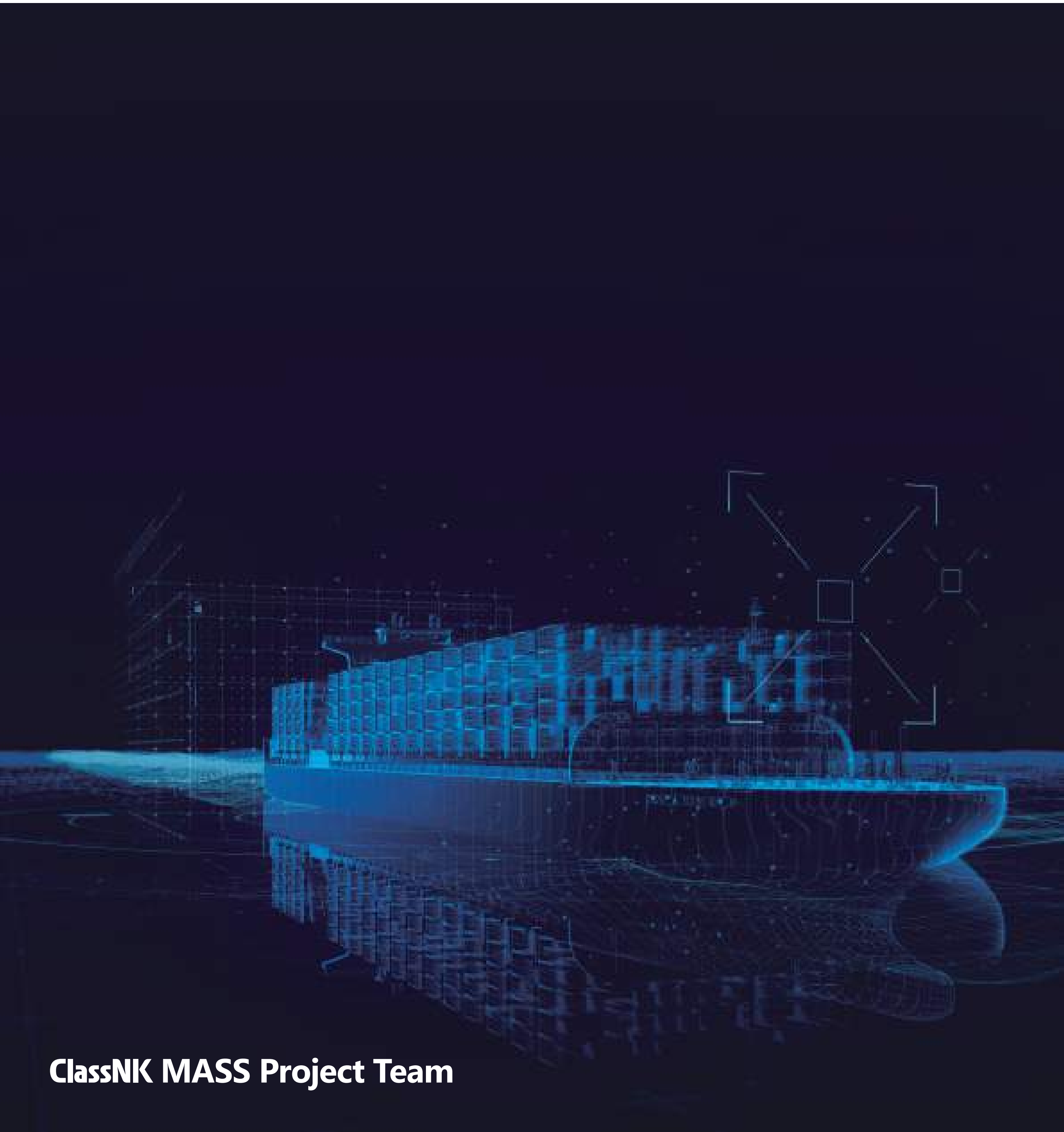
CHARTING THE FUTURE

ClassNK

WHITE PAPER

Towards MASS social implementation

[English]



ClassNK MASS Project Team

Summary

The development of MASS (Maritime Autonomous Surface Ships) is progressing worldwide, as seen in the accelerating development of MASS-related technologies and active demonstration experiments being conducted in many countries. For example, in the fully autonomous ship program “MEGURI 2040” of the Nippon Foundation in Japan, five consortia conducted demonstration tests on actual commercial shipping routes by a tourism boat, coastal container ships and large ferries. Demonstration tests of autonomous berth-to-berth navigation under the supervision of onboard seafarers were carried out and were also successful in automatically avoiding other vessels including fishing boats engaged in commercial activities. Based on the experience of these demonstration tests, the participating shipyards and equipment manufacturers are accelerating development with the aim of social implementation in 2025.

In parallel with technological development, active movements with respect to the development of international rule is ongoing. In the International Maritime Organization (IMO), MSC 105 endorsed a roadmap for developing a goal-based MASS Code, in which a non-mandatory MASS Code will be developed in 2024 and a mandatory goal-based MASS Code will be developed targeting entry into force in 2028. A correspondence group (MASS CG) has been set up to draft the MASS Code and work is currently underway. The MASS CG will submit an interim draft for consideration at MSC 107, which will be held from May 31 to June 9, 2023.

As social implementation of MASS in 2025 is now becoming a reality, the time has come to consider a new framework which supports the social implementation of state-of-the-art technologies and solutions that transcend the conventional framework, that is, a framework which can complement imperfect regulations and institutions. It is also necessary to accelerate introducing functional safety and systems engineering to the maritime industry.

For the safe social implementation of MASS, it is necessary to confirm that the system level of autonomy, the MASS operational envelope (OE) and override methods are appropriately designed based on the specific assumptions of MASS use cases. Therefore, in the design and development phases, ClassNK (hereinafter, the Society) focuses on the technology differences between the existing technology (conventional ships) and MASS, and conduct rational, effective and economical assessments of both the safety evaluation of the new technologies themselves and the evaluation of the entire system that integrates them. A framework for safety evaluation when proceeding with design development based on the V-model is also established to enable implementation in a timely manner.

On the other hand, since autonomous navigation technology is a new technology with no track record to date, the problem that “you won't know until you use it” will inevitably remain. Thus, it will be necessary to devise the actual operation method after recognizing its imperfections. As part of this effort, it will be necessary to create a mechanism for collecting data on defects and near-miss incidents found after implementation and updating regulatory requirements as appropriate and evaluation methods by third parties. To achieve it, the Society proposes the use of a vulnerability database in the operation phase. It is important to improve technology, regulations and evaluation by appropriately distributing feedback from seafarers as users to the technology development, rule development and safety evaluation processes. The Society believes that constructing a vulnerability database and appropriately applying the PDCA (Plan, Do, Check, Act) cycle will lead to improved safety in MASS operation.

In view of these matters, the Society has compiled this White Paper on the safety assessment framework for the MASS design and development phases and the PDCA cycle for the operation phase.

Revision History

No.	Date	Details od revision
1.0	April 28, 2023	First issue
1.1	June 7, 2023	Editorial corrections

Contents

Chapter 1 Introduction

1.1 Background

The development of MASS (Maritime Autonomous Surface Ships) is progressing worldwide, as seen in the accelerating development of MASS-related technologies and active demonstration experiments being conducted in many countries. For example, in the fully autonomous ship program "MEGURI 2040" of the Nippon Foundation in Japan, five consortia conducted demonstration tests on actual commercial shipping routes by a tourism boat, coastal container ships and large ferries. Demonstration tests of autonomous berth-to-berth navigation under the supervision of onboard seafarers were carried out and were also successful in automatically avoiding other vessels including fishing boats engaged in commercial activities. Based on the experience of these demonstration tests, the participating shipyards and equipment manufacturers are accelerating development with the aim of social implementation in 2025.

In parallel with technological development, active movements with respect to the development of international rule is ongoing. In the International Maritime Organization (IMO), MSC 105 endorsed a roadmap for developing a goal-based MASS Code, in which a non-mandatory MASS Code will be developed in 2024 and a mandatory goal-based MASS Code will be developed targeting entry into force in 2028. A correspondence group (MASS CG) has been set up to draft the MASS Code and work is currently underway. The MASS CG will submit an interim draft for consideration at MSC 107, which will be held from May 31 to June 9, 2023.

1.2 Terminology

Although the specific requirements for MASS are being considered at the IMO as described above, the definitions of terminology have not been finalized. Therefore, this paper tentatively defines the terms as follows for convenience. Please note that these definitions may be subject to change in accordance with decisions based on future international discussions.

MASS (Maritime Autonomous Surface Ships: MASS)
Ships that have transferred part or all of the role of safe navigation played by seafarers on conventional ships to automated systems or remote operators.

Autonomous Navigation System (ANS)
An automated system responsible for the navigation task, which has the functionalities of situational awareness, route planning and determination for collision and grounding risk avoidance, control of the ship's heading, speed and track, and alert management to detect deviations from the operational design domain (ODD) of itself.

Concept of Operation (ConOps)
A term is used in systems engineering and described in ISO/IEC/IEEE 29148. ConOps refers to a document that summarizes the concept and outline of system usage and operation and is positioned as an important document for eliciting stakeholder and system requirements. In the definition of system requirements, it is necessary to comprehensively define the capabilities and functions required. By creating use and operation scenarios that cover the entire life cycle of a system, it is considered possible to define requirements without omissions (or with few omissions).

Operational Envelope (OE)
OE is defined in ISO/TS 23860 as follows:
"Operational envelope: conditions and related operator control modes under which an autonomous ship system is designed to operate, including all tolerable events."

Referring to this description, in this paper, OE refers to the range of operations in which safe operation can be performed as a ship, including the division of roles between humans (seafarers or remote operators) and automated systems to distinguish it from ODD (defined below).

Operational Design Domain (ODD)

ODD refers to the design range in which a system can operate properly. ODD includes both ODDi, which is related to internal events such as system failures, and ODDe, which is related to external events. The following are possible as ODDe:

- ✓ Geographical factors such as navigational sea areas
- ✓ Environmental conditions such as day and/or night, weather and sea conditions, etc.
- ✓ Degree of traffic congestion
- ✓ Overboard monitoring and support environment, including port facilities, if applicable

In this paper, ODD is used to indicate the safe operating limits of the system (machine), and OE is used to indicate the safe operating limits of MASS (ship = machine + human). As the degree of autonomy of MASS increases, the difference between ODD and OE decreases because of the smaller human involvement. While crewed MASS is maintained within a safe area by humans functioning in the loop of a large system called MASS, fully autonomous ships eliminate the difference between ODD and OE because there is no human involvement.

Fallback

An action taken to minimize risk in the event that an automated system or remote operation system fails to operate properly. Fallback keeps the MASS state to the acceptable risk condition (ARC, defined below). This includes responses to deviations from the ODD. The state in which a system[1] is operated with limited functionality (degraded operation) is called the fallback state.

Override

The act of overriding the operational authority of the system at the discretion of a human, regardless of whether the system deviates from the ODD or not.

Acceptable Risk Condition (ARC)

The state in which the minimum functions necessary to perform the targeted task are maintained and risk is reduced to an acceptable level. For example, the ARC of a ship refers to the state of the ship (state in which the seaworthiness of the ship is maintained) which satisfies the classification societies and flag state requirements for performing the task.

Minimal Risk Condition (MRC)

The state that the MASS aims to achieve when an event occurs that prevents safe navigation due to system malfunction, etc. For example, the state might be stopping in the nearest predefined evacuation area or continuing turning at the minimum speed with the rudder fixed while waiting for rescue from outside.

