Council of the
European Union

Brussels, 27 February 2023
(OR. en)

6904/23

MAR 30
OMI 18

COVER NOTE

From:	Secretary-General of the European Commission, signed by Ms Martine DEPREZ, Director
To:	Ms Thérèse BLANCHET, Secretary-General of the Council of the European Union
No. Cion doc.:	SWD(2023) 52 final
Subject:	COMMISSION STAFF WORKING DOCUMENT Union submission to the 107th session of the International Maritime Organization's Maritime Safety Committee **suggesting a Risk-Based Assessment Tool for MASS**

Delegations will find attached document SWD(2023) 52 final.

Encl.: SWD(2023) 52 final

EUROPEAN
COMMISSION

Brussels, 27.2.2023
SWD(2023) 52 final

COMMISSION STAFF WORKING DOCUMENT

Union submission to the 107th session of the International Maritime Organization's Maritime Safety Committee suggesting a Risk-Based Assessment Tool for MASS

Union submission to the 107th session of the International Maritime Organization's Maritime Safety Committee suggesting a Risk-Based Assessment Tool for Maritime Autonomous Surface Ships (MASS)

PURPOSE

This Staff Working Document contains a draft Union submission to the International Maritime Organization’s (IMO) 107th session of the Maritime Safety Committee (MSC 107). The IMO has indicatively scheduled MSC 107 from 31 May to 9 June 2023.

The draft submission contains a proposal for a risk-assessment methodology, suitable to address risks associated to MASS operations and for assessing maritime safety levels and equivalence. The Risk-Based Assessment Tool (RBAT), based on functional safety, is tailored for application to MASS operations. It has been arranged for possible integration in the specific section (2.4) of the non-mandatory draft MASS Code. At MSC 106, preliminary considerations were already provided by some IMO members on the same matter and invited further substantive input.

The purpose is to forward the proposed text for technical discussion and consideration in the appropriate fora (MASS working group, if established at MSC 107, and/or the inter-sessional correspondence group).

EU COMPETENCE

The MASS Code aims initially to cover cargo ships (non-mandatory by end-2024) but with a clear intent to cover also passenger ships and to become mandatory by 2028. As soon as it becomes mandatory, it is likely to have an effect on all aspects of maritime safety rules, such as communication in navigation, vessel traffic systems and reporting, procedures for port State control inspections and the risk profiles of the ships for port State control, stability issues, fire-fighting among others. Such items related to safety are covered by the EU maritime safety legislation.

The development of a MASS Code may lead to amending IMO Instruments that have been implemented under the EU maritime safety legislation.

The EU maritime safety legislation concerned is the following:

- Directive 2009/16/EC on port State control[1].
- Directive 2002/59/EC establishing a Community vessel traffic monitoring and information system[2]. It establishes a vessel traffic monitoring and information system with a view to enhancing the safety and efficiency of maritime traffic, improving the response of authorities to incidents, accidents or potentially dangerous situations at sea, including search and rescue operations, and contributing to a better prevention and detection of pollution by ships.
- Directive 2014/90/EU on Marine Equipment[3] in the light of new and/or modified equipment necessary for the application of MASS ships, requiring amendments to performance and testing standards for existing equipment as well as new requirements for new equipment (and theirs type approvals).
- Directive 2003/25/EC on specific stability requirements for ro-ro passenger ships[4]. It lays down specific stability requirements for ro-ro passenger ships, which will improve the survivability of this type of vessel in case of collision damage and provide a high level of safety for the passengers and the crew.
- Directive 2009/45/EC on safety rules and standards for passenger ships[5].

[1] OJ L 131, 28.5.2009, p. 57.

[2] OJ L 208, 5.8.2002, p. 10.

[3] OJ L257/146, 28.8.2014

[4] OJ L 123, 17.5.2003, p. 22.

[5] OJ L 163, 25.6.2009, p. 1.

In light of all of the above, the present draft Union submission falls into areas where the Union has exercised its competence.[6] This Staff Working Document is presented to establish an EU position on the matter and to transmit the document to the IMO prior to the required deadline of 28 March 2023.

