DNV·GL

SAFEMASS

Study of the risks and regulatory issues of specific cases of MASS – Summary

European Maritime Safety Agency (EMSA)

Report No.: 2020-0279, Rev. 0
Document No.: 11GG2XH6-3
Date: 2020-03-25

Project name:	SAFEMASS	DNV GL AS Maritime Safety, Risk & Reliability Veritasveien 1 1363 Høvik Norway Tel: +47 67 57 99 00
Report title:	Study of the risks and regulatory issues of specific cases of MASS – Summary	
Customer:	European Maritime Safety Agency (EMSA), Cais do Sodré 1249-206 LISBOA - Portugal	
Customer contact:		
Date of issue:	2020-03-25	
Project No.:	10165993	
Organization unit:	Safety, Risk & Reliability	
Report No.:	2020-0279, Rev. 0	
Document No.:	11GG2XH6-3	

Applicable contract(s) governing the provision of this Report:

Objective:

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.

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

Prepared by:	Verified by:	Approved by:
Øie, Sondre — Digitally signed by Øie, Sondre Date: 2020.03.25 17:31:27 +01'00'	Engelhardtsen, Øystein — Digitally signed by Engelhardtsen, Øystein Date: 2020.03.25 19:44:46 +01'00'	Hoffmann, Peter Nyegaard — Digitally signed by Hoffmann, Peter Nyegaard Date: 2020.03.25 18:27:44 +01'00'
Sondre Øie Principal Consultant	Øystein Engelhardtsen Senior Researcher	Peter Hoffmann Head of Section Safety Risk & Reliability

DNV GL Distribution:

☐ OPEN. Unrestricted distribution, internal and external.

☒ INTERNAL use only. Internal DNV GL document.

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

☐ SECRET. Authorized access only.

*Specify distribution:

Keywords:
Maritime Autonomous Surface Ships, MASS, reduced manning, 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

Rev. No.	Date	Reason for Issue	Prepared by	Verified by	Approved by
A	2020-03-09	Draft issued for review	SONDO	OYSTE	
0	2020-03-25	Final report	SONDO	OYSTE	PHOFF

Table of contents

SUMMARY

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

1 STUDY OF THE RISKS AND REGULATORY ISSUES OF SPECIFIC CASES OF MASS (SAFEMASS) – PART 1

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

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

1.1 A3-B1 MASS concepts (Part 1)

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

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

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

1.2 Emerging risks (Part 1)

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

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

- Boundary parameters and MRCs have not been pre-defined or are incorrectly defined. In such cases notifications or alarms will not be generated by the system, or they are communicated incorrectly (e.g. too late).
- Alarms on portable device are not perceived by the operator, e.g. due to noisy environments, poor alarm design.
- The portable or local alarm device fails, e.g. malfunctions or runs out of battery.
- The operator does not carry or have the portable alarm device readily available.

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

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

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

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

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

- Opposite to the above, mode confusion or distrust in automation causes the operator to (incorrectly) overriding successful MASS system performance.

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

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

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

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

1.3 Risk control options and measures (Part 1)

A set of risk control measures (RCMs) were developed for the models' basic events to demonstrate and suggest risk-reduction effects. The RCMs were grouped into four different RCO categories (see below). Please note that the numbering of RCOs does <u>not</u> 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 for Part 1.

<u>RCO #1</u>

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

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

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

<u>RCO #2</u>

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

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

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

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

<u>RCO #3</u>

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

Recommended RCMs are:

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

<u>RCO #4</u>

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

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

1.4 Regulatory review (Part 1)

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

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

1.5 Concluding remarks (Part 1)

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

2 STUDY OF THE RISKS AND REGULATORY ISSUES OF SPECIFIC CASES OF MASS (SAFEMASS) – PART 2

The second part of the 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 *under*load 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.

2.1 A2-B0 MASS concept (Part 2)

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 sub-chapters.

2.2 Emerging risks (Part 2)

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 operator(s) 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.

2.3 Risk control options and measures (Part 2)

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 for Part 2.

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.

RCO #2

RCO #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.

RCO #3

RCO #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 where 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.

2.4 Concluding remarks (Part 2)

The study concludes that the need for supervision is directly related to the degree of system reliability (or *un*reliability). 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.

THIS PAGE IS INTENTIONALLY LEFT BLANK

About DNV GL