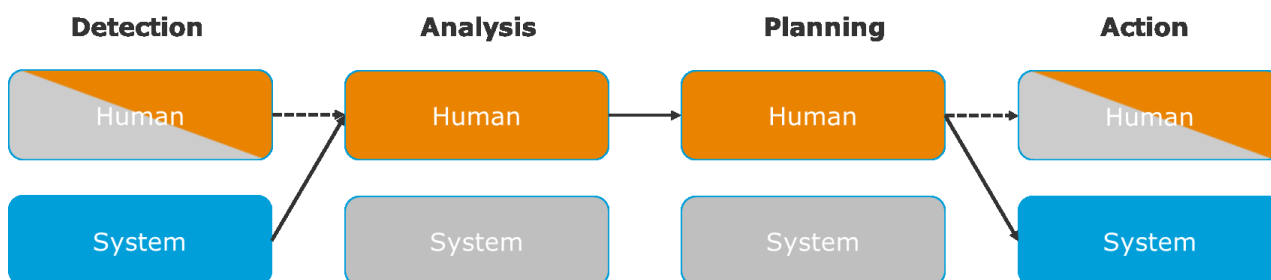


Figure 22 – Analysis and planning functions allocated to the human operator

Such realisations at the design stage opens for the possibility to include several compensating measures. Typical examples include human-machine interfaces being designed to match the task characteristics and demands of active supervision, as well as notifications and alarms being provided to the operator in due time. When having settled on a satisfying design, operational performance can be further improved by use of non-technical measures such as (list not exhaustive):

- Optimizing route planning and logistics to account for RCC supervision capacities.
- Introduce routines for presence of operators in the RCC, at which parts of the voyage vessels require supervision, etc.
- Provide the training required to respond to non-frequent critical system failures.

Lastly, the study provides additional support to several of the conclusions made in Part 1 of SAFEMASS, including:

- Automation is best designed at a system function and operator task level, as opposed to addressing it on a higher vessel level encouraged by commonly communicated Levels of Automation (LoA) models (ref. MSC 100/5/6 described in chapter 4.1).
- Design of automation should take consideration of the demands associated with various operational modes (e.g. transit vs. port manoeuvring), as well as abnormalities such as system failures or external hazards.
- Allocation of functions should be based on a relative comparison of the human's or available technologies' capabilities to (jointly or individually) perform the required functions.

9 REFERENCES

- /1/ EMSA Tender Request: Study of the Risks and Regulatory Issues of Specific Cases of Maritime Autonomous Surface Ships (SAFEMASS). Published 11.02.2019. Tender reference number: EMSA/OP/4/2019.
- /2/ DNV GL (2018) DNVGL-CG-0264 Class Guideline-Autonomous and remotely operated ships. Edition September 2018.
- /3/ ISO 23860 standard on MASS terminology (in progress)
- /4/ IMO (2018). Guidelines for Formal Safety Assessment (FSA) for use in the IMO rule-making process
- /5/ IMO (1972). Convention on the International Regulations for Preventing Collisions at Sea (COLREGs), 1972.
- /6/ 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>

APPENDIX A – SAFEMASS PARTICIPANTS (PART 2)

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 engineering and Integrated Software Dependent Systems (ISDS), Root cause analysis++

Name and position	Role	Expertise
<p>Svein David Medhaug Project Manager</p>	<p>Participant – expert on autonomous ships</p>	<p>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.</p>
<p>Petter Kyseth HSEQ Superintendent</p>	<p>Participant – expert on ship operations and navigation</p>	<p>Petter works as HSEQ Superintendent in Wilhelmsen Ship Management. Petter has previously been working as; Assistant Crew Manager, Captain and Chief Officer.</p>



APPENDIX B – HAZID LOG

ID	Control Room Operator response			Hazard Identification (What if....?)					
	Operator presence	Tasks	Information required	Guideword	Hazardous event	Cause	Consequence	Top event (worst case)	Safety measures
3.0 Bridge-related functions (Voyage) MASS 1, MASS 2 and MASS 3									
3.2 Navigation & Manoeuvring during transit - Collision and grounding avoidance MASS 1, MASS 2 and MASS 3									
Hazard scenario 1: Other ship B on collision course (from SB). However, MASS1 is not able to follow COLREG (give way) because another ship C on SB on same heading and speed and Ship D astern. "Locked-position",									
MASS 1 system response: Successful object detection and classification, collision alarm (CPA and TCPA) sent to operator. System analyse options to handle situation. System next moves to be displayed in remote control centre.									
1	From discontinuous monitoring (RM2) to full monitoring (RM3)	- Acknowledge collision warning alarm on MASS 1, obtain situational awareness and monitor system performance	- Alarm (visual and sound) - Closest Point of Approach (CPA) - Time to Closest Point of Approach (TCPA) - ECDIS, radar, camera, etc.	C1: Check omitted	Operator (Bridge) asleep, does not acknowledge collision alarm	-Task/ job factors (physical working environment, procedures, etc.) - Individual/ person factors (work overload/underload, fatigue, motivation) - Organisation factors (work pressures, manning level, organisational or safety culture, psychosocial working environment, etc.	- Lack of time to analysis and take correct action. - Escalation of situation → increased likelihood of major accident event (collision)	Major accident event: Ship collision → With potential for loss of life	Ensure: - Always more than 1 operator present in room - Sound alarm (collision warning) - Navigational Watch Alarm System (BNWAS), motion sensor system - Sufficient procedures, HMI and "Fit for duty" operator self-assessment - Last resort by ship systems → Minimum Risk Condition (MRC) to be defined for all expected scenarios - Alarm escalation path are defined.
2	From discontinuous monitoring (RM2) to full monitoring (RM3)	- Acknowledge collision warning alarm on MASS 1, obtain situational awareness and monitor system performance	- Closest Point of Approach (CPA) - Time to Closest Point of Approach (TCPA) - ECDIS, radar, camera, etc.	C1: Check omitted	Wrong prioritisation of alarm response	- Poor procedures - Occupied with other tasks - Alarm fatigue - Lack of competence	- Lack of time to analysis and take correct action. - Escalation of situation → increased likelihood of major accident event (collision)	Major accident event: Ship collision → With potential for loss of life	Ensure: - Alarm management philosophy (incl. alarm prioritisation) - See safety measures for ID 1

ID	Control Room Operator response			Hazard Identification (What if....?)					
	Operator presence	Tasks	Information required	Guideword	Hazardous event	Cause	Consequence	Top event (worst case)	Safety measures
3	From discontinuous monitoring (RM2) to full monitoring (RM3)	- Acknowledge collision warning alarm on MASS 1, obtain situational awareness and monitor system performance	- Alarm (visual and sound) - Closest Point of Approach (CPA) - Time to Closest Point of Approach (TCPA) - ECDIS, radar, camera, etc.	C1: Check omitted	Both operators asleep, does not wake up and does not acknowledge alarm, when alarm is given	-Task/ job factors (physical working environment, procedures, etc.) - Individual/ person factors (work overload/underload, fatigue, motivation) - Organisation factors (work pressures, manning level, organisational or safety culture, psychosocial working environment, etc.	- Lack of time to analysis and take correct action. - Escalation of situation → increased likelihood of major accident event (collision)	Major accident event: Ship collision → With potential for loss of life	See safety measures for ID 1
4	From discontinuous monitoring (RM2) to full monitoring (RM3)	- Acknowledge collision warning alarm on MASS 1, obtain situational awareness and monitor system performance	- Closest Point of Approach (CPA) - Time to Closest Point of Approach (TCPA) - ECDIS, radar, camera, etc.	C2: Check incomplete	Lack of time to obtain situational awareness	- Insufficient inf - Complexity of situation - Available response time - Occupied with other tasks -> System gives operator too little time to analyse and act, or; -> Human uses too long time to analyse and act	- Lack of time to analysis and take correct action. - Escalation of situation → increased likelihood of major accident event (collision)	Major accident event: Ship collision → With potential for loss of life	Ensure: - See safety measures for ID 1 - Time needed to obtain situational awareness in collision and grounding scenarios are defined. - Information needed for situational awareness and HMI are defined.
5	RM3 - Full monitoring	- Acknowledge collision warning alarm on MASS 1, obtain situational awareness and monitor system performance	- Closest Point of Approach (CPA) - Time to Closest Point of Approach (TCPA) - ECDIS, radar, camera, etc.	C2: Check incomplete	Operator acknowledge alarm, but does not follow-up, lets the ship continue	Over-confidence in autonomous system performance and ability to handle the situation	- Lack of time to analysis and take correct action. - Escalation of situation → increased likelihood of major accident event (collision)	Major accident event: Ship collision → With potential for loss of life	Ensure: - Operator knows the autonomous system performance capabilities, boundaries and system limitations. - Autonomous system performance capabilities, boundaries and system limitations are defined.