Minimal Risk Manoeuvre (MRM)

An action performed to keep the MASS in the MRC if an event that prevents safe navigation occurs, for example, if a fallback request was made but a human does not respond within the given time. An example of MRM might be to automatically or remotely navigating to the nearest predefined evacuation area and stopping the MASS in a safe place, or continuing to turn at the appropriate speed with the rudder fixed.

The relationship between these terms is shown in Figure 1.1. If the system deviates from ODD during autonomous navigation, the ARC of the MASS must be maintained by fallback. If the fallback does not function properly, the MASS will enter the accident or incident region. To prevent this, it is necessary to keep the MASS in the MRC by carrying out an MRM.

[1] The term “system” means to include both automated systems and remote operation systems in this paper.

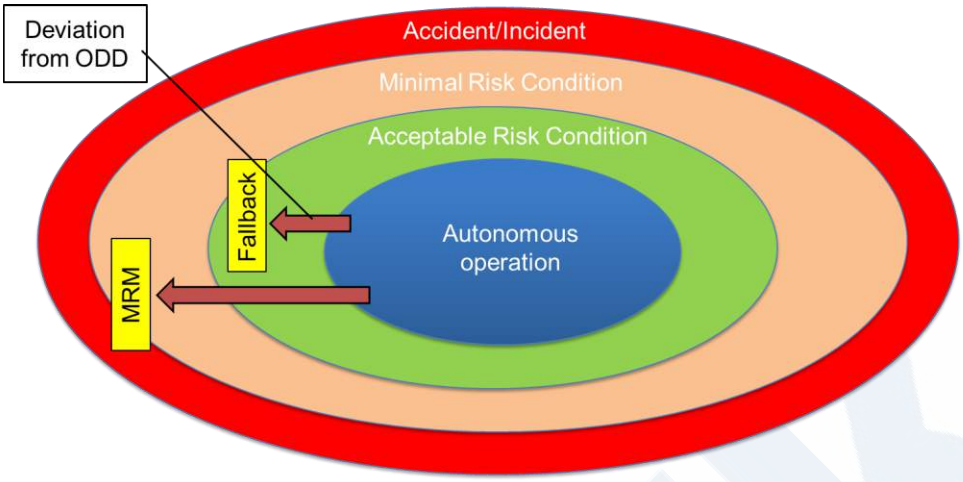


Figure 1.1 Relationship between terms

Chapter 2 MASS Safety

2.1 Absolute safety and functional safety

ISO/IEC GUIDE 51: 2014 defines safety as “freedom from risk which is not tolerable”. Although “zero risk from all possible causes (absolute safety)” would be ideal, this definition is appropriate from a technical point of view.

Safety can be divided into intrinsic safety and functional safety. Intrinsic safety indicates measures to reduce or eliminate causes of harm to humans or the environment, while functional safety indicates introduction of functions which ensure safety (safety functions) in order to achieve an acceptable level of safety. For example, considering the safety of railroad crossings, the concept of intrinsic safety is to remove the railroad crossing and create a grade separated crossing, while functional safety might mean adding a new function, namely, a crossing gate. Since it is generally difficult to completely eliminate the causes of harm by intrinsic safety alone, it is necessary to reduce the risk to an acceptable level by a combination of intrinsic and functional safety measures.

The viewpoint of functional safety is also important in MASS. Since MASS will delegate the role of safe navigation traditionally performed by onboard seafarers on conventional ships to automated systems and/or remote operators, it is necessary to examine whether automated systems and/or remote operators can adequately replace the role of safety functions originally performed by onboard seafarers, or whether additional safety functions need to be provided.

2.2 Safety level required for MASS

Because the purpose of introducing MASS is to improve not only safety but also convenience and economic efficiency, MASS does not necessarily require safety beyond the level of conventional ships. Therefore, it is necessary to confirm the equivalent risk level (equivalent safety) through a relative comparison with conventional ships. In other words, MASS also aims for the state in which “risk is reduced to an acceptable level (ARC)” maintained by onboard seafarers (qualified personnel with formal training).

Minimum competence requirements for seafarers are specified in the International Convention on Standards of Training, Certification and Watchkeeping for Seafarers (STCW). While there is some discussion as to whether these competence requirements should also be applied directly to automated system, how to achieve them when part of the onboard seafarers’ tasks is replaced by the system is an important issue. Similarly, how to make the system comply with maritime laws such as Convention on the International Regulations for Preventing Collisions at Sea, 1972 (COLREG) is also an important issue.

2.3 Safety under normal situations and safety under emergency situations

It is necessary to separately consider safety in normal situations or in emergency situations. Under normal situations, the minimum requirements defined in advance must always be satisfied. However, under emergency situations, the conditions are below the predefined minimum requirements. Therefore, it is important to “not make the situation worse”.

As shown in Figure 1.1, ARC should be achieved under normal situations and MRC should be the aim under emergency situations. In order to keep the condition of MASS within ARC, it is important to design the OE so that the condition of the MASS does not fall into MRC even if automated systems such as ANS are stopped.

Example

To maintain ARC even if systems deviate from ODD,

- ✓ A human operator stops or disconnects the system in order to continue operation, or
- ✓ the human operator operates the system in the fallback state while continuing ship operation.

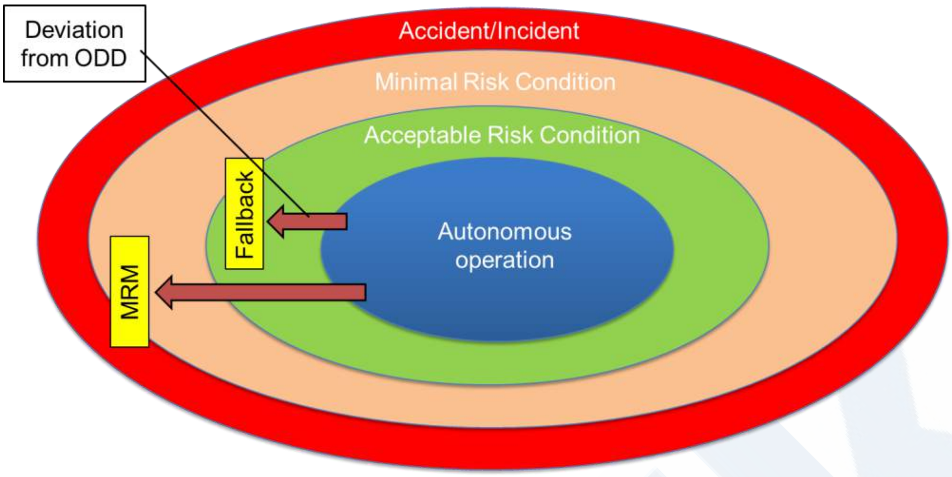


Figure 1.1 Relationship between terms (reprinted)

Since failure of equipment which is essential to operations is considered to be an emergency situation, this is a deviation from ARC. This must be taken into account, regardless of whether the ship is a conventional ship or MASS. In this case, to ensure that MASS conditions do not fall into the accident or incident region, appropriate MRCs must be set, and MRMs which can maintain MASS condition within MRC even under emergency situations must be set in advance. However, it is difficult to uniformly define MRC of ships. For example, in situations affected by waves and currents, the ship may drift if its main engines are stopped and anchoring to prevent drifting may actually endanger the condition of the ship in some situations. It is necessary to respond flexibly considering the surrounding conditions, atmospheric and sea conditions, and abnormal events occurring in the MASS. When an emergency occurs on a conventional ship, the onboard seafarers make appropriate decisions on actions (MRMs) to "not make the situation worse" according to the situation, and this flexible response capability of the onboard seafarers supports the safe operation of the ship.

It is technically very difficult for the system to be in charge of MRM in an emergency on MASS. A fully autonomous ship without any human intervention will appear only when the system can handle emergencies automatically, or when the probability of emergencies can be reduced to near zero.

2.4 Basic elements for ensuring safety to be considered in the design process

To evaluate the safety of MASS, it is necessary to understand their characteristics. Therefore, the ClassNK "Guidelines for Automated/Autonomous Operation of Ships" states that the following eight basic elements for ensuring safety are to be clarified in the conceptual design stage. The Society will verify the safety of MASS systems based on the combination of these elements, rather than ones individually.

1. Target task of automated/remote operation on a ship
2. Division of roles between systems and humans
3. Prerequisite specifications for system installation
4. Clarification of ODD
5. Fallback
6. Human Machine Interface (HMI)
7. Cybersecurity
8. Reliability of computer systems

2.5 Risk assessment

In the maritime industry, technological innovation and the complexity of such technologies occasionally lead to the development of concepts, designs, etc. which utilize new technologies that cannot be addressed by existing rules and standards. Since these new technologies differ significantly from the existing design concepts, their safety cannot be adequately confirmed because it is not possible to apply the existing regulatory requirements and underlying regulatory concepts, and this may lead to undesirable results to the new technologies. Therefore, it is necessary to identify the hazards that may arise as a result of the development and introduction of new technologies, and to evaluate the concepts and designs that use the new technologies.

This concept is presented in the IMO's MSC. 1/Cir. 1455 (2013) “Guidelines for the Approval of Alternatives and Equivalents as provided for in Various IMO Instruments”. In addition, “Guidelines for Technology Qualification” issued by ClassNK establishes specific processes for certifying new technologies which should be systematically evaluated through the process from verification of defined requirements for new technologies to their safety on a risk basis.

This concept and process can also be applied to MASS. Multiple classification societies including the Society have already issued guidelines on MASS, all of which emphasize risk assessment. IMO Interim Guidelines and other guidelines issued by some flag states also specify the implementation of risk assessment.

In particular, in large and complex systems, not only the failure of individual components/subsystems, but also the hazards inherent in the interactions between components/subsystems, may lead to accidents such as collisions, grounding and sinking. In conventional risk analysis for ships, hazards are identified by focusing on equipment failures through the use of a system configuration diagram centered on hardware. However, in the risk analysis of MASS, it is important to comprehensively extract hazards based on the above features. For that purpose, the hardware, software, and humans that configure MASS must be viewed as a large single system, and the tasks that each component is responsible for, the exchange of information between components, and the processes that require approval by humans, must be clearly defined.

The details of the specific techniques and points to note when conducting risk assessments are described in Chapter 6.

2.6 Systems engineering and use of simulation

To evaluate the safety of MASS, it is necessary to verify the life cycle of the system, including its design, development, installation and operation. The verification should be performed rationally, efficiently and economically. In recent years, development based on systems engineering has gained attention as a systematic approach to achieve this. Figure 2.1 shows the V-model, which represents the concept of the systems engineering approach. In the design phase on the left side of the V-model, checking correspondence between requirements and design in a top-down manner prevents the leakage of higher-level requirements and reduce reworking. In the verification phase on the right side, the verification is performed whether the components of the system are properly integrated and the intended requirements are achieved in a bottom-up manner. Referring to this process, when conducting safety evaluations, it is desirable to determine the verification items in a top-down manner in the design process and verify that those requirements are incorporated in a bottom-up manner in the verification process. In this verification, the highest-level requirements are the most important, and activities involving safety verifiers, such as flag states and classification societies, are required upstream in the design process to determine them. Since the risk assessment described in section 2.5 is used to identify the verification items, the results should be reviewed by the safety verifiers. This point is also mentioned in IMO's MSC. 1/Cir. 1455 (2013) “Guidelines for the Approval of Alternatives and Equivalents as provided for in Various IMO Instruments”, which provides for a certification procedure for alternative designs using new technologies, and the same concept should be applied to MASS.