[6] An EU position under Article 218(9) TFEU is to be established in due time should the IMO Maritime Safety Committee eventually be called upon to adopt an act having legal effects as regards the subject matter of the said draft Union submission. The concept of '*acts having legal effects*' includes acts that have legal effects by virtue of the rules of international law governing the body in question. It also includes instruments that do not have a binding effect under international law, but that are '*capable of decisively influencing the content of the legislation adopted by the EU legislature*' (Case C-399/12 Germany v Council (OIV), ECLI:EU:C:2014:2258, paragraphs 61-64). The present submission, however, does not produce legal effects and thus the procedure for Article 218(9) TFEU is not applied.

MARITIME SAFETY COMMITTEE 107th session Agenda item XX	MSC 107/xx/X 10 January 2023 Original: ENGLISH Pre-session public release: ☒

DEVELOPMENT OF A GOAL-BASED INSTRUMENT FOR MARITIME AUTONOMOUS SURFACE SHIPS (MASS)

Risk-Based Assessment Tool for MASS

Submitted by Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and the European Commission, acting joinlty in the interest of the European Union

SUMMARY

Executive summary:	This document proposes a risk-assessment methodology, suitable to address risks associated to MASS. The Risk-Based Assessment Tool (RBAT), based on functional safety is tailored for application to MASS. It has been arranged to be integrated in the MASS Code.
Strategic direction, if applicable:	2
Output:	2.23
Action to be taken:	Paragraph 21
Related documents:	MSC 106/WP.8, MSC 106/WP.10, MSC 107/INF.X

Introduction

1 At MSC 106 it was considered appropriate that the MASS Code should incorporate a risk assessment section, while considering at the same time that it was premature to propose a specific methodology. As reported in MSC 106/WP.8, some delegations were of the opinion that the Guidelines for the approval of alternatives and equivalents as provided for in various IMO instruments (MSC.1/Circ.1455) were most appropriate to be used assessing the safety level of MASS while there were also views that concluded that MSC.1/Circ.1455 may require modifications to be applicable to MASS.

2 In this document, the co-sponsors propose a risk-assessment methodology specifically designed for assessing the risks in relation to MASS. In particular, this document addresses Part 2 – **2.4 Risk assessment section** of the Draft International Code of Safety for Maritime Autonomous Surface Ships (MASS Code).

Risk-assessment methodology

3 The introduction of MASS relies on technologies with automated/autonomous functionalities that are introduced in a highly regulated maritime environment. Such functionalities carry new risks whose safety equivalence has to be proved.

4 To assess the risks introduced by increased automation/autonomy, questions such as:

- What is automated and why?
- How is it automated and why?
- How can it fail and how be mitigated?
- Is it safe (enough)?

will have to be answered in the frame of a suitable methodology.

5 To respond to these questions a methodology has been specifically developed to assess the risks caused by the implementation of MASS technologies. A Risk-Based Assessment Tool (RBAT), has been designed to address MASS functions, sub-functions and their interactions. In the following the motivations and the working principles are presented. For more in-depth information refer to MSC 107/INF.X.

5 Design and operation of automation/autonomy are approached in terms of **functions** that are performed by a MASS. This entails the development of function maps, which provide an overview of what, are the goals that the system(s) intend to achieve. Such multi-level function maps are then used to allocate functions between control systems and human operators to also allow for risk evaluation, functions failures and functions degradation.

6 The approach of **function decomposition** (multi-level function maps), is widely in use in several industries. Nuclear power generation, civil and military aviation, space, automotive and petroleum industries to mention some. Relevant is the experience of nuclear and aviation industries with use of remote-control function, relevant to remote control centres for MASS. The use of *hierarchical goal structure* (i.e. multi-level function maps) seems therefore appropriate for maritime applications.

7 The use of hierarchical goal structure, encompass also the notion of **operational goals** (or **missions** as used in aviation and space industries). Definition of operational goals are, therefore, standard practice across the industry; operational goals can be of various nature such as to provide controlled electricity generation or accomplish a mission for an aircraft.