ID	Control Room Operator response			Hazard Identification (What if....?)					
	Operator presence	Tasks	Information required	Guideword	Hazardous event	Cause	Consequence	Top event (worst case)	Safety measures
6	RM3 - Full monitoring	- Communication with conventional ships B/C/D (for MASS 1)	- Closest Point of Approach (CPA) - Time to Closest Point of Approach (TCPA) - ECDIS, radar, camera, etc.	I3: Information communication incomplete	Same hazards as on conventional ship (concerning communication errors and failures)	- Task/ job factors - Individual/ person factors - Organisation factors - External factors - Technical	- Escalation of situation → increased likelihood of major accident event (collision)	Major accident event: Ship collision → With potential for loss of life	Ensure: - Remote control centre is responsible for communication
7	RM3 - Full monitoring	- Manoeuvring MASS 1 (override system)	Navigation functions and systems	A7-Wrong operation on right object	- Lack of ability to correctly manoeuvre the ship	- Inadequate level of seamanship - Unfamiliarity with vessel - Lack of training	- Escalation of situation → increased likelihood of major accident event (collision)	Major accident event: Ship collision → With potential for loss of life	Ensure: - Autonomous system communicates its intentions, not only actions. Operator should supervise the intentions/planning and action. - 'Way of manoeuvring' are defined (manual and/or only change of waypoints, etc.) for operators.
8	RM3 - Full monitoring	- Manoeuvring MASS 1 (override system)	Navigation functions and systems	A7-Wrong operation on right object	- Operator manually changes heading to avoid collision. Takes vessel into 'Manual Mode' → Reduced/lack of supervision of MASS 2 and MASS 3.	- Operator intervention/ override (action) - Operator 100% focused on manoeuvring, requiring full attention.	- May lead to increased risk for other MASS.	Major accident event → With potential for loss of life	Consider: - Only one MASS in Manual Mode at a time. Ensure: - That number of remote controlled MASS match the: 1) Capacity of the operators 2) Capability and limitations of autonomous functions/systems 3) Monitoring possibilities (screens, HMI, etc.)
9	RM3 - Full monitoring	- Manoeuvring MASS 1 (override system)	Navigation functions and systems	A9-Operation incomplete	- Operator change Waypoint to avoid collision. Some attention required. Takes vessel out of planned voyage, but still in auto-mode.	Operator intervention/ override (action)	- Reduced supervision of MASS 2 and MASS 3. - May lead to increased risk for other MASS.	Major accident event → With potential for loss of life	See safety measures in ID 8

ID	Control Room Operator response			Hazard Identification (What if....?)					
	Operator presence	Tasks	Information required	Guideword	Hazardous event	Cause	Consequence	Top event (worst case)	Safety measures
10	RM3 - Full monitoring	- Manoeuvring MASS 1 (override system)	Navigation functions and systems	A8-Operation omitted	Failures related to modes (failure in putting MASS 1 back to 'auto mode' after 'manual mode')	- Task/ job factors - Individual/ person factors - Organisation factors - External factors - Technical	Ship continue on same course	Major accident event: Ship collision → With potential for loss of life	Ensure: - Monitoring screen clearly display 'mode' - Alarms are still active while in manual mode
11	RM3 - Full monitoring	- Manoeuvring MASS 1 (override system)	Navigation functions and systems	A8-Operation omitted	Operator does not monitor vessel after changing waypoint while i auto mode (and other vessel does unexpected movement)	- Overreliance in system - Occupied with other tasks	- Collision alarm, and more time critical situation - Same consequence as 'lack of time hazard'	Major accident event: Ship collision → With potential for loss of life	Ensure: - Situations for operator full attention are defined (until situation is back to 'normal'). - Operator ability to continuously monitor vessel navigational performance and traffic situation - Suitable alarm philosophy (warning, alarm, etc.)
MASS 1 system response: Starts initiating manoeuvre in close vicinity to ship B, C and D (system tries its best to handle situation by manoeuvring)									
12	RM3 - Full monitoring	Monitoring of system performance	Navigation functions and systems	A8-Operation omitted	Operator fail to detect that the ship is doing dangerous manoeuvre	- Overreliance in system - Occupied with other tasks	- Collision alarm, and more time critical situation - Same consequence as 'lack of time hazard'	Major accident event: Ship collision → With potential for loss of life	- Ensure that situations for operator full attention are defined (until situation is back to 'normal'). - Ensure operator ability to continuously monitor vessel navigational performance and traffic situation - Ensure suitable alarm philosophy (warning, alarm, etc.)
Hazard scenario 2: Operator in manual control of MASS 1, while collision alarm on MASS 2 (critical collision situation).									
MASS system response: Collision alarm on MASS 2									
13	RM3 - Full monitoring	Direct control of MASS 1, while monitoring MASS 2 and MASS 3	Navigation functions and systems	C1: Check omitted	Lack of monitoring of MASS 2 and MASS 3	- Occupied with system override MASS 1 - Low manning (only one bridge operator)	Critical situation with all MASS ships	Major accident event → With potential for loss of life	See safety measures in ID 8, 10, 11 and 12
14	RM3 - Full monitoring	Direct control of MASS 1, while monitoring MASS 2 and MASS 3	Navigation functions and systems	A6: Right operation on wrong object (or opposite)	Mixing up situations (correct control on wrong ship)	- Complexity - Stress - Inadequate differentiation of ships - Low manning (only one bridge operator)	Ship collision involving MASS 1 and/or MASS 2	Major accident event → With potential for loss of life	See safety measures in ID 8, 10, 11 and 12

ID	Control Room Operator response			Hazard Identification (What if....?)					
	Operator presence	Tasks	Information required	Guideword	Hazardous event	Cause	Consequence	Top event (worst case)	Safety measures
15	RC3 - Full direct control	Override MASS 1 and MASS 2 at the same time	Navigation functions and systems	A6: Right operation on wrong object (or opposite)	Mixing up situations (wrong control on wrong/correct ship)	- Insufficient capacity to handle two simultaneous critical navigational situations - Complexity - Stress - Low manning (only one bridge operator) - Inadequate differentiation of ships	Critical situation with all MASS ships	Major accident event → With potential for loss of life	See safety measures in ID 8, 10, 11 and 12
16	RC3 - Full direct control	Override MASS 1 and MASS 2 at the same time	Navigation functions and systems	A8-Operation omitted	Too many alarms to handle (alarm fatigue)	- Low manning (only one bridge operator)	Critical situation with all MASS ships	Major accident event → With potential for loss of life	See safety measures in ID 8, 10, 11 and 12
Hazard scenario 3: Remote controlled MASS 1 approach port in high density traffic close in sheltered waters (auto mode).									
17	RM2 - Discontinuous monitoring	System monitoring	Navigation functions and systems	A8-Operation omitted	MASS 1 tries to manoeuvre between sailboats, kayaks, etc. creating hazardous situations.	Ship system limits not fully known → MASS creates dangerous situations	- Less time for operator to detect and avoid collision - Less time for system to plan and go into MRC	Major accident event → With potential for loss of life	- Ensure that when approaching high density areas; full attention mode are defined - Ensure sufficient input for full monitoring; camera/video stream high quality, bandwidth etc.
18	RM2 - Discontinuous monitoring	Situation where operator should override	Navigation functions and systems	A8-Operation omitted	- Operator does not do anything	- Stress - Panic - Freezing - Complexity	- No action by operator - MRC	Major accident event → With potential for loss of life	- Ensure overriding philosophy to be defined
Hazard scenario 4: MASS 1 navigating close to grounding line, affected by strong currents, wind, etc.									

ID	Control Room Operator response			Hazard Identification (What if....?)					
	Operator presence	Tasks	Information required	Guideword	Hazardous event	Cause	Consequence	Top event (worst case)	Safety measures
19	RM2 - Discontinuous monitoring	Monitoring	Navigation functions and systems	A9-Operation incomplete	Deviation from planned route	- Environmental conditions (Sudden high winds, affecting ship)	- Ship goes into MRC (e.g. full ahead/continue - ensure steering speed, etc.), maintain position, etc. - Override possibility	Grounding → With potential for asset damage	- Voyage plan - MRC - Ensure that environmental limitations for system are defined
20	RM3 - Full monitoring	Monitoring	Navigation information	A9-Operation incomplete	Operator override in situation when ship is influenced by strong currents, wind etc.	- Lack of trust in autonomous system - Incomplete situational awareness of MASS decisions	Challenging to remotely 'manual control' MASS, situation may escalate	Grounding → With potential for asset damage	See safety measures in ID 19
21	RM3 - Full monitoring	Monitoring	Navigation information	A9-Operation incomplete	Ship grounding, lack of possibility to detect impact on ship	Remoteness	- Escalation of situation (water ingress) - System performance affected	Grounding → With potential for asset damage	Evaluate need for impact sensor for grounding and collision
Hazard scenario 5: Remote control centre hazards and connectivity									
22	RM1 - Available remote monitoring	Monitoring	Ship status	C2: Check incomplete	Operator of new watch does not arrive in control room, and on duty watch operator need to continue watch	- Stuck traffic - Sick	- Fatigue - Make mistakes	Major accident event → With potential for loss of life	- Watch change procedures - Ensure back-up personnel
23	RM1 - Available remote monitoring	Monitoring	Ship status	C1: Check omitted	Lack of situational awareness during change of watch	Change of operator watch during critical phase in port approach, or when in manual mode	- Erroneous action by operator	Major accident event → With potential for loss of life	- Ensure operator remain on watch until situation is back to normal - Consider minimum "overlap" change of watch time - Ensure formal log of handover