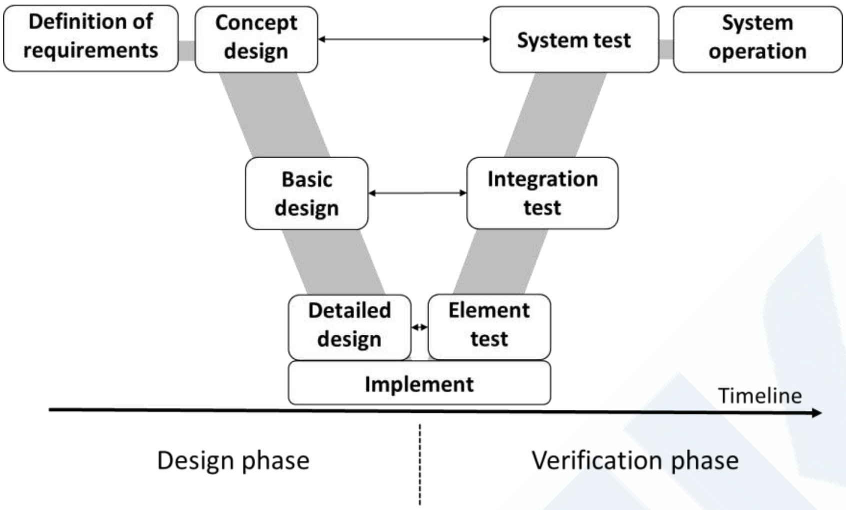


Figure 2.1 V-model representing the concept of the systems engineering approach

Ideally, the verification items established in the design process should be comprehensively verified through tests using actual equipment (e.g., sea trials), but in practice, some items are difficult to verify. For example, when an autonomous collision avoidance function is verified with an actual ship, it is necessary to conduct tests under scenarios in which collision or grounding may occur (accident scenarios), but it is undesirable to conduct such dangerous tests at sea, in the real situation. Therefore, it is essential to reproduce and verify the test environment by a computer simulation without changing the verification items. In addition, the simulations utilized in this process should be different depending on which design to be verified. For instance, the whole system would be verified by HILS (Hardware In the Loop Simulation), in which the environment of ships and the sea is reproduced by a simulator, and then they are connected to actual devices, while SILS (Software In the Loop Simulation), in which software is connected to a simulator for verification, would be used to verify collision avoidance algorithms in unit tests. There are also two types of simulation: Real-time simulation, which reproduces the environment in real time, and fast time simulation, which enables high-speed calculation, and it is necessary to select the type of simulation appropriately according to the scenarios and items to be verified. The scenarios to be used are important when conducting these simulations. In risk assessments in the design stage, it is important to identify hazards and then extract the scenarios under what circumstances does the hazard manifest itself and lead to an accident.

2.7 Cybersecurity

Cybersecurity for MASS will be an extremely important factor for safe operation of ships, when information is captured from OT equipment and used for automatic navigation, or when data is sent and received between ship and shore.

The International Association of Classification Societies (IACS) has issued IACS UR E26 and UR E27 “Cyber resilience of on-board systems and equipment,” which apply to ships contracted for construction on and after January 1, 2024 and is now in the process of applying cybersecurity measures to new ships in the future. These requirements will also be applied to MASS which are built in the future. However, considering the configuration of the MASS system, application of UR E26 and E27 alone is not expected to be sufficient because these requirements are mainly intended for cyberattacks from outboard to onboard network systems via satellite links, but not for cyberattacks that transmit disinformation to GPS, LiDAR, image recognition cameras, etc., which are important components of MASS. Given that jamming and spoofing of GPS still affect the navigation of ordinary ships at this point, it is expected that MASS will require more advanced cybersecurity based on UR E26 and E27, with additional protection requirements for GPS data, sensor data, etc.

2.8 Assessment for entire voyage (assessment of navigational modes and ensuring continuity)

In entire voyage, berth-to-berth operation, maneuvering and running equipment of conventional ships varies depending on their navigational mode, e.g., in the open sea, congested waters, narrow channels, inside bays, inside harbors or in berthing/unberthing. Therefore, when evaluating the safety of MASS, it is necessary to verify that the ANS has functions that behave appropriately in response to these situations. In particular, in waters where conventional ships may be present, MASS should be designed so as not to maneuver in a way that would cause anxiety on seafarers on those ships. For example, in autonomous collision avoidance, the necessary safety distance is different in open seas and congested waters, so the parameters set for these navigational modes may be different in ANS. In this case, it is necessary to confirm that the parameters are set appropriately for the navigational mode.

It is also important to ensure that changes between navigational modes are being made properly. In other words, it is necessary to focus on what is a trigger to change of the maneuvering mode and who (or what) is responsible for initiating the change, as well as whether the mode change is carried out automatically or by a remote operator.

Moreover, OE, Operational Envelop; refer to section 1.2, is variable depending on the navigational mode. For example, it is possible to operate in the “mind-off” state in the open sea and in the “hands-off” state in congested waters. (“Mind-off” and “hands-off” are used to describe the level of autonomy discussed in more detail in section 4.2.) If operation of this type is envisioned, it should be clearly stated in the ConOps.

2.9 Ensuring safety through the life cycle of MASS

Realizing social implementation of MASS will require not only verifying the safety of the systems in the design and development stages, but also checking the items to be confirmed and the requirements to be met when the system is installed on a ship. The methods and procedures for maintenance and management during operation should also be clarified. Existing frameworks for inspection and examination by classification societies can be applied to these matters and are also mentioned in the “Guidelines for Automated/Autonomous Operation of Ships” issued by ClassNK.

In particular, it is important to ensure that the system is functioning correctly during operations. In system operation, in addition to familiarizing the user with the operation of the system, incorrect usage with misunderstanding must be prevented. Training to become familiar with the operation and understand the nature of the system must be properly conducted. It is particularly important that the seafarers employed in MASS operation have a correct understanding of the ODD of the system and are able to perform fallbacks and overrides reliably so that MASS can maintain ARC.

If a serious malfunction is discovered after a system is onboard, the relevant parties must be promptly notified of this fact and the specific countermeasures that should be taken. After social implementation of MASS, a framework to enable system suppliers, system integrators and system users to work together appropriately is also needed.

Chapter 3 Use Cases

3.1 Importance of clarifying use cases

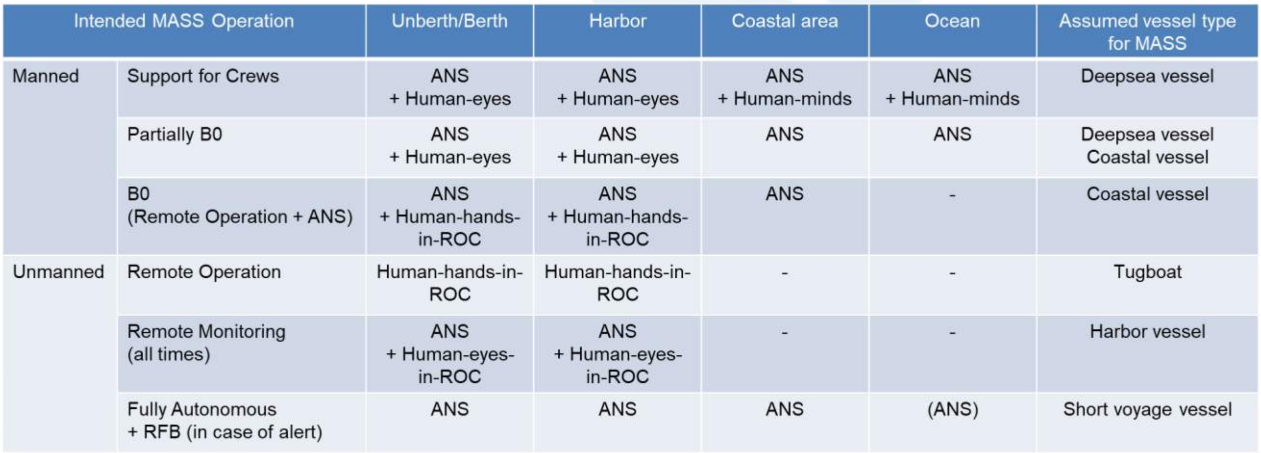
As the result of accumulating demonstration projects, the MASS-related technology development has been reaching to the close level of social implementation. The time has come to consider specific use cases of MASS. Clarifying use cases will accelerate discussions on the concretization and standardization of safety requirements. What do we hope to achieve by social implementation of MASS? (What social issues do we want to solve? What kind of business does the operator intend to do?) What kind of MASS is needed to achieve this? (Which is necessary, a fully automated ship or a remotely-operated ship?) What kind of technology is necessary to achieve it? The answers to these questions need to be organized, documented in the ConOps, and shared among the stakeholders.

The ConOps must be socially acceptable and, of course, must comply with the applicable laws and regulations. It must also be technically and economically feasible. Therefore, it also needs to validate in detail whether the maturity of technology is at a socially acceptable level.

For example, because autonomous navigation technology is being developed as a solution to the social issue of a global shortage of seafarers, automated/remotely controlled operation of navigation tasks is being discussed first. In this case, the assumed use cases for MASS can be clarified by organizing the following items in the form shown in Table 3.1.

- ✓ Whether tasks are automated/remotely controlled during the entire voyage, or only specific area.
- ✓ Whether the automated/remotely controlled level is fixed during the entire voyage or is varied depending on the navigational mode.
- ✓ Whether the target of tasks is on crew, officer, or both.

Table 3.1 Examples of MASS Use Cases



Intended MASS Operation		Unberth/Berth	Harbor	Coastal area	Ocean	Assumed vessel type for MASS
Manned	Support for Crews	ANS + Human-eyes	ANS + Human-eyes	ANS + Human-minds	ANS + Human-minds	Deepsea vessel
	Partially B0	ANS + Human-eyes	ANS + Human-eyes	ANS	ANS	Deepsea vessel Coastal vessel
	B0 (Remote Operation + ANS)	ANS + Human-hands-in-ROC	ANS + Human-hands-in-ROC	ANS	-	Coastal vessel
Unmanned	Remote Operation	Human-hands-in-ROC	Human-hands-in-ROC	-	-	Tugboat
	Remote Monitoring (all times)	ANS + Human-eyes-in-ROC	ANS + Human-eyes-in-ROC	-	-	Harbor vessel
	Fully Autonomous + RFB (in case of alert)	ANS	ANS	ANS	(ANS)	Short voyage vessel

<Notes>

ROC:	Remote Operations Centre	RFB:	Remote Fallback
ANS:	Autonomous Navigation System	B0:	With crew somewhere on board

(Provided by the Japan Ship Technology Research Association)

3.2 Importance of accumulating experience

For social implementation of unproven new technologies, it is necessary to conduct in-depth studies on specific use cases and accumulate experience by working together with not only technology developers and users but also rule developers and safety evaluators. Without that experience, discussions on the standardization of safety requirements may not efficiently progress.

As long as technology concerned is a new technology with no proven track record, the problem that "you won't know until you try it" will inevitably remain. Therefore, even in the case of uncrewed technology, until the technology is sufficiently mature, it will be necessary to use it with safety margins, for example, the technology is only used under the constant supervision of onboard seafarers. It is also necessary to accumulate experience in order to bring the technology to maturity level where social implementation is possible. Creating a pathway where the accumulation of experience leads to expansion of the scope of use, and having technology developers, users, rule developers and safety evaluators working in the same direction to improve safety, will lead to benefit the maritime industry.

Chapter 4 Three Perspectives for Considering Safety Requirements

4.1 Overview

Guidelines on establishing rules for new technologies, procedures for deliberation and procedures for certification have already been done by the IMO. For example, the IMO has established MSC.1/Circ. 1394/Rev. 2 (2019) "Generic Guidelines for Developing IMO Goal-Based Standards" as its rulemaking standard, MSC/Circ. 1023, MEPC/Circ. 392 (2002) "Guidelines for Formal Safety Assessment (FSA) for Use in the IMO Rule-Making Process" as its deliberative procedure for developing cost-effective safety standards, and MSC.1/Cir. 1455 (2013) "Guidelines for the Approval of Alternatives and Equivalents as provided for in Various IMO Instruments" as its certification procedure for alternative designs using new technologies.