8 Operational goals/missions seem appropriate to describe high-level goals, while functions (functional goals) seem appropriate to describe design and implementation level. For example, IEC 61508-2010 (all parts)-Functional safety of electrical/electronic/programmable electronic safety-related systems – sets methodologies for **functional safety** including *inter-alia*, methods on how to **decompose functions and sub-functions** in relation to their abstraction level. The lowest decomposition level is when operators' intervention is foreseen. This forms the bottom level of the function hierarchy and is commonly referred to as control functions (IEC, 2010). **Control functions** are defined as control actions performed by humans or machines for the accomplishment of a functional goal including the associated information acquisition and processing. **Task** is reserved for activities performed by humans.

9 Most of the standards and guidance reviewed (ref. To MSC 107/INF.X) do not make use of Level of Automation (LoA) but rather describe how to automate certain functions.

10 Within the framework sketched above, in which operational goals, functions, sub-functions, control functions and tasks can be defined, a Functional Hazard Assessment (FHA) can be devised and tailored specifically for MASS applications.

11 The application of the traditional risk-assessment analysis is challenging due to lack of statistical data on which the risk-model can be built. The classical definition of risk as

(probability x consequence) becomes of difficult application. Many of these risks are control related and it is considered advantageous instead of applying the classical definition of risk (risk=probability x consequence), to evaluate the risk as explained below.

12 Focusing on the control functions, failures of such functions can be categorized in broad terms in: (1) operator mistakes, (2) impact from the environment; (3) deliberate actions, (4) random hardware failures, (5) systematic failures, (6) systemic failures.

13 **Systematic failure** events are the consequence of inadequate work processes and may be introduced at all stages in the system lifecycle. **Systemic failure** is an event which occurs even if no individual component in the system has failed.

14 While failure types from 1 to 4 can be analysed by traditional risk-assessment methods and dealt within the traditional risk definition, systematic and systemic failures cannot be properly dealt within the traditional risk definition framework. Systematic and systemic failures are indeed typical for systems in which there is a relevant algorithmic and software element, for which the estimation of probability of the initiating event becomes extremely difficult due to the extremely high number of combinations, under which the failure mechanism can occur. Such number of combinations cannot be tested (even though testing can indeed reduce its number). Systematic and systemic failures also, cannot be addressed by system redundancy, as the same system made redundant still is prone to the same systematic and systemic failures.

15 Methods to manage the risks related to control functions systemic failures, again in broad terms, can be divided in the following groups:

- Use of independent protection systems
- Use of operational restrictions
- Use of alternative control capabilities (human in the loop or other system)
- Use of high-integrity control function

16 It is considered that high-integrity control functions in compliance with relevant standards such as IEC 61508, IEC 61511 and other function-specific standards, may result in an extremely cumbersome process, with requirements of complex application and components/systems not available to the maritime industry.

17 It is, therefore, considered that systematic and systemic failures can be dealt by **mitigation layers** that can be alternative control capabilities / operational restrictions / independent protection systems or the combination thereof.

18 On this basis, risk is evaluated as a combined function of:

- Severity of the worst-case outcome of an undesired event
- Effectiveness of the mitigation concept to prevent any loss

Risk Based Assessment Tool – Methodology

19 The risk assessment methodology consists of four major modules:

- **Define use of automation** - This module describes the overall mission and operations and assigning the responsibility for either performing or supervising functions to software or humans. This process should be part of an integrated part of developing and documenting the Concept of Operations (ConOps). The ConOps includes a description of the functions, the allocation of the functions to different agents[7], supervision of the functions

[7] Agent is machine (usually a computer) that executes a function that maybe previously carried out by a human.

and the agents responsible for this, the location of the agents (on the vessel or remote) and mapping the systems and other roles involved in performing a control action.

- **Hazard analysis** - This module is applied to identify unsafe conditions that are associated with the control actions, to identify causal factors, which initiate unsafe conditions, and to describe the worst-case outcomes from unsafe conditions. Furthermore, the module is applied to rank the worst-case outcomes severity and to describe the relevant operational restrictions and limitation.