ID	Control Room Operator response			Hazard Identification (What if....?)					
	Operator presence	Tasks	Information required	Guideword	Hazardous event	Cause	Consequence	Top event (worst case)	Safety measures
24	RM1 - Available remote monitoring	Monitoring	Ship status	C1: Check omitted	Operator serious acute health issue (e.g. heart attack), need to leave room	- Health condition - Workload	- No bridge operator to monitor MASS 1, 2 and 3 - Engine operator to handle the operator with illness	Major accident event → With potential for loss of life	- Consider MASS fleet emergency stop button, all MASS to go into MRC. - Ensure more than one bridge operator per remote control centre - Consider cross competency of operators (bride and engine) to extent possible - Ensure no MASS sail un-supervised
25	RM1 - Available remote monitoring	Monitoring	Ship status	C1: Check omitted	Operator away from desk for a long time	- Restroom - Admin tasks	- Lack of situational awareness - Long latency	Major accident event → With potential for loss of life	- Ensure proper procedures (not leave desk in critical situation) - Evaluate if engine operator to alert bridge operator if something happens - Ensure proper communication philosophy and responsibility
26	RM1 - Available remote monitoring	Monitoring	Ship status	R1: Information not obtained	Communication from other ship, when operator is not at desk	Need for communication to handle situations	Less time to handle the situation	Major accident event → With potential for loss of life	See safety measures in ID 25
27	RM1 - Available remote monitoring	Monitoring	Ship status	C1: Check omitted	Operator temporarily health issue or injury (e.g. skin burn from coffee)	- Health condition - Workload	No/reduced monitoring of MASS	Major accident event → With potential for loss of life	- Health certificate
28	RM1 - Available remote monitoring	Monitoring	Ship status	C2: Check incomplete	Wrong focus (mobile phone, tv, talking to others, etc.)	- Poor work environment - Lack of proper procedures	No/reduced monitoring of MASS - Lack of situational awareness	Major accident event → With potential for loss of life	- Procedures

ID	Control Room Operator response			Hazard Identification (What if....?)					
	Operator presence	Tasks	Information required	Guideword	Hazardous event	Cause	Consequence	Top event (worst case)	Safety measures
29	RM1 - Available remote monitoring	Monitoring	Ship status	I1: Information not communicated	Operator monitors the MASS (not knowing that settings are adjusted), leading to critical situation	- Operator on previous watch adjust parameter settings, e.g. due to too many alarms - No proper information given to the new operator.	No/reduced monitoring of MASS - Lack of situational awareness	Major accident event → With potential for loss of life	- Evaluate if operators should be able to customize settings - Ensure safe design and HMI
30	RM1 - Available remote monitoring	Monitoring	Ship status	I3: Information communication incomplete	Misunderstanding of information provided by system	- Too little/much information provided by the system - Poor HMI	Lack of situational awareness to perform monitoring	Major accident event → With potential for loss of life	- Standard display - All screens should have "standard mode"
31	RM1 - Available remote monitoring	Monitoring	Ship status	A9-Operation incomplete	Anticipated mechanical or control/ software failure on MASS	Technical/software failure	Depending on critically, should be able to continue operation	Major accident event → With potential for loss of life	- Component criticality assessment - Redundancy
32	RM1 - Available remote monitoring	Monitoring	Ship status	A9-Operation incomplete	Hidden failure, operator tries to override/ compensate	- Software updates - Maintenance	Reduced performance of MASS	Major accident event → With potential for loss of life	- FMECA - Verification of all software updates
33	RM1 - Available remote monitoring	Monitoring	Ship status	A9-Operation incomplete	Third party interfering (logging into) with the system software on MASS while in operation (sailing)	- Need for system updates (regular and ad-hoc updates)	Reduced performance of MASS	Major accident event → With potential for loss of life	- Ensure procedures of updates and maintenance of control systems (incl. verification, simulations, software/hardware in the loop testing etc.)
34	RM1 - Available remote monitoring	Monitoring	Ship status	A9-Operation incomplete	Third party interfering with the system software on Remote Control system	- Need for system updates (regular and ad-hoc updates)	Reduced performance of MASS	Major accident event → With	- Ensure procedures of updates and maintenance of control systems (incl. verification, simulations, software/hardware in the loop testing etc.)

ID	Control Room Operator response			Hazard Identification (What if....?)					
	Operator presence	Tasks	Information required	Guideword	Hazardous event	Cause	Consequence	Top event (worst case)	Safety measures
								potential for loss of life	
35	RM1 - Available remote monitoring	Monitoring	Ship status	I1: Information not communicated	Loss of ship-shore communications (common cause, affecting all MASS)	- Weather conditions - Technical issue	MASS fleet have possibility to go into MRC (ship should be "self-contained")	Major accident event → With potential for loss of life	- Redundancy in communication equipment - Re-sync systems
36	RM1 - Available remote monitoring	Monitoring	Ship status	I3: Information communication incomplete	Loss of situational awareness, due to: - Information overload - Lack of info	Systems get back online after loss of communication	Lack of ability to make decision about next action	Major accident event → With potential for loss of life	- Ensure that sequence of events that occurred offline should be shown when system gets back online. Must be comprehensible in a short time (no alarm flood). - Alarm and event management
37	RM1 - Available remote monitoring	Monitoring	Ship status	I3: Information communication incomplete	Remote control systems and display is out of sync after communication is lost	Communication lost for various reason	Don't know the system status when monitoring or taking decisions	Major accident event → With potential for loss of life	- System should be designed for loss of communication and re-sync of systems - Safe restart of systems
38	RM1 - Available remote monitoring	Monitoring	Ship status	A9-Operation incomplete	Data overload, connecting issues	- Weather conditions - Technical issue	MASS fleet have possibility to go into MRC (ship should be "self-contained")	Major accident event → With potential for loss of life	-Reduce amount of sensor data to what is needed - Prioritisation of data - Requirements for minimum data amount and latency to keep functions online

ID	Control Room Operator response			Hazard Identification (What if....?)					
	Operator presence	Tasks	Information required	Guideword	Hazardous event	Cause	Consequence	Top event (worst case)	Safety measures
39	RM1 - Available remote monitoring	Monitoring	Ship status	C2: Check incomplete	Control room unavailable (e.g. fire in remote control room)	- Several causes, leading to fire	MASS fleet have possibility to go into MRC (ship should be "self-contained")	Lack of capability to monitor MASS - Major accident event → With potential for loss of life	- Fire prevention and fighting measures in control room - Ensure to define functional requirements for back-up systems - Ensure redundancy in servers, networks, etc. other physical locations - Consider portable systems for minimum functions (stop, pause, safe state for MASS, etc) - Ensure remote control centre and MASS support on technical issues (back-office)
40	RM1 - Available remote monitoring	Monitoring	Ship status	C1: Check omitted	Cyber-attack, sabotage or attempt to take control of MASS	Deliberate sabotage or terror	Other external party in control of MASS	Major accident event → With potential for loss of life	- Ensure cyber security (Prevention and Recovery): Philosophy (standard, test, simulations, etc.) - Operators should have cyber security awareness
41	RM1 - Available remote monitoring	Monitoring	Ship status	C2: Check incomplete	Blue screen, screen freeze, coffee spill	- Accidents - Technical issues	Lack of information to do proper monitoring	Major accident event → With potential for loss of life	- Procedures, design - Multi display - Possibility to switch to other work station
42	RM1 - Available remote monitoring	Monitoring	Ship status	C2: Check incomplete	Navigation training (doing simulations)	Need to build competence	- Occupying operator and station - Potential for working on live system, not "simulations system"	Major accident event → With potential for loss of life	- Consider simulator available in other centre (other location) for larger drills/training) - When On-the-job-training in the Remote Control Centre, ensure clear marking on interfaces.
43	RM1 - Available remote monitoring	Monitoring	Ship status	C1: Check omitted	Operators leaving office	Regular facility fire drills	Lack of ability to monitor MASS	Major accident event → With potential for loss of life	- Procedures (concerning leaving room)

ID	Control Room Operator response			Hazard Identification (What if....?)					
	Operator presence	Tasks	Information required	Guideword	Hazardous event	Cause	Consequence	Top event (worst case)	Safety measures
44	RM1 - Available remote monitoring	Monitoring	Ship status	C1: Check omitted	Multi-tasking (lunch, administration, monitoring MASS)	Operator normal tasks	- Lack of ability to monitor MASS - Safety of MASS reduced (human out of the loop)	Major accident event → With potential for loss of life	- Work load analysis - Cross competence - Procedures - 2nd bridge operator (supervisor)
Hazard scenario 6: Abnormal situations									
45	RM3 - Full monitoring	In control	Ship status	I1: Information not communicated	- Lack of ability to assess severity of damage and compartments affected - Not able to physically observe (vibration, noise) grounding due to being in remote control centre	- Lack of possibility for physical damage assessment	Missing information to perform correct assessment and action	MASS sinking, flooding → Asset damage	- Bilge/flooding detection - Consider sound and vibration detection --grounding detection-- (to enable operator to early initiate MRC, safe state)
46	RM3 - Full monitoring	In control	Ship status	R1: Information not obtained	Operator or MASS not able to confirm severity of impact with small object (kayak, rib, sailboat), e.g. if persons are involved or not., and continue sailing.	Lack of system or operator capability to assess severity of impact and situation understanding.	- Does not initiate SAR operation	- Fatality or injury to third party persons	- Video camera (live stream) and play back functionality - Some systems may detect people in water (infrared) - Call emergency services
47	RM3 - Full monitoring	In control	Ship status	A8-Operation omitted	MASS not able to perform rescue after being involved with Collision, or detecting people in distress	- No crew onboard - Lack of technology / systems to assist	MASS not able to perform rescue (may be able to perform search)	- Fatality or injury to third party persons	- SAR functionality of MASS (unmanned) to be defined