The IMO MASS Code is being developed as a goal-based standard referring to the above-mentioned guidelines. However, the requirements are expected to remain at the Tier 1 (Goal) and Tier 2 (Functional Requirements) levels, as the MASS Code aims to describe requirements that are commonly applicable to all MASS. Therefore, for the time being, it will be necessary to establish specific safety requirements based on an understanding of the characteristics of MASS for each individual ship.

When considering specific safety requirements for MASS as goal-based standards, it is important to comprehensively examine these requirements from three perspectives: the level of system autonomy, the operational envelope (OE) of MASS, and override methods. It is noted that MASS can achieve more advanced missions as the volume covered by the triaxial increases.

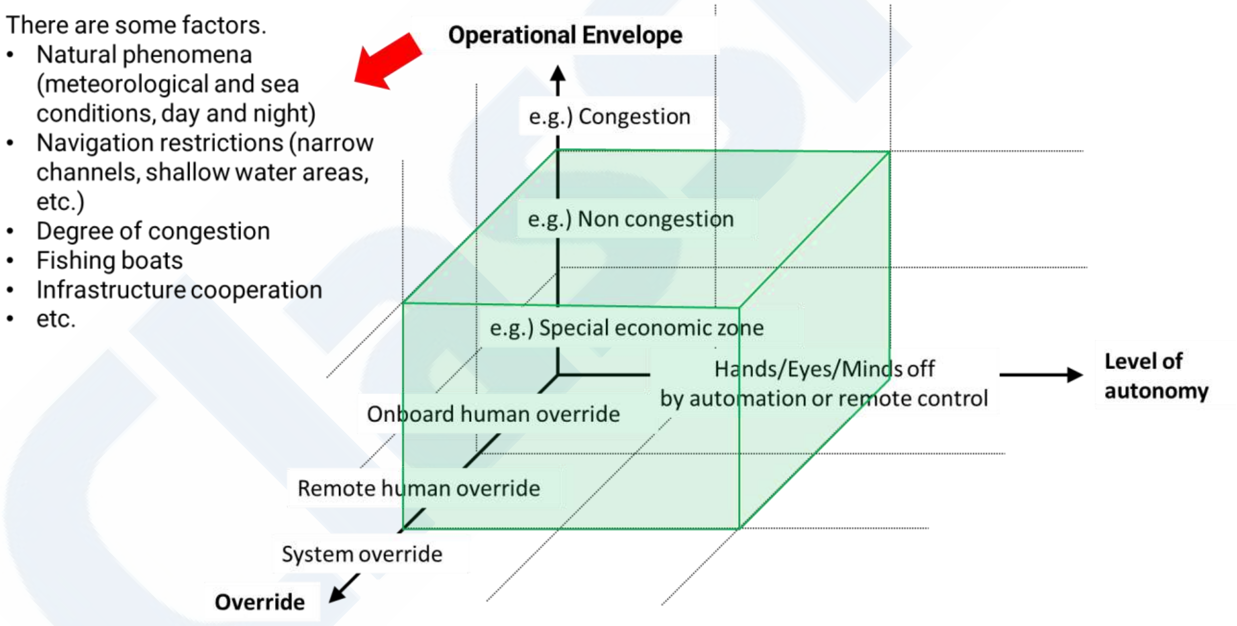

There are some factors.
• Natural phenomena (meteorological and sea conditions, day and night)
• Navigation restrictions (narrow channels, shallow water areas, etc.)
• Degree of congestion
• Fishing boats
• Infrastructure cooperation
• etc.
Operational Envelope
e.g.) Congestion
e.g.) Non congestion
e.g.) Special economic zone
Hands/Eyes/Minds off
by automation or remote control
Level of autonomy
Onboard human override
Remote human override
System override
Override

Figure 4.1 Three perspectives for considering safety requirements

4.2 System autonomy level

In the case of self-driving automobiles (automated driving technologies), the autonomy level is described by the terms Hands-off, Eyes-off and Mind-off. In MASS, this is interpreted as follows.

Hands-off

✓ The state in which the target onboard task is left to the system, but continuous human monitoring is required.

  - In the case of automated systems, the target task is simply left to the machine.
  - In the case of remote operation systems, a human operator in a remote operations centre (ROC) executes the target task. However, it is necessary to confirm that the stability of communication sufficiently ensured so that the remote operator can execute situational awareness required for the target task in the ROC (i.e., the necessary information is available without delay and without deterioration).
  - In the case of remote operation systems, the meaning of "continuous monitoring" is different from that of automated systems. It means that continuous monitoring for that the remote operation system can send and receive information properly.

Eyes-off

✓ The state in which the target onboard task is left to the system, and continuous human monitoring is not required. However, human supervisors remain in the target task (still "human-in-the-loop") so that they can respond to alarms, etc. if they sound.

Mind-off

✓ The state in which the target task onboard is left to the system, and continuous human monitoring is not required, and human supervisors do not have to remain in the target task but can perform other tasks. However, the human supervisors must remain ready to respond to fallback requests from the system. Although human supervisors' continuous monitoring is not required, drinking or sleeping, for example, is not allowed.

In one case, MASS might be operated in the Hands-off state in congested waters and in the Mind-off state in the open sea. In the other case, MASS could be operated on the Mind-off state, but when the system reliability decreases, switching to the Eyes-off state is needed to continue operation.

Table 4.1 System autonomy levels

	Onboard execution by a human	Continuous monitoring by a human	Human-in-the-loop
Hands-off	Not required	Required	Required
Eyes-off	Not required	Not required	Required
Mind-off	Not required	Not required	Not required

4.3 Operational envelope (OE)

It is important to determine the OE in advance. In general, as the level of system autonomy increases, the OE of MASS becomes smaller. Therefore, careful verification is required in order to expand the OE of MASS equipped with high-level-of-autonomy systems.

4.4 Override methods

MASS should be designed so that the system can be properly overridden if deemed necessary by the supervisor during operation. Consequently, when the supervisor detects abnormal system behavior during supervision or receives an external report to a MASS under supervision, an override should be executed as necessary, even if the system is in its ODD.

Override methods can be briefly organized by the entity responsible for override, as follows:

✓ Human onboard

✓ Human at ROC

✓ System(s)

There are the three possible cases, and the difficulty of override increases in the order of "human onboard," "human at remote locations" and "system(s)".

When verifying the safety of MASS, it is necessary to confirm two points: (1) the design specification provides the override appropriately, and (2) the procedures for override are properly established.

4.5 Remote control

In discussions of MASS, automation and remote control are often confused, but automation and remote control are fundamentally different technologies. For example, it is assumed that remote operators can serve in coastal areas where stable communications can be maintained, automated systems can be used in congested waters with assistance or monitoring by remote operators, and automated systems can be used in open seas without human monitoring. Berthing and unberthing may be done by an automated system or may be done by a remote operator.

In the case of automated systems, the validity of the algorithm is the main subject of evaluation, but in the case of remote operation systems, the stability of the communications between the MASS and the ROC is of paramount importance. To properly evaluate the safety of MASS, it is necessary to recognize the characteristic difference between automation and remote control, and decide which technology is to be applied to the target task. Therefore, safety assessments should be conducted considering both the ODD of the system and the OE of the MASS or the MASS system[2].

4.6 Summary

The required level of safety depends on "what technology is used in the MASS or MASS system and under what circumstances". The safety evaluation of the MASS verifies the ConOps to determine whether its OE is properly established by considering its level of autonomy and whether override can be properly conducted.

[2] If a remote operation centre (ROC) is involved in the operation, it is considered as a MASS system (MASS+ROC)

Chapter 5 Technology Differences between Conventional Ships and MASS

5.1 Overview

In conventional ships, the aforementioned “state in which risk is reduced to an acceptable level (ARC)” is maintained by human seafarers, but in MASS, ARC will be realized by autonomous navigation technology (automation and/or remote operation). In other words, it is necessary to confirm the technology differences between conventional ships and MASS, and to verify that the safety of conventional ships is not compromised by technology differences. This chapter summarizes the differences between the technologies installed in MASS and conventional ships.

5.2 Navigation task

5.2.1 Lookout function

For visual information:

To realize autonomous navigation, it is necessary to replace the crew's lookout with a system. A typical technology that is currently being developed is the camera system. The main functions of the camera system are as follows:

1. Visual information is acquired by the camera system.
2. Image analysis of the information acquired by the camera system is performed to detect and classify target objects such as ships and buoys.
3. The detected and classified targets are fused with information from sensors (radar, AIS, etc.) other than the camera system, and the result is superimposed on the camera image.
4. The result of fusion of the sensor information and camera system is transmitted to the situational awareness function, which will be described later, and is expected to be used as an information source for avoiding collisions and grounding.

The above is an example of using a camera system as an automated system, but it can also be used as a remote operation system, as follows:

1. Visual information is acquired by the camera system.
2. The information acquired by the camera system is transmitted to a remote operator without delay or degradation.
3. The remote operator performs situational awareness by utilizing auxiliary tools (AR markers, birds-eye view, etc.) if necessary.

Whether a camera system is used as an automated system or as a remote operation system, the ability to detect and classify targets appropriately from images captured by the system is an essential requirement. Also, whether the system functions properly under rainy, snowy and foggy conditions, under twilight and night-time conditions, and under backlit conditions must be organized as part of the ODD.

For auditory information:

In addition to visual information, a response to the sounds a seafarer hears is also required. The approach to handling sounds is also different in automated systems and remote operation systems.

When using as an automated system, after sound data is collected by a microphone, the machine (system) must be able to understand what the sound means. Technological development is necessary so that machines can understand the directions of sounds and the meaning of the sound pitch and length, but is difficult due to environmental noise, etc. Therefore, it may be necessary to develop some means of obtaining the information that seafarers have obtained from sound without directly hearing the sound, based on an essential analysis to determine the types of information that seafarers acquire from sound.

Technical development may be less difficult if it is used as a remote operation system. For example, since the remote operator can understand the meaning of the sound, no new technological development is required as long as the sound can be transmitted to the ROC with the same quality (without delay or degradation) as on board. In other words, it would be sufficient to give the remote operator the same “awareness” as an on-board lookout. However, if sound signal is actually heard, an on-board lookout can visually confirm which ship sounded it. For this reason, a tool for quickly checking the surrounding situation after the remote operator has “awareness” is essential. In addition to the camera systems described above, PTZ cameras or other devices that can be operated freely by remote operators may also be necessary.

5.2.2 Situational awareness function

Integration of information for situational awareness is already stipulated in the Integrated Navigation System (INS) standard, IMO Resolution MSC. 252(83), and we believe that this standard should also be followed in MASS. In the case of MASS, it is possible that equipment will be added to the sensing system (e.g., the aforementioned camera system and LiDAR) to measure the distance to quays when berthing and unberthing, etc. Therefore, this will increase the types of information that must be integrated, and technology to properly integrate these new types of information will be a target of new development.

The risk of collisions or groundings will be calculated based on the information integrated by the situational awareness function, and an avoidance route will be planned as necessary. In INS, calculation of this risk and planning of avoidance routes were the tasks of the seafarer, but in MASS, new requirements will need to be added because these ships will be automated or remotely controlled.

5.2.3 Route planning function for collision/grounding avoidance

This function is the most distinctive feature of MASS. Based on the integrated information, it is necessary to carefully examine what type of theory is to be used to calculate the risk of collisions or groundings, and what algorithm is to be used to plan an avoidance route when it is determined that an avoidance is necessary.