- **Mitigation analysis** - This module is applied to identify the control's ability to self-recover or withstand a failure event and to determine whether the additional mitigation layers are successfully implemented to prevent any further losses. The mitigation layers could also involve entering a minimum risk condition (MRC) as a measure to stay as safe as possible while the system is attempting to regain the desired control level. MRC is considered the desired condition that can be achieved when the system (ship) is experiencing an abnormal situation. The MRC mode of operation can be achieved by the successful use of the mitigation layers that exist and can be realized by a single function or a combination of functions. These functions could also bring the ship to a normal operation state or to state that can be accepted.

- **Risk control** - The risk evaluation and control is the last module of the methodology where a risk evaluation is performed to compare the risk level of each assessed scenario against a set of risk acceptance criteria to determine the need for risk control. For each scenario one has to assess the combination of causal factor, unsafe condition or mode, mitigation layers and worst-case outcome.

Conclusion

20 It is proposed to consider Annex II as basis for further discussion and the inclusion of risk-based assessment tool (RBAT) as methodology in the frame of Section 2.4 Risk Assessment from MASS. The full scope of the methodology is presented in MSC 107/INF.X[8].

Action requested by the Group

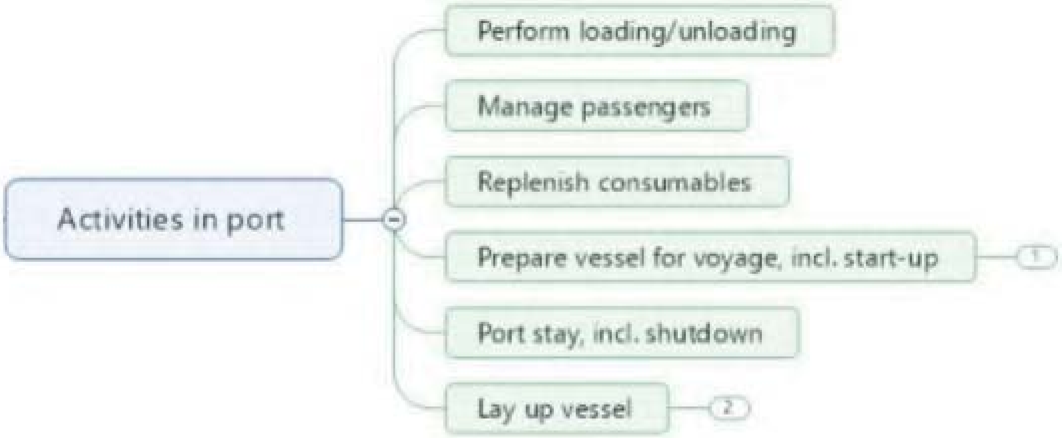
21 The Committee is invited to:

.1 consider the conclusion (point 20) and forward the proposed text for discussion in the appropriate fora (MASS working group, if established, and/or the inter-sessional correspondence group) with a view for inclusion in Section 2.4 on risk assessment in the MASS code, and,
.2 note the information provided in MSC107/INF. X and comment as appropriate.

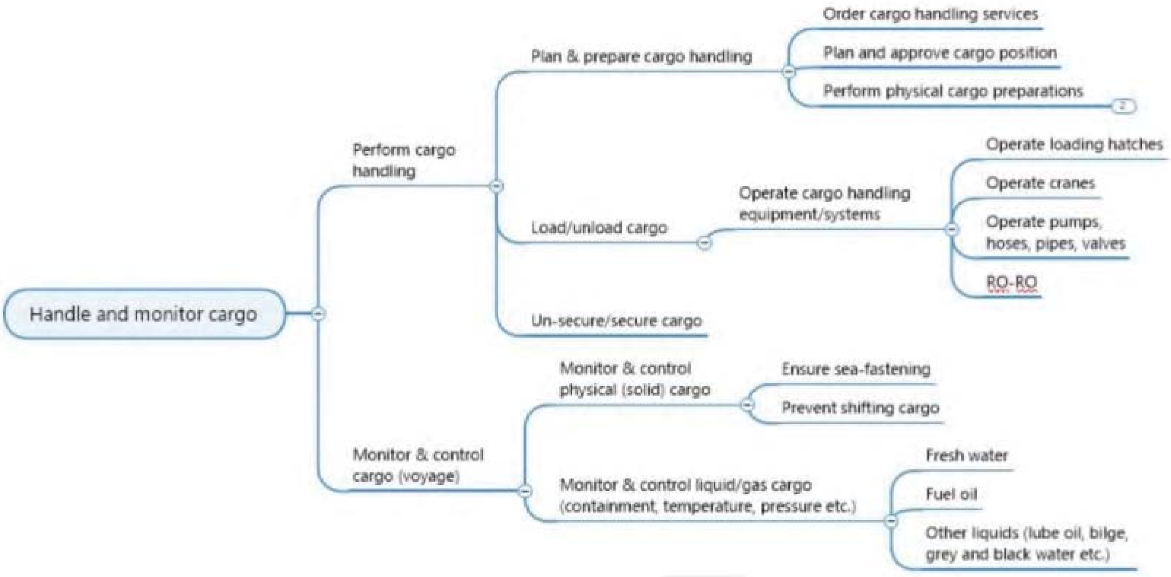
[8] also available on https://www.emsa.europa.eu/