ID	Control Room Operator response			Hazard Identification (What if....?)					
	Operator presence	Tasks	Information required	Guideword	Hazardous event	Cause	Consequence	Top event (worst case)	Safety measures
48	RM3 - Full monitoring	In control	Ship status	R1: Information not obtained	Lack of ability to confirm fire detect onboard	- No crew onboard to physically detect, check, assess	- Delayed firefighting response, or; - Initiating firefighting operation on incorrect basis (leading to equipment damage and loss of ship functionality)	Major accident	- More than one detector and/or different means of detection - CCTV, infrared, etc
49	RM3 - Full monitoring	In control	Ship status	A8-Operation omitted	Inability to extinguish fire	- No crew onboard for manual FF action	Fire escalation	Major accident	- External support available within a certain time - Firefighting means to be evaluated against loss potential
50	RM3 - Full monitoring	In control	Ship status	A8-Operation omitted	Lack of ability to maintain navigation function due to malfunction of equipment in essential systems (propulsion, power generation, etc.)	- Technical failure - Control/software failure	- MASS to handle certain expected failures (robustness of system), also by help of operator - MASS goes into MRC	Major accident	- Ensure system is designed for unmanned operations (built-in robustness, fault-tolerance, automation, etc.)

APPENDIX C – GUIDEWORDS

Table 12 – HAZID guidewords based on the SHERPA taxonomy /6/

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	

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 /4/.

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

FTA ID	Fault tree analysis			Risk control measures		
	Event description	Causes	Accident scenario/ sequence of events	RCM ID	Topics	RCM descriptions
0.0	TOP event: MASS fails in collision avoidance					
1.1.1.1	Loss of RADAR	i. Power failure ii. Hardware failure iii. Software failure (incl. cyber attacks)	-->1.1.1 Loss of detection system --->1.1 MASS system fails to detect object ---->1.0 MASS fails in detection phase ----->0.0 MASS fails in collision avoidance	RCM-01	Loss of single systems should not prevent successful detection of objects.	a) Multiple independent detection systems (e.g. RADAR, LIDAR, AIS, Camera) should be used to provide redundancy and reliable object detection. b) Decisions about type and number of detection systems (e.g. RADAR, LIDAR, AIS, Camera) should take into account the effects from failure modes, such as the RCC operator being able to respond to alarms, and/or successfully entering an MRC. c) Availability and reliability of object detection systems should be determined based on their relative capabilities, also in case of failures. d) Define criteria for when navigation systems is considered to have failed in performing their respective functions (object detection/ classification, situation analysis, planning or action), and for which single or combination of failures manual support from the RCC operators is required (see RCM-09 a) and RCM-18 c) about alarm system). e) Define criteria for which object detection system(s) combined with monitoring by RCC operators is sufficient to maintain normal MASS operations (see also RCM-01 d)). f) Regular and preventive maintenance of object detection systems (both soft- and hardware). g) Apply a "defenses-in-depth" approach with multiple layers of defense mechanisms to hinder, detect and limit the damage from cyber security breaches. The infrastructure of network components, servers, operator workstations and other endpoints both on board and in the RCC should be hardened to reduce the risk associated with cyber threats. It may also be relevant to assess the cyber security of IT service providers, telecom providers, hosting services, external servers, relay stations, satellites, etc , depending on scope of the project.

FTA ID	Fault tree analysis			Risk control measures		
	Event description	Causes	Accident scenario/ sequence of events	RCM ID	Topics	RCM descriptions
1.1.1.2	Loss of LIDAR	i. Power failure ii. Hardware failure iii. Software failure (incl. cyber attacks)	->1.1.1.4 Loss of Camera AND '->1.1.1.3 Loss of AIS AND '->1.1.1.2 Loss of LIDAR AND '->1.1.1.1 Loss of RADAR -->1.1.1 Loss of detection system --->1.1 MASS system fails to detect object ---->1.0 MASS fails in detection phase ----->0.0 MASS fails in collision avoidance	RCM-02	Loss of single systems should not prevent successful detection of objects.	Same as: - RCM-01 a) to f)
1.1.1.3	Loss of AIS	i. Power failure ii. Hardware failure iii. Software failure (incl. cyber attacks)	->1.1.1.4 Loss of Camera AND '->1.1.1.3 Loss of AIS AND '->1.1.1.2 Loss of LIDAR AND '->1.1.1.1 Loss of RADAR -->1.1.1 Loss of detection system --->1.1 MASS system fails to detect object ---->1.0 MASS fails in detection phase ----->0.0 MASS fails in collision avoidance	RCM-03	Loss of single systems should not prevent successful detection of objects.	Same as: - RCM-01 a) to f)
1.1.1.4	Loss of camera	i. Power failure ii. Hardware failure iii. Software failure (incl. cyber attacks)	->1.1.1.4 Loss of Camera AND '->1.1.1.3 Loss of AIS AND '->1.1.1.2 Loss of LIDAR AND '->1.1.1.1 Loss of RADAR -->1.1.1 Loss of detection sensor signal --->1.1 MASS system fails to detect object ---->1.0 MASS fails during the detection phase ----->0.0 MASS fails in collision avoidance	RCM-04	Loss of single systems should not prevent successful detection of objects.	Same as: - RCM-01 a) to f)

FTA ID	Fault tree analysis			Risk control measures		
	Event description	Causes	Accident scenario/ sequence of events	RCM ID	Topics	RCM descriptions
1.1.2.1	Radar fails to detect	i. Poor visibility (fog, rain, snow etc.) ii. Software limitations (insufficient algorithm)	->1.1.2.4 Camera fails to detect AND '->1.1.2.3 AIS fails to detect AND '->1.1.2.2 LIDAR fails to detect AND '->1.1.2.1 RADAR fails to detect -->1.1.2 Sensors fails to detect object --->1.1 MASS system fails to detect object ---->1.0 MASS fails in the detection phase ----->0.0 MASS fails in collision avoidance	RCM-05	Detection failure by a singel system should not prevent successful detection of objects.	Same as: - RCM-01 a) to f) - and in addition; a) Each object detection system should be capable of identifying detection failures by comparing the accuracy of weighted object detection measurements performed by other object detection systems. b) Each object detection system should be able to confirm its functionality by performing self-diagnostics.
1.1.2.2	LIDAR fails to detect	i. Poor visibility (fog, rain, snow etc.) ii. Software limitations (insufficient algorithm)	->1.1.2.4 Camera fails to detect AND '->1.1.2.3 AIS fails to detect AND '->1.1.2.2 LIDAR fails to detect AND '->1.1.2.1 RADAR fails to detect -->1.1.2 Sensors fails to detect object --->1.1 MASS system fails to detect object ---->1.0 MASS fails in the detection phase ----->0.0 MASS fails in collision avoidance	RCM-06	Detection failure by a singel system should not prevent successful detection of objects.	Same as: - RCM-01 a) to f) - RCM-05 a) and b)
1.1.2.3	AIS fails to detect	i. Poor visibility (fog, rain, snow etc.) ii. Software limitations (insufficient algorithm)	->1.1.2.4 Camera fails to detect AND '->1.1.2.3 AIS fails to detect AND '->1.1.2.2 LIDAR fails to detect AND '->1.1.2.1 RADAR fails to detect -->1.1.2 Sensors fails to detect object --->1.1 MASS system fails to detect object ---->1.0 MASS fails in the detection phase ----->0.0 MASS fails in collision avoidance	RCM-07	Detection failure by a singel system should not prevent successful detection of objects.	Same as: - RCM-01 a) to f) - RCM-05 a) and b)

FTA ID	Fault tree analysis			Risk control measures		
	Event description	Causes	Accident scenario/ sequence of events	RCM ID	Topics	RCM descriptions
1.1.2.4	Camera fails to detect	i. Poor visibility (fog, rain, snow etc.) ii. Software limitations (insufficient algorithm)	-->1.1.2.4 Camera fails to detect AND '->1.1.2.3 AIS fails to detect AND '->1.1.2.2 LIDAR fails to detect AND '->1.1.2.1 RADAR fails to detect -->1.1.2 Sensors fails to detect object --->1.1 MASS system fails to detect object ---->1.0 MASS fails in the detection phase ----->0.0 MASS fails in collision avoidance	RCM-08	Detection failure by a single system should not prevent successful detection of objects.	Same as: - RCM-01 a) to f) - RCM-05 a) and b)
1.2.1	Operator fails in identifying MASS system detection failure	i. Insufficient self-diagnostic capabilities of system ii. No or insufficient alarm notification (poor alarm prioritization or categorization, alarm flood etc.) iii. Operator(s) does not investigate alarm (alarm fatigue) iv. Operator distracted, asleep, fatigued or temporary outside RCC, combined with poor routines for providing relief/ support v. Technical failures, such as frozen HMI/ blue screens	-->1.2.1 Operator fails in identifying MASS System detection failure -->1.2 Bridge operator fails to detect object --->1.0 MASS in the detection phase ---->0.0 MASS fails in collision avoidance	RCM-09	RCC operator to be able to identify object detection system failure.	a) Ensure a clear visual and audible alarm presentation of system failures, including alarm categorization and prioritization. Consider planning the MASS fleet's logistics and voyages (incl. speed) in ways which minimize the RCC operators' workload, and, which in case something should happen, provides enough time to gain sufficient situational awareness – e.g. avoid having several MASS doing port maneuvering at the same time. c) Bridge Navigational Watch Alarm System (BNWAS) motion sensor system in RCC to sound an alarm if the watch officer on the bridge of a ship falls asleep, becomes otherwise incapacitated, or is absent for too long a time. d) Task design and work shift arrangements to support RCC operator vigilance and "fitness for duty" - e.g. avoid long and/or boring periods (work underload). e) Provide RCC operator with training to gain sufficient knowledge about MASS automated capabilities (and limitations).