The ability to plan avoidance routes that comply with COLREGs is an important functional requirement. A certain level of quality is also required in terms of performance, such as collision avoidance behavior which does not make the own crew onboard feel wrong, and at the same time, the crew on other ships perceive anxiety

A method for properly evaluating this route planning function is necessary and is one of the most important focuses of the Society in MASS-related technology. The evaluation flow, evaluation metrics, evaluation scenarios, etc. have mostly been finalized through repeated exchanges of opinions with industry stakeholders, and we are currently in the stage of developing pass/fail thresholds.

5.2.4 Heading, speed and track control

In autonomous berth-to-berth navigation, existing track control systems (TCS) can be used in ocean areas, but more precise control of hull movement is required in waters such as narrow channels, bays and harbors, and during berthing and unberthing operations. In particular, because low-speed range control is required in harbors and during berthing/unberthing, advanced control logic is necessary to control the hull motion by making full use of devices such as thrusters and CPP as well as the rudder. The fact that a ship becomes susceptible to disturbances when entering a certain low speed range must also be taken into account. Even if the control logic is appropriate, it is necessary to tune various parameters appropriately, according to the capabilities of the individual ship.

Depending on the type and size of the MASS, it may be difficult to increase the autonomy level in low-speed range control berthing/unberthing for the time being. For example, even if the Hands-off level is achieved, can the system be trusted to reach Eyes-off? Unlike deviation from ODD during ocean navigation, failure of the system during low-speed range control or in berthing/unberthing means that the ship will immediately fall into a dangerous situation. Since there will be little time for an onboard seafarer or remote operator to take fallback or override action, the person in charge of fallback or override must always monitor the ship's operation in a ready state. Thus, in order to raise the autonomy level to Mind-off during low-speed control berthing/unberthing, it may be necessary to accumulate results over a considerable period of time. Alternatively, for berthing and unberthing, it may be necessary to consider using facilities on the port side.

5.2.5 System condition monitoring function (alert management system)

The IMO’s INS standard has provisions for alert management, and MASS should also be based on those provisions.

As a new functional requirement, it must be possible to issue appropriate alerts when the system installed in MASS deviates from the ODDi. It is also necessary to consider where the alert will be issued and whether cooperation with a ROC will be required. In particular, when alerts are to be issued at a ROC, the items that cannot be handled at the absence of seafarer onboard must be identified in advance.

5.2.6 Ship-shore communications and remote operations centre

One of the MASS use cases is remote operation. In order to operate a ship remotely, the ROC must be equipped accordingly.

Digital communication between MASS and shore must be ensured for remote operation. In addition to communication stability, redundancy is also required in the communication systems. shore It is necessary to consider whether it utilizes terrestrial mobile communications or satellite communications, how these are combined, and how the switching logic between two is designed.

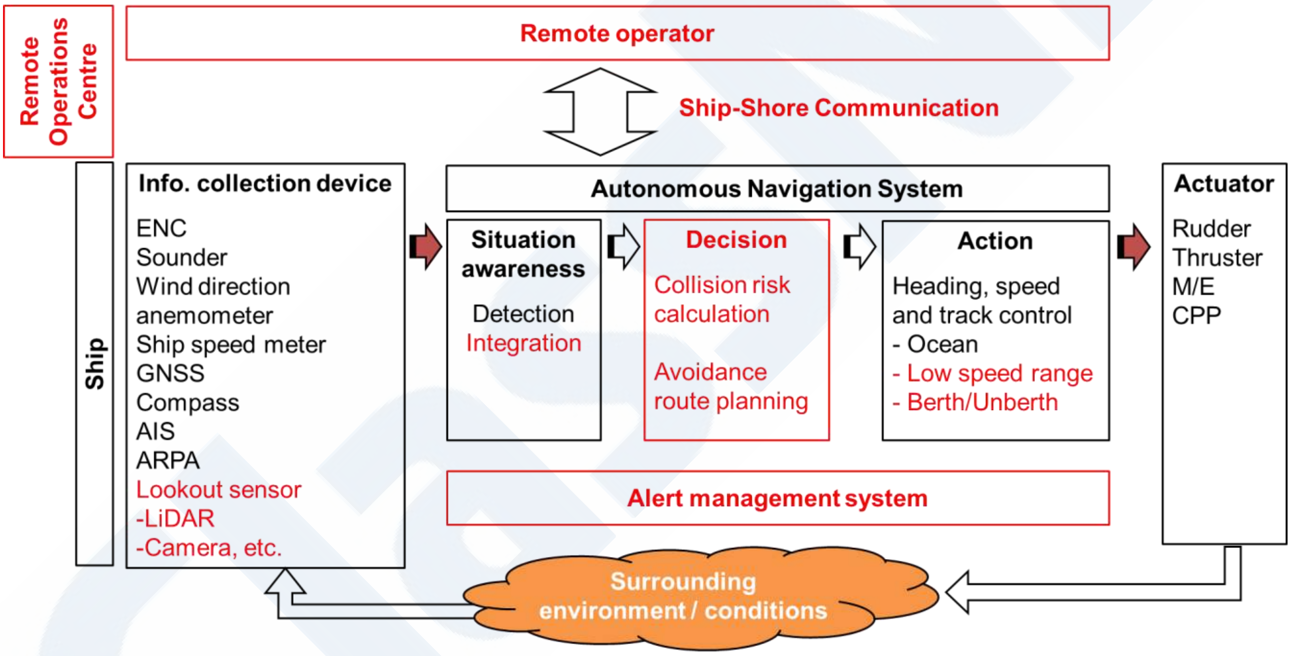


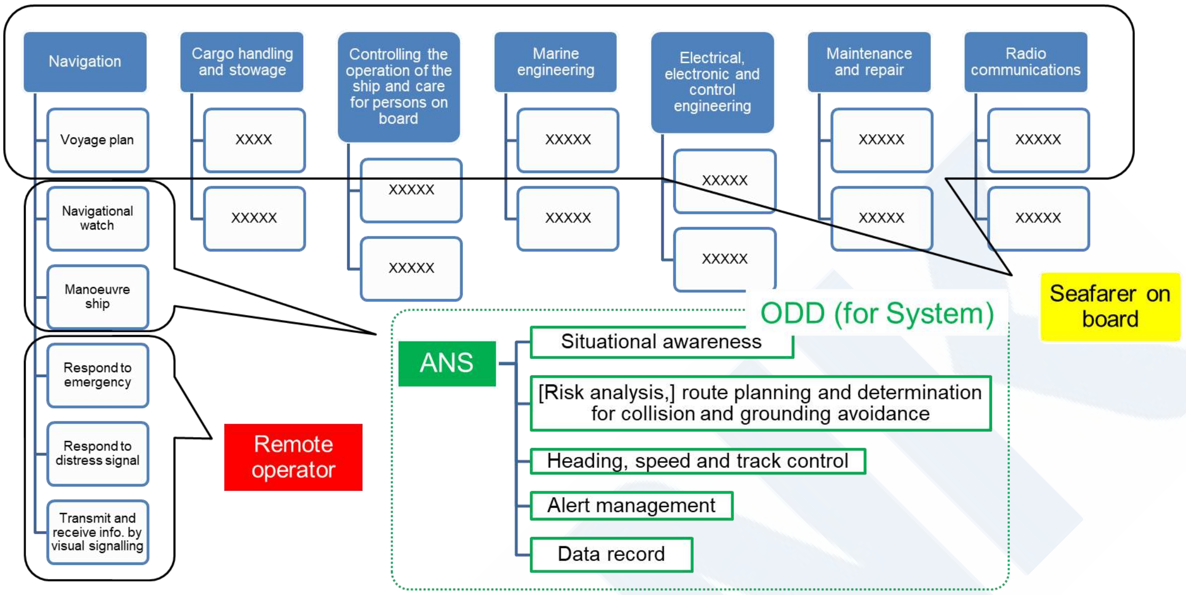
Figure 5.1 Technology differences between conventional ships and MASS in navigation tasks

5.3 Non-navigational tasks

A wide variety of tasks exist on ships. Navigation task is ranked the first priority, but even if navigation task is automated or remotely operated, uncrewed operations will not be possible unless other tasks are also automated or remotely operated.

Moreover, even in the case of navigation task, while the development of technology to the level of autonomous navigation watchkeeping (lookout, communication, steering, etc.) is progressing, automation/remote operation of other tasks such as mooring/unmooring, anchoring/un-anchoring, etc., is part of the future agenda.

In engine watchkeeping (main engine operation, patrols including troubleshooting, response to alarms, regular maintenance and inspections, etc.) and cargo management (cargo status management, hull attitude maintenance, etc.), it is assumed that technologies such as M0 (Periodically Unattended Machinery Space) and CBM (Condition Based Maintenance) will be incorporated in a way that suits the MASS use cases. However, as mentioned above, the use cases have not been clearly defined, and it is still unclear whether existing technologies can be applied without modification or new technologies will need to be developed.


Navigation
Cargo handling and stowage
Controlling the operation of the ship and care for persons on board
Marine engineering
Electrical, electronic and control engineering
Maintenance and repair
Radio communications
Voyage plan
XXXX
XXXXX
Navigational watch
Manoeuvre ship
Respond to emergency
Respond to distress signal
Transmit and receive info. by visual signalling
Seafarer on board
Remote operator
ODD (for System)
ANS
Situational awareness
[Risk analysis,] route planning and determination for collision and grounding avoidance
Heading, speed and track control
Alert management
Data record

(Provided by Japan Ship Technology Research Association)

Fig. 5.2 Example of onboard tasks and the scope of automated/remote operation

5.4 AI (Artificial Intelligence)

The movements to utilize AI to MASS has already begun. For example, application to the functionalities of lookout, collision avoidance route planning and ship motion control are being considered as follows.

- ✓ Lookout: Automatic recognition of environmental changes and obstacles, providing needed information in real time.
- ✓ Collision avoidance route planning: Predicting obstacles and hazards during navigation and providing optimal routes.
- ✓ Ship motion control: Minimizing ship shaking and maintaining ship speed.

In addition to improvements in computer processing performance such as GPUs, refinements in the database environment, and the open sourcing of tools and libraries needed for AI development, significant evolution in algorithms are a major reason for this progress. AI is expected to lead to resolve a wide range of problems. On the other hand, so-called black-box AI has emerged, and accountability for these AI systems has become an issue.

Self-supervised-learning is also a hot topic, but it may learn biased information. Even though AI is gaining attention, we must be aware of the reality that products are appearing only at the level of support for daily life, and are not being used in ways that lead directly to “safety.” Since the perspective of "unmanned" is also included in MASS, careful evaluation is needed when incorporating AI into automatic ship technology.. Considering these situations, the Society has tentatively established the following precautions when using AI.

Precautions

- ✓ Make AI a complement to human judgment. It is desirable to avoid using solution made by AI without human judgment.
- ✓ Clarify the basis of solutions derived by AI. If not, it is desirable to avoid using AI.
- ✓ Ensure that datasets are sufficiently diverse. If not, it is desirable to avoid using AI.
- ✓ Clarify who is responsible for AI systems.
- ✓ Avoid use of AI when the person responsible for the AI system cannot be identified.

Internationally, there are no evaluation criteria related to the safety of AI and there is a lack of consistency in evaluation methods. Therefore, it is important to standardize the evaluation process on a global scale as soon as possible.

5.5 Communications technology

Terrestrial radio waves in mobile communications networks, which are now routinely used for personal computers and mobile phones, have a limited range, so their use at sea is limited. For this reason, data communication using geostationary orbit (GEO) satellites is common on open sea where terrestrial radio waves cannot reach the ship. Redundant configurations can be secured by using and combining multiple frequencies. However, because of the distance from the earth, delays may occur, which may not be suitable for data communication when real-time performance is required.

In the near future, data communication services using low-earth orbit (LEO) satellites and high-altitude pseudo satellites (HAPS) will be available, and data communication with higher capacity and lower latency than GEO is expected to be possible at open sea.