Annex I

Mission and Function Models - examples


Activities in port
Perform loading/unloading
Manage passengers
Replenish consumables
Prepare vessel for voyage, incl. start-up
1
Port stay, incl. shutdown
Lay up vessel
2

Mission model - example


Handle and monitor cargo
Perform cargo handling
Plan & prepare cargo handling
Order cargo handling services
Plan and approve cargo position
Perform physical cargo preparations
2
Load/unload cargo
Operate cargo handling equipment/systems
Operate loading hatches
Operate cranes
Operate pumps, hoses, pipes, valves
RO-RO
Un-secure/secure cargo
Monitor & control cargo (voyage)
Monitor & control physical (solid) cargo
Ensure sea-fastening
Prevent shifting cargo
Monitor & control liquid/gas cargo (containment, temperature, pressure etc.)
Fresh water
Fuel oil
Other liquids (lube oil, bilge, grey and black water etc.)

Function tree - example

Annex II

Proposal for Section 2.4 Risk- assessment

2.4 Risk assessment

[2.4.1 Application

- A risk assessment shall be conducted to ensure that risks arising from the implementation of MASS functions are addressed.

2.4.2 Principle

MASS functions are in general relying on the application of automated/autonomous systems, whose safety assessment should be carried out by using a risk-assessment methodology able to assess the risks associated with the automated/autonomous function(s), sub-functions (and their combinations) taking into consideration all possible sources of failures and their combinations.

Risk-assessment methodology should be able to properly address systematic and systemic failures.

2.4.3 Definition

Function is specific purpose or objective to be accomplished, that can be specified or described without reference to the physical means of achieving it (EN 15380-4 2010).

Systematic failure events are the consequence of inadequate work processes and may be introduced at all stages in the system lifecycle.

> *Note: Some examples are incomplete risk analysis, inadequate development of barrier strategies, incomplete requirement specifications, weaknesses in software design, programming errors, quality problems in hardware production, and inadequate planning of maintenance.*

Systemic failure is an event which occurs even if no individual component in the system has failed.

> *Note: This may be caused e.g., by overlooked dependencies among the technical, operational, human, and organisational elements of systems, specifications that are based on inadequate understanding of physical processes, or unexpected inputs for which no specific response has been specified. Particularly relevant for systems containing software functions. It can be related to intricate dependencies and feed-back mechanisms among system components leading to nonlinear and unpredictable system behaviour. Lack of knowledge and understanding of interactions in a system increase the risk of systemic failures as it makes it difficult to implement robust barrier strategies to prevent them.*

2.4.4 Procedure
2.4.4.1 Team of evaluation
2.4.4.2 Safety standards
2.4.4.3 Hazard identification
2.4.4.4 Control measures
2.4.4.5 Record
2.4.5 Risk management
......
2.4.6 Risk assessment methods
2.4.6.1 Functional Hazard Assessment (FHA)
2.4.6.2 Failure Modes and Effects Analysis (FMEA)
2.4.6.3 Systems-Theoretic Accident Model and Processes (STAMP)]
2.4.6.4 Risk-Based-Assessment Tool (RBAT)

For a full reference see MSC 107/INF.X