FTA ID	Fault tree analysis			Risk control measures		
	Event description	Causes	Accident scenario/ sequence of events	RCM ID	Topics	RCM descriptions
1.2.2	Operator identifies detection failure, but is unable to detect object	i. Poor visual representation of object (operator interprets alarm as being false) ii. Poor visibility on camera images (rain, fog, snow etc.) iii. Degraded input from sensor (e.g. salt on lenses) iv. Operator(s) have limited surveillance capacity; - low manning/ high workload - other competing tasks, e.g. working with other MASS v. Operator detects wrong object/ vessel vi. Operator going on shift is not informed about object detection alarm (poor handover) vii. Operator fails to contact vessel (assuming the object is a vessel) viii. Operator acknowledges alarm, but does not pursue to resolve it (overreliance in automation and/or alarm fatigue) ix. Information is out of sync following recovery from loss of communication link (see ID 5.1.1.2)	->1.2.2 Operator identifies detection failure, but is unable to detect object -->1.2 Bridge operator fails to detect object --->1.0 MASS fails during the detection phase ---->0.0 MASS fails in collision avoidance	RCM-10	Ensure that RCC operator is able to detect maritime objects.	a) A minimum of two systems shall (seperately) have the capability to present information of sufficient quality for the operator to successfully perform object detection and classification in due time (quality may refer to resolution, color depth, frame-rate, coverage etc.). b) Provide the RCC operators with training in how to perform object detection, classification, situation analysis, planning and implementation of action in case of failures in the various navigation systems (see also RCM-09 e), RCM-15 b) and RCM-24 b)). c) Establish routine for the RCC operators to check and confirm presence of other vessels via radio communication in case of degraded object detection systems. d) Design of sensors and cameras to take into account possible impairments due to environmental conditions (snow, salt, rain etc.). e) Clear procedures and routines for RCC operators' tasks, roles and responsibilities in case of responding to system failures/ unavailability.
2.1.1.1	MASS system is not able to classify object	i. Software limitations (insufficient algorithm or database) ii. Degraded input data from cameras/ sensors (see ID 1.1.2.1 to 1.1.2.4)	->2.1.1.2 Operator fails to classify AND ->2.1.1.1 MASS system is not able to classify object -->2.1.1 Unable to classify --->2.1 Fails in classifying object ---->2.0 Fails in the analysis phase ----->0.0 MASS fails in collision avoidance	RCM-11	MASS system to be able to classify all foreseeable objects potentially posing a danger for navigation	Same as: - RCM-01 d) - and in addition; a) Perform testing and verification of object classification system's capabilities prior to deployment.

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	Operator is unaware of system not being able to classify	i. Insufficient self-diagnostic capabilities of system ii. No or insufficient alarm notification (poor alarm prioritization or categorization, alarm flood etc.) iii. Operator(s) does not investigate alarm (alarm fatigue) iv. Operator distracted, asleep, fatigued or temporary outside RCC, combined with poor routines for providing relief/ support v. Technical failures, such as frozen HMI/ blue screens	-->2.1.1.2.1 Operator Is unaware of system not being able to classify -->2.1.1.2 Operator fails to classify AND -->2.1.1.1 MASS system is not able to classify object --->2.1 Unable to classify ---->2.1 Fails in classifying object ----->2.0 Fails in the analysis phase ----->0.0 MASS fails in collision avoidance	RCM-12	RCC operator to be able to identify object classification system failure.	Same as: - RCM-09 a) to e)
2.1.1.2.2	Operator identifies classification failure, but is unable to classify object	i. Poor visual representation of object (e.g. on HMI) ii. Poor visibility on camera images (rain, fog, snow etc.) iii. Degraded input from sensor (e.g. salt on lenses) iv. Operator(s) have limited surveillance capacity; - low manning/ high workload - other competing tasks, e.g. working with other MASS v. Operator classifies wrong object/ vessel vi. Operator going on shift is not informed about object classification alarm (poor handover) vii. Operator fails to contact vessel (assuming the object is a vessel) viii. Operator acknowledges alarm, but does not pursue to resolve it (e.g. due to	-->2.1.1.2.2 Operator identifies classification failure, but is unable to classify object -->2.1.1.2 Operator fails to classify AND -->2.1.1.1 MASS system is not able to classify object --->2.1 Unable to classify ---->2.1 Fails in classifying object ----->2.0 Fails in the analysis phase ----->0.0 MASS fails in collision avoidance	RCM-13	Ensure that RCC operator is able to classify maritime objects.	Same as: - RCM-10 a) to c) and e).

Fault tree analysis				Risk control measures		
FTA ID	Event description	Causes	Accident scenario/ sequence of events	RCM ID	Topics	RCM descriptions
		overreliance in automation and/or alarm fatigue) ix. Information is out of sync following recovery from loss of communication link (see ID 5.1.1.2)				
2.1.2.1	MASS system performs incorrect classification of object	i. Software limitations (insufficient algorithm or database) ii. Degraded input data from cameras/ sensors (see ID 1.1.2.1 to 1.1.2.4) iii. Insufficient self-diagnostic capabilities of object classification system	'->2.1.2.2 Operator fails to identify incorrect classification AND ->2.1.2.1 MASS system performs incorrect classification of object -->2.1.1 Unable to classify --->2.1 Fails in classifying object ---->2.0 Fails in the analysis phase ----->0.0 MASS fails in collision avoidance	RCM-14	Ensure sufficient reliability of object classification system.	a) The object classification system should be able to automatically generate reliable/verified confidence scores indicating accuracy of object classification.

FTA ID	Fault tree analysis			Risk control measures		
	Event description	Causes	Accident scenario/ sequence of events	RCM ID	Topics	RCM descriptions
2.1.2.2	Operator fails to identify incorrect classification	i. Operator not presented with cue (warning or alarm) ii. Operator(s) have limited surveillance capacity; - low manning/ high workload - other competing tasks, e.g. working with other MASS iii. Operator distracted, asleep, fatigued or temporary outside RCC, combined with poor routines for providing relief/ support iv. Limitations in the number and surface area of visual display units used for vessel and traffic monitoring v. Poor routines for monitoring unalarmed events	'->2.1.2.2 Operator fails to identify incorrect classification AND ->2.1.2.1 MASS system performs incorrect classification of object -->2.1.1 Unable to classify --->2.1 Fails in classifying object ---->2.0 Fails in the analysis phase ----->0.0 MASS fails in collision avoidance	RCM-15	MASS system to be able to classify all foreseeable objects potentially posing a danger for navigation	a) Objects should be visually presented (e.g. on HMI) to the operator in a manner which supports human recognition, i.e. clear and unambiguous images or visualizations combined with information about distances. b) Provide RCC operator(s) with training in how and when to expect incorrect classification by the system (i.e. knowledge about system limitations and capabilities). c) Establish routines and cues (e.g. on HMI) for when the RCC operator(s) is required to actively supervise and assist in object detection, classification, situation analysis and action planning. For object detection and classification this can be aided by a system-generated score of accuracy and machine learning. d) Provide RCC operator(s) with enough visual display surface area (e.g. a large screen) to simultaneously monitor MASS fleet movements while at the same time support the individual MASS with specific challenges or failures, such as classification of specific objects.
2.2.1	MASS system fails in situation analysis	i. Software limitations (insufficient algorithm or database) ii. Degraded input data from cameras/ sensors (see ID 1.1.2.1 to 1.1.2.4) iii. Applies incorrect object classification (see ID 2.1.2.1)	'->2.2.2 Operator fails in situation analysis AND ->2.2.1 MASS system fails in situation analysis -->2.2 Fails in situation analysis --->2.0 Fails the analysis phase ---->0.0 MASS fails in collision avoidance	RCM-16	MASS system to be able to analyse navigational situations (e.g to some degree COLREG compliant).	Same as: - RCM-01 d) - and in addition; a) MASS system to be able to comprehend the navigational situation based on a combined evaluation of the object classification data and observations of external environment (wind, current, depth, vessels location, heading and speed etc.). Comprehension includes predicting movements of other vessels to identify potential future dangers to navigation. b) MASS system for situation analysis should incorporate suitable safety margins for any given conditions, including its own capabilities combined with uncertainty estimates for all input data.
2.2.2.1	Operator fails to identify situation analysis failure	i. Insufficient self-diagnostic capabilities of system ii. No or insufficient alarm notification (poor alarm prioritization or categorization, alarm flood etc.) iii. Operator(s) does not investigate alarm (alarm fatigue) iv. Operator distracted,	->2.2.2.1 Operator fails to identifying situation analysis failure -->2.2.2 Operator fails in situation analysis AND -->2.2.1 MASS system fails in situation analysis --->2.2 Fails in situation analysis ---->2.0 Fails in the analysis phase ----->0.0 MASS fails in collision avoidance	RCM-17	Operator to be able to identify and analyse navigational situations.	Same as: - RCM-09 a) to e)