In the longer term, a communication environment with enhanced robustness is expected to be established through the cooperative use of multilayered communication networks in space and the stratosphere. Implementation of this concept is already underway and technical hurdles are being cleared, and it is expected that a stable communication environment might be sustainably achieved, even on voyages.

The movements to establish international standards for the ship data communication field are also beginning. As an example, the International Organization for Standardization (ISO) established the Technical Committee (TC) ISO/TC 8 to develop international standards for the field of data communication on ships, and international standards such as the Inboard LAN Equipment Guidelines (ISO 16425), Inboard Data Server Requirements (ISO 19847) and Inboard Data Standards (ISO 19848) have already been established. Based on these standards, the ISO succeeded in establishing new general requirements for ship-to-shore data communication (ISO 23807) in March 2023.

It is necessary to clarify the rules for data communication in accordance with international standards while complying with the regional communication regulations applicable to the sea area to be navigated.

5.6 Changes in development methods (adoption of MBD and MBSE)

Development method based on systems engineering is one of notable changes. There are also cases where development methods using models have been adopted, such as Model Based Design (MBD), which is a development method using simulations, and Model Based System Engineering (MBSE), which uses models for systems engineering. Use of these tools has significant advantages when developing large and complex systems. For example, design changes that can be noticed only after verification by real tests at sea in conventional development can be greatly reduced by upstream modification in the design stage. Systems engineering is also required to provide necessary information so that processes can be traced, and since this information can be confirmed by an executable specification called a model, it can provide important materials for safety assessments. Therefore, not only developers, but also safety evaluators such as flag states and ship classification societies, should fully understand such changes in development methods.

Chapter 6 Risk Assessment

6.1 Overview

In the development of MASS, careful consideration should be given to avoid predictable failures under various operational scenarios. From this viewpoint, risk assessment is a very effective method for evaluating the safety of MASS.

As mentioned in sections 2.1 and 2.2, safety can be divided into intrinsic safety and functional safety, and risk that cannot be eliminated by intrinsic safety must be reduced to an acceptable level by cooperation with seafarers and implementation of system functions. Since MASS will delegate the role of safe navigation traditionally performed by seafarers on conventional ships to automated systems and/or remote operators, it is necessary to focus on the difference between MASS and conventional ships and confirm that risk is reduced to the same level or less than that of conventional ships. Therefore, MASS should be designed so that reasonably predictable and preventable accidents do not occur under both normal and emergency conditions. To achieve this, risk assessment should be carried out based on an accurate understanding of the characteristics of MASS that emerge from the clarification of the basic elements for ensuring safety described in section 2.4. In particular, it is important to ensure that the relationship between ODD and fallback is properly designed and is examined under various scenarios, including critical scenarios where fallback and MRM are required, after specifically assuming the use cases of MASS.

Risk assessment in the development of MASS has two objectives: The first is to extract functional requirements, including safety functions, in concept design, and the second is to ensure that risk is reduced to an acceptable level by the established safety functions. Risk assessment can also be considered a very important process in safety assessments of MASS, since the accident scenarios extracted in the risk analysis process will be used for simulations and field sea trials.

6.2 Risk analysis

Risk assessment refers to a series of processes consisting of hazard identification, risk analysis to assess the magnitude of risk, and risk control options. In other words, the risk assessment implemented beforehand or during operation consists of hazard identification, risk extraction and estimation of its magnitude, assessment of whether the extracted risk is acceptable or not, and formulation and implementation of measures to suit the magnitude of the risk. The general flow of risk assessment is shown in Figure 6.1.

There are several risk analysis methods. In the field of maritime risk analysis, SWIFT (Structured What IF Technique) is commonly used to identify hazards through brainstorming by repeating questions that assume deviations from normal conditions such as “what if.” Other techniques include Failure Modes and Effects Analysis (FMEA) and HAZard and OPerability Study (HAZOP).

Systems theory approaches such as STAMP/STPA (Systems-Theoretic Accident Model Processes/System-Theoretic Process Analysis) have also attracted attention as safety analysis methods for large and complex systems. STAMP/STPA is an analysis method that considers hazard factors in functional units that interact with each other. There is a view that STAMP/STPA is useful for risk analysis in the early design stage of large and complex systems. It is also considered useful to separate the analysis methods according to the design stage. The application of STAMP/STPA to MASS has already been verified in several papers.

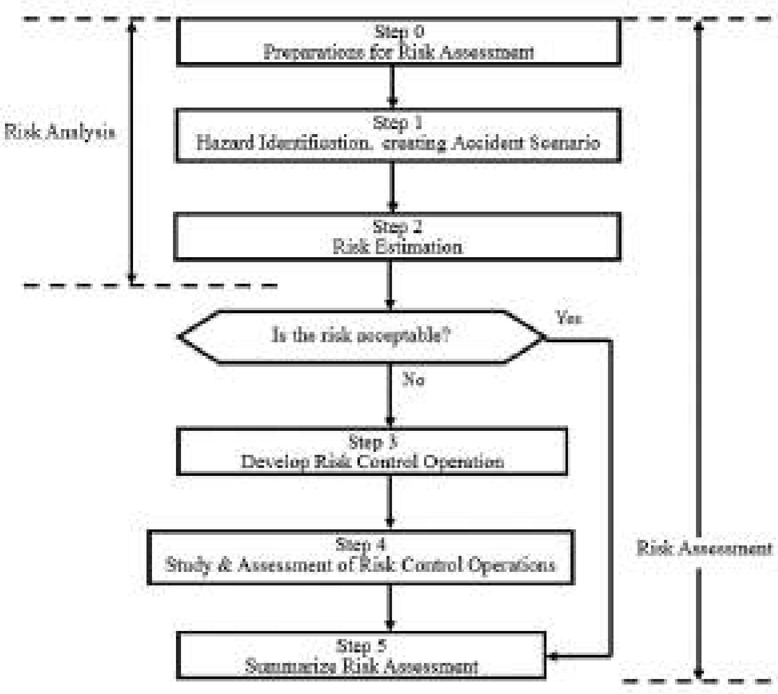

Step 0
Preparations for Risk Assessment
Risk Analysis
Step 1
Hazard Identification, creating Accident Scenario
Step 2
Risk Estimation
Is the risk acceptable?
Yes
No
Step 3
Develop Risk Control Operation
Step 4
Study & Assessment of Risk Control Operations
Risk Assessment
Step 5
Summarize Risk Assessment

Figure 6.1 General flow of risk assessment

6.3 Scope and methodology for conducting risk assessments

The society considers the scope and methodology for conducting risk assessments for MASS as follows:

1. Conceptual design of MASS: SWIFT, STAMP/STPA
   Based on the ConOps of the MASS, the intended functions and their functional requirements needed to achieve the mission are extracted, together with the required safety functions.
2. Detailed design: FMEA, HAZOP
   The main focus in detailed design is on identification of hazards to the system itself for each intended function identified by the risk analysis during conceptual design. Confirming the reliability of the system units that constitute the MASS will make it easier to conduct the risk assessment for installations that will be conducted later on.
3. Ship on board: SWIFT, HAZOP, STAMP/STPA
   Assuming that the risks arising from the system alone have already been verified by the risk assessment in the detailed design of the system, a risk assessment is carried out with the main focus on risks relating to the linkage between the ship and the system.

6.4 Considerations when conducting risk assessments

When conducting risk assessments for MASS, at least the following points should be kept in mind:

- ✓ Since the uncertainty associated with the novelty of MASS technologies (differences from existing technology) is a risk, designers should strive to reduce this uncertainty by identifying the relevant hazards through a risk-based approach and taking appropriate measures to address them.
- ✓ Potential risks need to be assessed comprehensively and systematically.
- ✓ The concept in risk assessment will change between the most recent technological developments (in which machines carry out some human tasks) and the distant future (fully autonomous operation by machines). In particular, recent technological developments have a strong nuance of support, in which machines conduct some tasks. In this case, the risk is revealed in the Human Machine Interface (HMI).
- ✓ The analysis using STAMP/STPA is limited to the identification of loss scenarios and does not provide a framework for carrying out semi-quantitative or quantitative risk analysis. From the perspective of safety assessment of MASS, it is desirable to use in combination

with another method to determine whether the risks posed by the identified scenarios are acceptable.

✓ Since more complex systems require more equipment and a greater amount of analysis, it is also useful to combine the strengths of each assessment method when conducting a comprehensive safety verification, for example, by first focusing the analysis on humans and equipment, and then using FMEA to evaluate the risks between equipment or equipment alone depending on the system.

✓ Since a quantitative risk analysis is not possible with STAMP/STPA, it is necessary to carefully establish a framework for discussing the necessity of measures among stakeholders.

✓ FMEA is suitable for failure analysis within equipment alone or in a closed scope of systems. However, since MASS technologies such as ANS are highly novel, external factors should also be considered in addition to the failure mode of the equipment as a risk that takes into account specific operational aspects. Therefore, risk analysis in conjunction with SWIFT or STAMP/STPA is required.

✓ The gap in the assumptions on MASS use should be filled by risk assessment meetings, because the assumptions of developers and users may differ. In some cases, this will lead to correction of the ConOps.

✓ For highly novel equipment specific to MASS, such as a system which has route planning function for collision/grounding avoidance, the need for a risk assessment of the equipment itself must be adequately considered. If a risk assessment is deemed necessary, it is important that the accident scenarios and critical scenarios extracted from this risk assessment are used for additional validation, e.g., by simulation tests.

✓ Since the timing of actions such as the beginning or end of autonomous operation and emergency stops by fallback makes an especially large contribution to safety, it is important to carefully analyze each possible scenario.

Chapter 7 Framework for Safety Assessment

7.1 Framework

Since MASS is expected to have a variety of use cases, it is necessary to consider the required safety level based on “what kind of technology is intended to be used in what situation”. For this reason, it is necessary to involve the flag states and classification societies from the initial stage and conduct goal-based discussions.

Evaluating the safety of MASS requires verification that considers the entire life cycle of the system, from design and development to installation and operation. In the conceptual design and initial design stages of MASS, the functions/roles that should be fulfilled as a system are clarified, and in the detailed design stage, the functions that each system component should fulfill are clarified. In each stage, a risk assessment should be performed to verify the validity of the design. After the design is completed, tests are required to prove that the developed components and systems have the functions as designed, so it is necessary to prepare the plan for this test at the time of design.

With these scopes in mind, the Society considers the procedure for safety evaluation when proceeding with design development based on the V-model shown in Figure 7.1 as follows.

1. Share the ConOps and core system features (including the ODD) of the target MASS with the related parties.
2. Conduct a risk assessment in the conceptual design stage. Extract the functional requirements (including safety functions) and functional requirements of the target system and form a consensus among the stakeholders (flag state, ship classification society, developer, ship owner, etc.).
3. Confirm with drawings that the functions extracted by the risk assessment are appropriately reflected in the relevant drawings. In particular, confirmation of the safety functions to be implemented as risk mitigation measures is an important point.
4. Confirm that these functions are properly implemented and operate properly through operation tests. Therefore, it is necessary to prepare a test plan in the design stage.
5. For the quality of the system, the Society will conduct a document-based review to confirm that the system has been developed and manufactured in a process, including design, procurement, manufacturing, inspection, change management, approved by a third party organization, and that all the necessary pre-verifications have been completed. The Society may require tests under specified conditions.
6. When the system is manufactured, proper operation must be confirmed by a shipping test.
7. In principle, system integration tests should be conducted onboard. This process should be rationalized by making effective use of simulations. At this time, it is necessary to verify the accident occurrence scenarios and important scenarios extracted during the risk assessment (that is, the scenarios leading to fallback and MRM, and scenarios related to additionally installed risk mitigation methods).
8. For sea trials, the minimum items to be implemented in the actual sea area will be identified in steps (1) to (3), and the final decision will be made after discussion among the stakeholders on the tests to be performed in the actual sea area, depending on how far tests could be substituted up to step (7).
9. Utilize the vulnerability database (See section 7.3 for details).

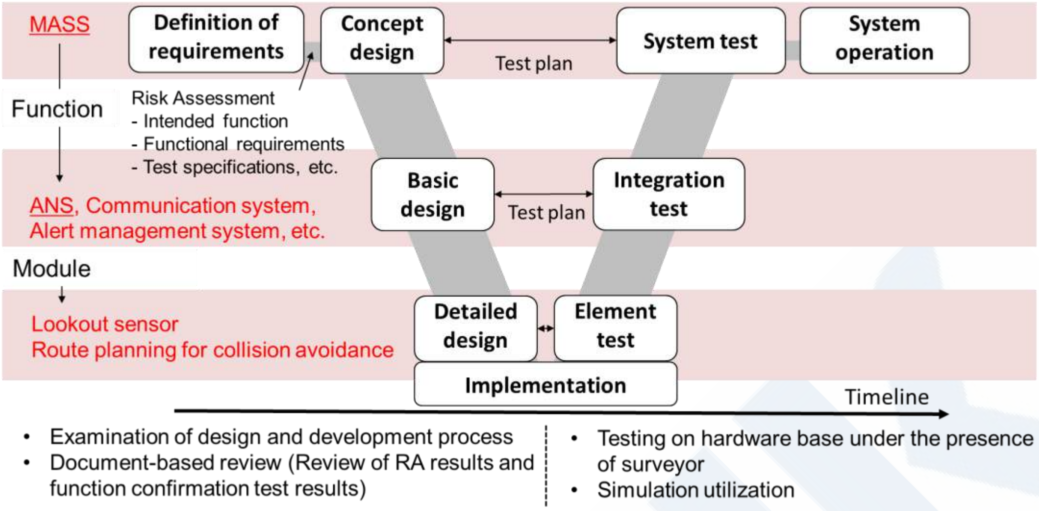

MASS
Definition of requirements
Concept design
Test plan
System test
System operation
Function
Risk Assessment
- Intended function
- Functional requirements
- Test specifications, etc.
ANS, Communication system,
Alert management system, etc.
Basic design
Test plan
Integration test
Module
Lookout sensor
Route planning for collision avoidance
Detailed design
Element test
Implementation
Timeline
• Examination of design and development process
• Document-based review (Review of RA results and function confirmation test results)
• Testing on hardware base under the presence of surveyor
• Simulation utilization

Figure 7.1 Safety assessment based on V-model

7.2 Consideration for applying the framework

✓ Conduct safety verification efficiently and effectively by the above flow, focusing on technology differences with conventional ships.

✓ If it is considered necessary to check the safety and functionality of interoperation across the multiple systems before the whole system integration, simulation tests such as HILS should be carried out. After the simulation tests, onboard testing should be conducted in the final environment where whole integrated systems interact, and the following items should be confirmed by actual operation.

- Function as intended
- Safety response to faults caused by equipment internal or external to the system
- Safety of interoperation between multiple systems

When it is difficult to verify the scenarios in actual operation, it is allowed to use simulation, but the accident scenarios and critical scenarios identified during the risk assessment (scenarios leading to fallback or MRM and scenarios related to additional risk control methods installed) should be verified.

✓ Safety goals must be technically and economically feasible. In addition to the risks to human life and environment, it is also important to set safety goals with the various risks in mind to life, society, and the environment posed by the operation or non-operation of MASS. Although the number of serious accidents involving ships is smaller than that of automobiles, once an accident happens, the impact is extremely large. MASS is expected to provide a solution to social issues such as the shortage of seafarers. In other words, if MASS were to become inoperable, we could come to a standoff situation in the future. With this in mind, we need a process to link new technologies that have not yet been proven to be implemented in society. In principle, we must avoid creating direct damage to people, the environment, and so on. Moreover, to be able to estimate how MASS would affect social convenience and economic efficiency, the perspectives of various stakeholders need to be taken into account.

✓ One of the aims of sharing the ConOps and safety goals among stakeholders is to eliminate information asymmetry among the developers, users and administrative authorities, which sometimes occurs due to a lack of information sharing between them in terms of demanding and supplying. Sharing the specific image of the technical readiness level (TRL) currently being developed for the technology from the developer side and the types of businesses that users intend to conduct with MASS with the administrative side will make it possible to establish socially acceptable safety standards.

✓ One major characteristic of the maritime industry is the existence of classification societies as safety evaluation organizations. Since classification societies can also contribute to resolving the problem of information asymmetry, information should be actively shared with classification societies.

✓ In addition to confirming that the design of the target MASS satisfies safety standards, it is also important to operate the MASS properly. From this perspective, the operator of MASS should be an entity that is competent to use such a highly advanced system and is able to undertake its responsibilities.

7.3 Vulnerability database

7.3.1 Background

As social implementation of MASS is now becoming a reality, the time has come to consider a new framework which supports the social implementation of state-of-the-art technologies and solutions that transcend the conventional framework, that is, a framework which can complement imperfect regulations and institutions. It is also necessary to accelerate introducing functional safety and systems engineering to the maritime industry.

Since a public institution such as government agencies and classification societies will be responsible for discovering potential accident scenarios for MASS from the viewpoint of social safety, it will be necessary to establish a mechanism for discussing the scope of responsibility for the response.

7.3.2 Overview of vulnerability

Vulnerability is a concept adopted by the National Institute of Standards and Technology (NIST) in the United States, which publishes many security-related documents. For example, the Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 (April 2018) describes the consideration of vulnerability when judging risk and the disclosure cycle of vulnerability information. The SP-800 series also requires reuse of vulnerability information. It is interesting to note that vulnerability information is made available from a variety of public and private sources, including the National Vulnerability Database (NVD). In other words, since NIST assumes that information security is fragile and vulnerabilities will always be breached, the scope of security includes the response to cases where a vulnerability has been breached.

7.3.3 Safety and vulnerability

As mentioned in Chapter 2, ISO/IEC GUIDE 51: 2014 defines safety as “freedom from risk which is not tolerable”. Safety includes intrinsic safety and functional safety. As systems become more complex, the concept of functional safety, which ensures an acceptable level of safety by installing functional devices (safety functions), has been adopted in various industries. In MASS as well, safety is ensured by making full use of safety functions based on the concept of functional safety.

However, if vulnerability remains in a safety function, it poses a great risk, so it is necessary to quickly and accurately collect information on the vulnerability of safety functions.

7.3.4 Example of the commercial aviation industry

The commercial aircraft industry, which achieved rapid development after World War II, has a history of improving safety by revising rules based on “accidents”.

As with the maritime industry, the International Civil Aviation Organization (ICAO), a subordinate organization of the United Nations, establishes international standards for the civil aviation industry, and member countries have introduced frameworks which obligate them to develop domestic laws that comply with these international rules. However, there are no third-party organizations similar to the classification societies in the maritime industry.

This rule was enacted as an annex to the Convention on International Civil Aviation (commonly known as the Chicago Convention) adopted in 1944. As one important feature, fields related to aircraft design, manufacturing, operation, etc. are inclusively covered under one Convention Annex.

Annex 13 defines “Aircraft Accident and Incident Investigation”. Its Chapter 3 GENERAL OBJECTIVE OF THE INVESTIGATION states that “3.1 The sole objective of the investigation of an accident or incident shall be the prevention of accidents and incidents. It is not the purpose of this activity to apportion blame or liability”. This expresses the idea that it is necessary to recognize that the enacted regulations are not perfect, and to learn from actual accidents and incidents in order to prevent future accidents and incidents which have the same cause, since accidents and incidents are unavoidable events in aircraft. In fact, the United States has enacted a law that does not impose criminal penalties except in cases of intentional or malicious negligence in order to enable accurate interviews for investigations of aircraft accidents.

Based on this spirit, in the commercial aircraft industry, a framework has been introduced for each industry stakeholder (including the government authorities of each country) to report, disclose, analyze and formulate countermeasures not only for accidents and incidents but also for various failure cases, and a framework for improving aviation safety on a daily basis has been put in place.

The important parts of this safety activity can be summarized in the following two points.

(1) Accidents and incidents are inevitable events, and measures should be taken to lead to improved safety.

(2) Collecting information on various defects including accidents and incidents, we should make the information available to public.

This is an example showing that the concept of vulnerability is very effective in improving safety. Figure 7.2 shows an overview of the PDCA cycle based on vulnerability in the commercial aircraft industry.

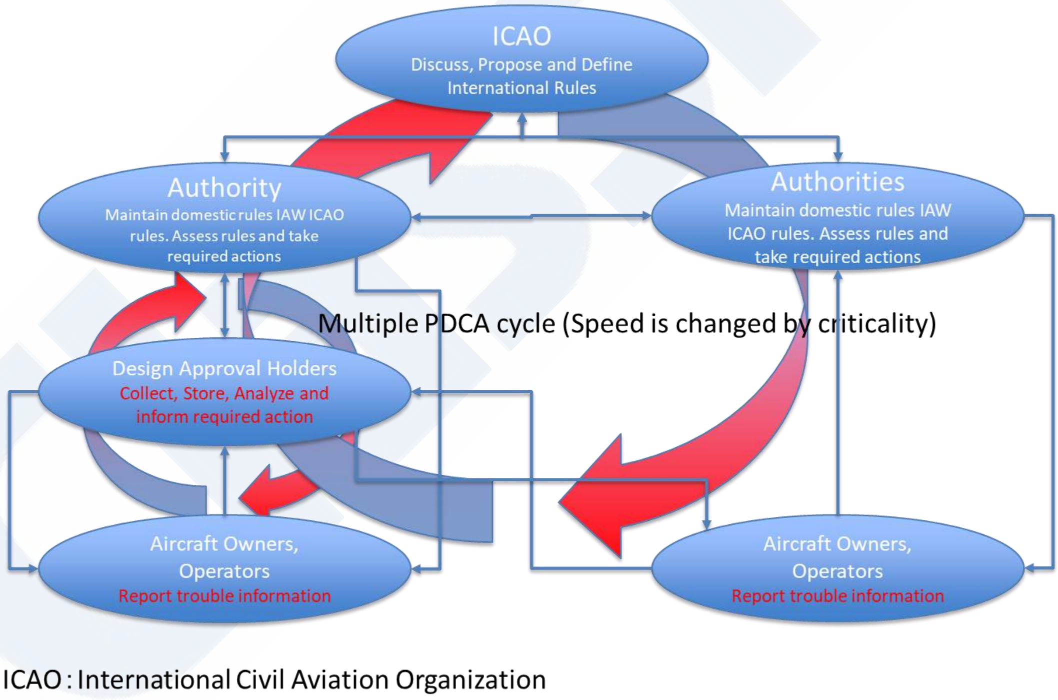

ICAO
Discuss, Propose and Define International Rules
Authority
Maintain domestic rules IAW ICAO rules. Assess rules and take required actions
Authorities
Maintain domestic rules IAW ICAO rules. Assess rules and take required actions
Multiple PDCA cycle (Speed is changed by criticality)
Design Approval Holders
Collect, Store, Analyze and inform required action
Aircraft Owners, Operators
Report trouble information
Aircraft Owners, Operators
Report trouble information
ICAO : International Civil Aviation Organization

Figure 7.2 Overview of the PDCA cycle based on vulnerability in the commercial aircraft industry

7.3.5 Application to MASS

As mentioned above, accepting a certain degree of imperfection and considering what is the most appropriate operation method under this condition is an important mindset when confronted with new technologies. It is also necessary to create a framework for social acceptance of those technologies. The framework of collecting cases related to vulnerability, creating a database and using it to improve the accuracy of safety evaluations has already been adopted in other industries, and we believe that it will also be an effective approach for MASS.