	Fault tree analysis			Risk control measures		
FTA ID	Event description	Causes	Accident scenario/ sequence of events	RCM ID	Topics	RCM descriptions
		asleep, fatigued or temporary outside RCC, combined with poor routines for providing relief/ support v. Technical failures, such as frozen HMI/ blue screens				

FTA ID	Fault tree analysis			Risk control measures		
	Event description	Causes	Accident scenario/ sequence of events	RCM ID	Topics	RCM descriptions
2.2.2.2	Operator identifies failure, but is unable to perform a correct analysis of the situation	<p>i. Task complexity (several objects/ vessels, unpredictable movements, external environment etc.)</p> <p>ii. Poor visibility on camera images (rain, fog, snow etc.)</p> <p>iii. Poor visual representation of situation (on HMIs)</p> <p>iv. Operator lacks sensory perception input due to not being physically present (e.g. orientation, sense of speed, heading etc.)</p> <p>v. Operator(s) have limited analysis capacity;</p> <p>- low manning/ high workload</p> <p>- other competing tasks, e.g. working with other MASS</p> <p>vi. Operator has limited time available to analyse situation (too late warning/ alarm)</p> <p>vii. Operator analyse wrong situation/ situation for another MASS</p> <p>viii. Operator acknowledges alarm, but does not pursue to resolve it</p> <p>- over(-reliance) in automation</p> <p>- does not perceive situation as critical/ misinterpretation</p> <p>ix. Operator going on shift is not informed about situation analysis failure alarm (poor handover)</p> <p>x. Information is out of sync following recovery from loss of communication link-> may cause mode confusion (see ID 5.1.1.2)</p>	<p>-->2.2.2.2 Operator identifies failure, but is unable to perform a correct analysis of the situation</p> <p>-->2.2.2 Operator fails in situation analysis AND</p> <p>-->2.2.1 MASS system fails in situation analysis</p> <p>--->2.2 Fails in situation analysis</p> <p>---->2.0 Fails in the analysis phase</p> <p>----->0.0 MASS fails in collision avoidance</p>	RCM-18	Enable operators to quickly achieve situational awareness.	<p>Same as:</p> <p>- RCM-10 d) and e)</p> <p>- RCM-15 c)</p> <p>- and in addition;</p> <p>a) Define criteria for what is considered successful and failed situational analysis by the MASS system (covered more in detail by RCM-01 d)).</p> <p>b) MASS system to notify RCC operator in due time when its detection, classification, situational analysis, planning and action capabilities have been exceeded (use limits/ levels for notifications, warnings and alarms as cues).</p> <p>c) The design of HMI and other visual display units (e.g. camera images) should support RCC operators in quick comprehension of situation, incl. wind, current, water depths, vessels type, location, heading and speed etc. A combination of overview (e.g. AIS) and camera images could be used.</p> <p>d) HMI to clearly indicate which situation, and for which MASS, analysis, planning and/ or action has failed.</p> <p>e) MASS system to clearly indicate when information is in-/out of sync, e.g. following a loss of, or delays (latently) in the communication link.</p>

Fault tree analysis				Risk control measures		
FTA ID	Event description	Causes	Accident scenario/ sequence of events	RCM ID	Topics	RCM descriptions
		xi. Overload of information when system returns online after broken communication link is re-established				

FTA ID	Fault tree analysis			Risk control measures		
	Event description	Causes	Accident scenario/ sequence of events	RCM ID	Topics	RCM descriptions
3.1	MASS system fails in action planning	i. Software limitations (insufficient algorithm or database) ii. Degraded/ incorrect input data from situation analysis system (see ID 2.2.1) iii. Operator performs error after (incorrectly) overriding system due to distrust in automation	-->3.2 Operator fails in action planning AND -->3.1 MASS system fails in action planning -->3.0 Fails in action planning phase --->0.0 MASS fails in collision avoidance	RCM-19	MASS system to be able to plan action to avoid collision (e.g. to some degree COLREG compliant)	Same as: - RCM-01 d) - and in addition; 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 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.
3.2.1	Operator fails in identifying MASS action planning failure	i. Insufficient self-diagnostic capabilities of system ii. No or insufficient alarm notification (poor alarm prioritization or categorization, alarm flood etc.) iii. Operator(s) does not investigate alarm (alarm fatigue) iv. Operator distracted, asleep, fatigued or temporary outside RCC, combined with poor routines for providing relief/ support v. Technical failures, such as frozen HMI/ blue screens	-->3.2.1 Operator fails in identifying MASS action planning failure -->3.2 Operator fails in action planning AND -->3.1 MASS system fails in action planning --->3.0 Fails in action planning phase ---->0.0 MASS fails in collision avoidance	RCM-20	Operator to be able to identify poor action planning conducted by MASS	Same as: - RCM-09 a) to e)

Fault tree analysis				Risk control measures		
FTA ID	Event description	Causes	Accident scenario/ sequence of events	RCM ID	Topics	RCM descriptions
3.2.2	Operator identifies failure, but is unable to perform correct action planning	i. Poor or incorrect situational analysis (see ID 2.2.1 and 2.2.2.1) ii. Operator plans for wrong situation (i.e. situation for another MASS) iii. Operator acknowledges alarm, but does not pursue to resolve it - over(-reliance) in automation - does not perceive planning as critical/ misinterpretation iv. Operator(s) have limited planning capacity; - low manning/ high workload - other competing tasks, e.g. working with other MASS v. Operator going on shift is not informed about planning failure alarm (poor handover)	`->3.2.2 Operator identifies failure, but is unable to perform correct action planning -->3.2 Operator fails in action planning AND -->3.1 MASS system fails in action planning --->3.0 Fails in action planning phase ---->0.0 MASS fails in collision avoidance	RCM-21	Operator to be able to plan action to avoid collision	Same as: - RCM-01 d) - RCM-15 c) - RCM-18 a), b) and d) - and in addition; a) MASS to always inform RCC operator about key decisions/ intentions in due time before they are executed (part of A2-B0 concept)
4.1	MASS system fails in action	i. Incorrect planning by MASS system (see ID 3.1) ii. Operator performs error after deliberately overriding system due to; - distrust in automation - limitations in MASS capabilities - operator trying to compensate for hidden/ latent failures (mode confusion) iii. Operator fails to re-instate automated mode after taking control in manual mode (e.g. due to poor handover) iv. Technical failures such as with propulsion, steering etc. (similar as for conventional	-->4.2 Operator fails in action AND -->4.1 MASS system fails in action (Technical issues) -->4.0 Fails in Action phase ---->0.0 MASS fails in collision avoidance	RCM-22		Same as: - RCM-01 d) - and in addition; - RCM-19 a) and b)

FTA ID	Fault tree analysis			Risk control measures		
	Event description	Causes	Accident scenario/ sequence of events	RCM ID	Topics	RCM descriptions
		vessels) v. Cyber attack (sabotage) takes control of MASS				
4.2.1	Operator fails in identifying MASS action failure	i. Insufficient self-diagnostic capabilities of system ii. No or insufficient alarm notification (poor alarm prioritization or categorization, alarm flood etc.) iii. Operator(s) does not investigate alarm (alarm fatigue) iv. Operator distracted, asleep, fatigued or temporary outside RCC, combined with poor routines for providing relief/ support v. Technical failures, such as frozen HMI/ blue screens	->4.2.1 Operator fails in identifying MASS action failure -->4.2 Operator fails in action AND -->4.1 MASS system fails in action (Technical issues) --->4.0 Fails in Action phase ---->0.0 MASS fails in collision avoidance	RCM-23	Operator to be able to identify incorrect action conducted by MASS	Same as: - RCM-09 a) to e)
4.2.2	Operator identifies action failure, but is unable to perform correct action in time	i. Insufficient planning (see ID 3.2.2) ii. Operator(s) have limited intervention capacity; - low manning/ high workload - other competing tasks, e.g. working with other MASS iii. Operator acknowledges alarm, but does not pursue to resolve it (overreliance in automation and/or alarm	->4.2.2 Operator identifies action failure, but is unable to perform correct action in time -->4.2 Operator fails in action AND -->4.1 MASS system fails in action (Technical issues) --->4.0 Fails in Action phase ---->0.0 MASS fails in collision avoidance	RCM-24	Operator to be able to conduct action to avoid collision	Same as: - RCM-15 c) - RCM-18 a), b) and d) - and in addition; a) RCC operator to have certified competence as a navigator according to STCW. b) Frequent enough training in how to manually control MASS from a remote location as means to prevent skill deterioration and out-of-the-loop task unfamiliarity. Could be by use of simulators for trainin in how to respond to automation failures, but also by taking manual control during normal operations at scheduled intervals. c) Implement strict and clear procedures for how many MASS can be operated in

Fault tree analysis				Risk control measures		
FTA ID	Event description	Causes	Accident scenario/ sequence of events	RCM ID	Topics	RCM descriptions
		fatigue) iv. HMI, visual display units and controls does not support complexity of task; - Accurate maneuvering and navigation, incl. position of own and other vessels - Awareness of environmental condition (wind, current, speed etc.) v. Operator unaware of/ applies incorrect automation mode (mode confusion) vi. Operator lacks skills to take control due to infrequent manual operations/ insufficient training (skill deterioration) vii. Stressors causes operator to trust automation over own skillset viii. Third party influences MASS performance, e.g. software updates ix. Operator intervenes to take action on wrong MASS				manual mode simultaneously, and when. The allowed number of automated vs. manually operated MASS should be based on; - Capacity and workload of RCC operators - MASS capabilities in various operational modes - External conditions, such as environment and traffic density - RCC setup with regards to monitoring capabilities (size/ number of visual displays) d) Consider whether other MASS in automated mode should enter MRC in case of the RCC operators being occupied with manual operations on another MASS. E.g. a MASS in automated mode may not be allowed to sail unsupervised through areas with high traffic density. e) HMI to clearly indicate which MASS is being controlled.

Fault tree analysis				Risk control measures		
FTA ID	Event description	Causes	Accident scenario/ sequence of events	RCM ID	Topics	RCM descriptions
5.1.1.1.1.1	Loss of main power supply to RCC	i. Loss of power from grid ii. Misc. hardware failure (e.g circuit boards, cables etc.)	->5.1.1.1.1.3 Loss of UPS for RCC equipment AND '->5.1.1.1.1.2 Loss of secondary power supply to RCC AND '->5.1.1.1.1.1 Loss of main power supply to RCC '-->5.1.1.1.1 Loss of power in RCC '--->5.1.1.1 Loss of power ---->5.1.1 Loss of connection due to technical issues ----->5.2 MASS fails to go in MRC AND ----->5.1 Loss of RCC supervision capability ----->5.0 MASS fails due to loss of RCC supervision capability ----->0.0 MASS fails in collision avoidance	RCM-25	RCC to have available power to be operational during abnormal conditions	a) Ensure sufficient redundancy, reliability and availability of RCC power supply to avoid loss of MASS monitoring and control due to single failures.
5.1.1.1.1.2	Loss of secondary power supply to RCC	i. Loss of power from grid ii. Misc. hardware failure (e.g circuit boards, cables etc.)	->5.1.1.1.1.3 Loss of UPS for RCC equipment AND '->5.1.1.1.1.2 Loss of secondary power supply to RCC AND '->5.1.1.1.1.1 Loss of main power supply to RCC '-->5.1.1.1.1 Loss of power in RCC '--->5.1.1.1 Loss of power ---->5.1.1 Loss of connection due to technical issues ----->5.2 MASS fails to go in MRC AND ----->5.1 Loss of RCC supervision capability ----->5.0 MASS fails due to loss of RCC supervision capability ----->0.0 MASS fails in collision avoidance	RCM-26	RCC to have available power to be operational during abnormal conditions	Same as: - RCM-25 a)

		Fault tree analysis		Risk control measures		
FTA ID	Event description	Causes	Accident scenario/ sequence of events	RCM ID	Topics	RCM descriptions
5.1.1.1.1.3	Loss of UPS to RCC equipment	i. Misc. hardware failure (e.g circuit boards, cables etc.)	->5.1.1.1.1.3 Loss of UPS for RCC equipment AND '->5.1.1.1.1.2 Loss of secondary power supply to RCC AND '->5.1.1.1.1.1 Loss of main power supply to RCC '-->5.1.1.1.1 Loss of power in RCC '--->5.1.1.1 Loss of power ---->5.1.1 Loss of connection due to technical issues ---->5.2 MASS fails to go in MRC AND ---->5.1 Loss of RCC supervision capability ---->5.0 MASS fails due to loss of RCC supervision capability ----->0.0 MASS fails in collision avoidance	RCM-27	RCC to have sufficient redundancy to maintain operation during power loss	Same as: - RCM-25 a)
5.1.1.1.2.1	Loss of main power supply on MASS	i. Misc. hardware failure (e.g circuit boards, cables etc.) - as for conventional vessels.	->5.1.1.1.2.3 Loss of UPS for MASS equipment AND '->5.1.1.1.2.2 Loss of secondary power supply on MASS AND '->5.1.1.1.2.1 Loss of main power supply on MASS '-->5.1.1.2 Loss of power on MASS '--->5.1.1 Loss of power ---->5.1.1 Loss of connection due to technical issues ---->5.2 MASS fails to go in MRC AND ---->5.1 Loss of RCC supervision capability ---->5.0 MASS fails due to loss of RCC supervision capability ----->0.0 MASS fails in collision avoidance	RCM-28	RCC to have sufficient redundancy to maintain operation during power loss	a) Ensure sufficient redundancy, reliability and availability of MASS power supply to avoid loss of MASS monitoring and control due to single failures.

Fault tree analysis				Risk control measures		
FTA ID	Event description	Causes	Accident scenario/ sequence of events	RCM ID	Topics	RCM descriptions
5.1.1.1.2.2	Loss of secondary power supply on MASS	i. Misc. hardware failure (e.g circuit boards, cables etc.) - as for conventional vessels.	->5.1.1.1.2.3 Loss of UPS for MASS equipment AND '->5.1.1.1.2.2 Loss of secondary power supply on MASS AND '->5.1.1.1.2.1 Loss of main power supply on MASS '-->5.1.1.1.2 Loss of power on MASS '--->5.1.1.1 Loss of power ---->5.1.1 Loss of connection due to technical issues ----->5.2 MASS fails to go in MRC AND ----->5.1 Loss of RCC supervision capability ----->5.0 MASS fails due to loss of RCC supervision capabilit ----->0.0 MASS fails in collision avoidance	RCM-29	RCC to have sufficient redundancy to maintain operation during power loss	Same as: - RCM-28 a)
5.1.1.1.2.3	Loss of UPS for MASS equipment	i. Misc. hardware failure (e.g circuit boards, cables etc.) - as for conventional vessels.	->5.1.1.1.2.3 Loss of UPS for MASS equipment AND '->5.1.1.1.2.2 Loss of secondary power supply on MASS AND '->5.1.1.1.2.1 Loss of main power supply on MASS '-->5.1.1.1.2 Loss of power on MASS '--->5.1.1.1 Loss of power ---->5.1.1 Loss of connection due to technical issues ----->5.2 MASS fails to go in MRC AND ----->5.1 Loss of RCC supervision capability ----->5.0 MASS fails due to loss of RCC supervision capabilit ----->0.0 MASS fails in collision avoidance	RCM-30	MASS to have sufficient redundancy to operate essential equipment during power loss	Same as: - RCM-28 a)

FTA ID	Fault tree analysis			Risk control measures		
	Event description	Causes	Accident scenario/ sequence of events	RCM ID	Topics	RCM descriptions
5.1.1.2	Loss of communication link	i. Loss of satellite/cellular connection	->5.1.1.2 Loss of communication link -->5.1.1 Loss of connection due to technical issues --->5.2 MASS fails to go in MRC AND --->5.1 Loss of RCC supervision capability ---->5.0 MASS fails due to loss of RCC supervision capabilit ----->0.0 MASS fails in collision avoidance	RCM-31	MASS to have sufficient redundancy to operate essential equipment during communication loss	a) Ensure sufficient redundancy, reliability and availability of communication link between MASS and RCC to prevent loss of MASS monitoring and control due to single failures. b) All MASS to enter MRC in case of losing communication link or communication of critical information.
5.1.1.3	Software issues (system failure, freezing etc)	i. Software freeze/ error ii. Software maintenance (untimely updates)	->5.1.1.3 Software issues (system failure, freezing etc) -->5.1.1 Loss of connection due to technical issues --->5.2 MASS fails to go in MRC AND --->5.1 Loss of RCC supervision capability ---->5.0 MASS fails due to loss of RCC supervision capabilit ----->0.0 MASS fails in collision avoidance	RCM-32	Reliable software to be installed and tested	a) Strict protocol and routine for software updates, maintenance and access. b) Comprehensive testing of software to confirm reliability both as part of commissioning (e.g. hardware-in-the loop testing) as well as after updates, to verify functionality and absence of failures.
5.1.1.4	Loss of navigational sensor data input to RCC	i. Loose/ damaged cables ii. Software failures iii. Communication link issues	->5.1.1.4 Loss of navigational sensor data input to RCC -->5.1.1 Loss of connection due to technical issues --->5.2 MASS fails to go in MRC AND --->5.1 Loss of RCC supervision capability ---->5.0 MASS fails due to loss of RCC supervision capabilit ----->0.0 MASS fails in collision avoidance	RCM-33	MASS to have sufficient redundancy to operate essential equipment during communication loss	Same as: - RCM-31 a) and b) - RCM-32 a) and b)

Fault tree analysis				Risk control measures		
FTA ID	Event description	Causes	Accident scenario/ sequence of events	RCM ID	Topics	RCM descriptions
5.1.2.1.1.1	Bridge operator leaves do to necessities	i. Toilet brakes ii. Meal brakes iii. Admin tasks iv. Private matters	->5.1.2.1.1.1 Bridge operator leaves do to necessities (toilet brakes, lunch etc) '--> 5.1.2.1.2 Engine operator leaves workstation AND '-->5.1.2.1.1 Bridge operator leaves workstation '--->5.1.2.1 No operators supervising Bridge workstation during normal operations ---->5.1.2 Loss of connection due to physical absence ---->5.2 MASS fails to go in MRC AND ---->5.1 Loss of RCC supervision capability ----->5.0 MASS fails due to loss of RCC supervision capabilit ----->0.0 MASS fails in collision avoidance	RCM-34	Workstation to never be left unattended	Same as: - RCM-09 b) - and in addition; a) Operators to have a portabel alarm or radio in case having to temporarily leave RCC so he or she quickly be notified to support the operator on watch. b) Consider providing (bridge and engine) RCC operators with minimum amount of cross-competency to handle critical tasks, such as enabling the engine operator to supervise navigation of a MASS in case the bridge operator is absent or occupied with other tasks (e.g. manual control over another MASS).
5.1.2.1.1.2	Bridge operator leaves due to acute medical episode	i. Serious health issues ii. Accident at work	->5.1.2.1.1.2 Bridge operator leaves do to acute medical episode '--> 5.1.2.1.2 Engine operator leaves workstation AND '-->5.1.2.1.1 Bridge operator leaves workstation '--->5.1.2.1 No operators supervising Bridge workstation during normal operations ---->5.1.2 Loss of connection due to physical absence ---->5.2 MASS fails to go in MRC AND ---->5.1 Loss of RCC supervision capability ----->5.0 MASS fails due to loss of RCC supervision capabilit ----->0.0 MASS fails in collision avoidance	RCM-35	Acute medical episodes not to compromise SAFE MASS operation	Same as: - RCM-09 b) - RCM-34 a) and b) a) Consider having a MASS fleet emergency stop button which causes all vessels controlled from RCC to enter a MRC state. b) RCC operators to have valid health certificates to prevent incidents of acute illness while on-duty in RCC. c) Off-duty RCC operators to be on-call and in relatively close proximity of RCC as back-up in case assistance is required on a short notice.

Fault tree analysis				Risk control measures		
FTA ID	Event description	Causes	Accident scenario/ sequence of events	RCM ID	Topics	RCM descriptions
5.1.2.1.1.3	Bridge operator leaves workstation due to lack of motivation, boredom etc. (violation)	i. Poor psychosocial working environment (balance between work demands, control and support, e.g. long and quiet periods causing boredom) ii. Poor work culture and routines	->5.1.2.1.1.3 Bridge operator leaves workstation due to lack of motivation, boredom etc. (violation) '--> 5.1.2.1.2 Engine operator leaves workstation AND '-->5.1.2.1.1 Bridge operator leaves workstation '--->5.1.2.1 No operators supervising Bridge workstation during normal operations ---->5.1.2 Loss of connection due to physical absence ----->5.2 MASS fails to go in MRC AND ----->5.1 Loss of RCC supervision capability ----->5.0 MASS fails due to loss of RCC supervision capabilit ----->0.0 MASS fails in collision avoidance	RCM-36	RCC operator to be present at workstation	Same as: - RCM-09 b) and d)
5.1.2.1.2.1	Engine operator leaves do to necessities	i. Toilet brakes ii. Meal brakes	->5.1.2.1.2.1 Engine operator leaves do to necessities (toilet brakes, lunch etc) '--> 5.1.2.1.2 Engine operator leaves workstation AND '-->5.1.2.1.1 Bridge operator leaves workstation '--->5.1.2.1 No operators supervising Bridge workstation during normal operations ---->5.1.2 Loss of connection due to physical absence ----->5.2 MASS fails to go in MRC AND ----->5.1 Loss of RCC supervision capability ----->5.0 MASS fails due to loss of RCC supervision capabilit ----->0.0 MASS fails in collision avoidance	RCM-37	Workstation to never be left unattended	Same as: - RCM-09 b) - RCM-34 a) and b)

Fault tree analysis				Risk control measures		
FTA ID	Event description	Causes	Accident scenario/ sequence of events	RCM ID	Topics	RCM descriptions
5.1.2.1.2.2	Engine operator leaves do to acute medical episode	i. Serious health issues ii. Accident at work	->5.1.2.1.2.2 Engine operator leaves do to acute medical episode '--> 5.1.2.1.2 Engine operator leaves workstation AND '-->5.1.2.1.1 Bridge operator leaves workstation '--->5.1.2.1 No operators supervising Bridge workstation during normal operations ---->5.1.2 Loss of connection due to physical absence ---->5.2 MASS fails to go in MRC AND ---->5.1 Loss of RCC supervision capability ----->5.0 MASS fails due to loss of RCC supervision capabilit ----->0.0 MASS fails in collision avoidance	RCM-38	Acute medical episodes not to compromise SAFE MASS operation	Same as: - RCM-09 b) - RCM-34 a) and b) - RCM-35 a), b) and c)
5.1.2.1.2.3	Engine operator leaves workstation due to lack of motivation, boredom etc. (violation)	i. Poor psychosocial working environment (balance between work demands, control and support, e.g. long and quiet periods causing boredom) ii. Poor work culture and routines	->5.1.2.1.2.3 Engine operator leaves workstation due to lack of motivation, boredom etc. (violation) '--> 5.1.2.1.2 Engine operator leaves workstation AND '-->5.1.2.1.1 Bridge operator leaves workstation '--->5.1.2.1 No operators supervising Bridge workstation during normal operations ---->5.1.2 Loss of connection due to physical absence ---->5.2 MASS fails to go in MRC AND ---->5.1 Loss of RCC supervision capability ----->5.0 MASS fails due to loss of RCC supervision capabilit ----->0.0 MASS fails in collision avoidance	RCM-39	RCC operator to be present at workstation	Same as: - RCM-09 b) and d)

FTA ID	Fault tree analysis			Risk control measures		
	Event description	Causes	Accident scenario/ sequence of events	RCM ID	Topics	RCM descriptions
5.1.2.1.2.4	Engine operator not instructed to supervise bridge operators workstation	i. Lack of proper procedures/handover routines	->5.1.2.1.2.4 Engine operator not instructed to supervise Bridge operators workstation !-> 5.1.2.1.2 Engine operator leaves workstation AND !->5.1.2.1.1 Bridge operator leaves workstation !->>5.1.2.1 No operators supervising Bridge workstation during normal operations ---->5.1.2 Loss of connection due to physical absence ----->5.2 MASS fails to go in MRC AND ----->5.1 Loss of RCC supervision capability ----->5.0 MASS fails due to loss of RCC supervision capability ----->0.0 MASS fails in collision avoidance	RCM-40	Workstation to never be left unattended	Same as: - RCM-09 b)
5.1.2.1.2.3	Abnormal event causes both operators to leave RCC	i. Abnormal events (e.g. fire, terror, earthquake etc.) ii. Fire drill mistaken for actual fire	->5.1.2.1 Abnormal event causes both operators to leave RCC -->5.1.2 Loss of connection due to physical absence --->5.2 MASS fails to go in MRC AND --->5.1 Loss of RCC supervision capability ----->5.0 MASS fails due to loss of RCC supervision capability ----->0.0 MASS fails in collision avoidance	RCM-41	Safe MASS operation to be maintained during unattended RCC	Same as: - RCM-35 a) - and in addition: a) Have a backup RCC workstation in an alternative geographical location for essential control of MASS fleet, incl. the possibility to have MASS enter an MRC. b) Have a portable system available to provide essential control of MASS fleet from outside RCC, incl. the possibility to make a MASS enter an MRC.
5.1.2.1.2.4	MASS fails to go in MRC	i. Insufficient automated capabilities ii. Operator fails to support MASS (see 1.2.1, 1.2.2, 2.1.1.2.1, 2.1.1.2.2, 2.1.2.2, 2.2.2.1, 2.2.2.2, 3.2.1, 3.2.2, 4.2.1 and 4.2.2). iii. Technical failures (same as for a conventional vessel - propulsion, steering etc.)	->5.2 MASS fails to go in MRC AND ->5.1 Loss of RCC supervision capability -->5.0 MASS fails due to loss of RCC supervision capability --->0.0 MASS fails in collision avoidance	RCM-42	MASS to have MRC capability	Same as: - RCM-31 b) - RCM-41 a) and b) - and in addition: a) MRCs to be defined for all critical system failures and external events which can threaten the MASS's or other involved vessels' safety.







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.