In constructing a vulnerability database for MASS-related technologies, it is necessary to organize the classification and collection methods, but these methods should be based on a recognition of the fact that vulnerability tends to decrease as technology maturity increases. Therefore, we propose that the vulnerability levels be divided into two axes, that is, the status of the technology and the application area, and the frequency of reporting be set according to the level, as shown in Tables 7.1 and 7.2. Although these tables are only examples, when setting the levels and reporting frequency according to the level of technical maturity at the time of social implementation, periodic reviews corresponding to improvements in the level of technology maturity should be considered.

Table 7.1 Example of vulnerability classification

		Technology Status		
		Proven	Limited field history	New or unproven
Application Area		SOLAS mandatory	On-shore ISO/IEC	Others
Known	On-market products	1	2	3
Unknown	On-market products	2	3	4
New	Development / Update	3	4	5

Table 7.2 Example of vulnerability reporting frequency

	Level of Vulnerability				
	1	2	3	4	5
A	Immediately				
B	Semi-annually	Quarterly			Monthly
C	Annually	Semi-annually	Quarterly	Monthly	

A. Defects that caused an accident

B. Defects that caused disengagement of autonomous mode

C. Other defects found during operation

7.3.6 Utilization in risk assessment

Risk assessment is also being carried out in the MASS demonstration project, and the safety of MASS is evaluated by analyzing the risks inherent in the new technology itself and the risks when the technology is installed on ships while verifying the differences with the existing technology. However, in the trial verification stage, it is very difficult to extract all the hazards of new technologies that have no track record and accurately estimate the risks that they may cause. Therefore, at present, evaluations are made in conjunction with the safety margin set for the demonstration experiments.

For social implementation, it will be necessary to optimize this safety margin. In this regard, we believe that incorporating the concept of vulnerability is one option. For example, use of a vulnerability database will ensure that risk assessments can always be performed based on the latest information. This will not only prevent the omission of verification of important risks, but will also contribute to prevent excessive safety measures, that is, rationalization of safety margins.

7.3.7 Building and implementing the PDCA Cycle

In the development phase, information and experiences such as failure cases and near-miss incidents should be shared with the rule development and safety evaluation side from the stage of demonstration experiments in order to prevent omission of verification when certificating the technology.

In the operation phase, considering the fact that new technologies with little track record can be understood only after they are used, feedback from seafarers, who are the users, should be appropriately distributed to those responsible for technology development, rule development and safety evaluation. This will lead to improvements in technology, regulations and evaluation. Building a vulnerability database and appropriately using the PDCA cycle will lead to improve the safety of MASS operation.

First, the vulnerability database is expanded, and the PDCA cycle is constructed based on vulnerability from the standpoints of technology development, rule development and safety evaluation. Then, this PDCA cycle should continue to be used effectively. We believe that such a framework is necessary for MASS, in which hardware failures, software defects, operation and management problems and other factors are interrelated in a complex manner.

Chapter 8 Sustainability

MASS is just a part of the means to be a sustainable maritime industry. To achieve a sustainable social system, MASS should be developed in a way that closely matches the changing workstyles and roles of seafarers, and changes in education and logistics should be required to accommodate these trends. As this suggests, the important thing is whether to envision a new social system with MASS at its core from a broader social perspective, rather than simply limiting MASS to technological innovations for ships.

For example, MASS is expected to provide a countermeasure to the social issues such as seafarer shortage by the voyage with reduced number of crews or uncrewed operation as one of the solutions. Considering social implementation of MASS, one of issues is how the seafarer onboard can cooperate with port facilities to get the safe navigation like the one with the conventional ship, etc. Specifically, MASS should be able to handle with ship’s routing system, navigation warnings, meteorological services and warnings, Ice Patrol Service, vessel traffic services, etc. which are described in SOLAS Chapter V. Technical breakthroughs will be required for MASS to handle all of these items. Since MASS is expected to provide a solution to the social problem of the shortage of seafarers, it is necessary to develop technologies for the port facility side rather than focusing entirely on technological development for ships. For example, developing the following technologies on the basis of cooperation with MASS on the port side can accelerate social implementation.

✓ Docking and mooring equipment
✓ Equipment for safe embarkation
✓ MASS traffic control
✓ Digitization of route signs
✓ Expansion of communications infrastructure
✓ Digitization of geographic information

Remote operation of MASS is being discussed, and this relates to transforming the workstyle of seafarers. However, whether the skills of remote operators should be lower, higher or the same as those of conventional seafarers also needs to be discussed.

Education and training are also being discussed. Acquisition of a basic knowledge of MASS and proficiency in the operation of automated and/or remote operation systems are indispensable for social implementation of MASS, and the division of roles should be determined among industry, government and academia.

A fundamental element in the effective promotion of these discussions is to share the information among industry, government and academia. Since MASS is becoming drivers of social change, it is important for stakeholders to be aware of the potential benefits of technological advances to society from their respective positions.

Chapter 9 Conclusion

The development of MASS-related technologies is accelerating, and demonstration experiments are being actively conducted. As social implementation of MASS in 2025 is now becoming a reality, the time has come to consider a new framework which supports the social implementation of state-of-the-art technologies and solutions that transcend the conventional framework, that is, a framework which can complement imperfect regulations and institutions. It is also necessary to accelerate introducing functional safety and systems engineering to the maritime industry. Since autonomous navigation technology is a new technology with no track record, the problem that “you won't know until you use it” inevitably remains. In view of these matters, the Society has compiled this White Paper on a safety assessment framework for the MASS design and development phases and the PDCA cycle in the operation phase.

For safe social implementation of MASS, it is necessary to confirm that the system level of autonomy, the extent of the MASS operational envelope and system override methods are appropriately designed based on the specific assumptions of MASS use cases. Therefore, in the design and development phases, the Society will focus on the technology differences between the existing technology (i.e., conventional ships) and MASS, and conduct rational, effective and economical assessments of both the safety evaluation of the new technologies themselves and the evaluation of the entire system that integrates them. A framework for safety evaluation when proceeding with design development based on the V-model was established to enable implementation in a timely manner.

Since autonomous navigation technology has no track record and can only be understood when it is used, it will be necessary to devise the actual operation method after recognizing the imperfections of the technology. As part of this effort, a mechanism for collecting data on defects and near-miss incidents found after implementation and constantly updating regulatory requirements and evaluation methods by third parties will be needed. As a mechanism for this, the Society proposes using a vulnerability database in the operation phase. It is important to improve technology, regulations and evaluation by appropriately distributing feedback from users (i.e., seafarers) to technology development, rule development and safety evaluation. The Society believes that constructing a vulnerability database and appropriately applying the PDCA cycle will lead to improved safety in MASS operation.

MASS is just a part of the means to be a sustainable maritime industry. To achieve a sustainable social system, MASS should be developed in a way that closely matches the changing workstyles and roles of seafarers, and cooperation with education and logistics is also important. To create a complete image of a new social system with MASS at its core, rather than confining ourselves to only technological innovations for ships, it is important for stakeholders to be aware of the potential benefits of the evolution of technology to society from their respective standpoints as a broader framework. The Society believes that classification societies, which are in a neutral position, can play a significant role in this regard. The Society would like to encourage further discussion on social implementation of MASS from this viewpoint.

Bibliography

IMO and IACS documents

1. IMO MSC. 1/Circ. 1604: INTERIM GUIDELINES FOR MASS TRIALS, 2019.
2. IMO Resolution A. 1103(29): PRINCIPLES TO BE CONSIDERED WHEN DRAFTING IMO INSTRUMENTS, 2015.
3. IMO MSC. 1/Circ. 1394/Rev. 2: GENERIC GUIDELINES FOR Developing IMO GOAL-BASED STANDARDS, 2019.
4. IMO MSC-MEPC. 2/Circ. 12/Rev. 2: GUIDELINES FOR FORMAL SAFETY ASSESSMENT (FSA) FOR USE IN THE IMO RULE - MAKING PROCESS, 2018.
5. IMO MSC.1/Circ.1455: GUIDELINES FOR THE APPROVAL OF ALTERNATIVES AND EQUIVALENTS AS PROVIDED FOR IN VARIOUS IMO INSTRUMENTS, 2013.
6. IMO MSC. 1/Circ. 1638: OUTOCOME OF THE REGULATORY SCOPING EXERCISE FOR THE USE OF MARITIME AUTONOMOUS SURFACE SHIPS (MASS), 2021.
7. IACS UR E22/Rev. 2: On Board Use and Application of Computer based systems, 2016.
8. IACS UR E26: Cyber resilience of ships, 2022.
9. IACS UR E27: Cyber resilience of on-board systems and equipment, 2022.

Related ClassNK documents

1. Guidelines for Automated/Autonomous Operation on ships, Ver. 1.0, 2020.
2. Risk Assessment Guidelines, Ver. 1.0, 2009.
3. Guidelines for Technology Qualification, Ver. 1.0, 2022.
4. Guidelines for Designing Cyber Security Onboard Ships, Second Edition, 2020.

Industry standards

1. ISO 31073:2022, Risk management – Vocabulary.
2. ISO/IEC/IEEE 29148: 2018, Systems and software engineering - Life cycle processes - Requirements engineering.
3. ISO/TS 23860: 2022, Ships and marine technology - Vocabulary related to autonomous ship systems.
4. ISO/IEC Guide 51: 2014, Safety aspects — Guidelines for their inclusion in standards.
5. ISO 16425: 2013, Guidelines for the installation of ship communication networks for shipboard equipment and systems.
6. ISO 19847: 2018, Shipboard data servers to share field data at sea.
7. ISO 19848: 2018, Standard data for shipboard machinery and equipment.
8. ISO 23807: 2023, General requirements for the asynchronous ship-shore data communication.

Technical documents

1. Maritime Bureau Ministry of Land, Infrastructure, Transport and Tourism, Safety Guidelines for Maritime Autonomous Surface Ships (MASS) (available only in Japanese), 2020.
2. VTMIS, EU OPERATIONAL GUIDELINES FOR SAFE, SECURE AND SUSTAINABLE TRIALS OF MARITIME AUTONOMOUS SURFACE SHIPS (MASS), 2020.
3. Norwegian Maritime Authority, Guidance in connection with the construction or installation of automated functionality aimed at performing unmanned or partially unmanned operations, No. RSV 12-2020, 2020.
4. S Kuwahara et al., Research and Development of Collision Risk Decision Method for Safe Navigation and Its Verification, ClassNK Technical Journal, No. 3(2021), pp. 13-40.
5. H Hashimoto et al., Development of AI-based Automatic Collision Avoidance System and Evaluation by Actual Ship Experiment, ClassNK Technical Journal, No. 3(2021), pp. 41-50.

6. T Suzuki, Challenge of Technology Development through MEGURI 2040, ClassNK Technical Journal, No. 3(2021), pp. 51-58.
7. S Inoue and H Mori, Development of Automated Ship Operation Technologies, ClassNK Technical Journal, No. 3(2021), pp. 59-66.
8. S Miyoshi and T Ioki, Development of Maneuvering System for Realizing Autonomous Ships, ClassNK Technical Journal, No. 3(2021), pp. 67-79.
9. T Yamada, Safety Evaluation for Technologies Related to Autonomous Ships, ClassNK Technical Journal, No. 3(2021), pp. 81-92.
10. T Nakashima, et al., Model-Based Design and Safety Assessment for Crewless Autonomous Vessel, MTEC-ICMASS-2022, Vol. 2311 (2022).
11. T Yamada, et al., Evaluation of effectiveness of the STAMP / STPA in risk analysis of autonomous ship systems, MTEC-ICMASS-2022, Vol. 2311 (2022).
12. Japan Ship Technology Research Association and National Maritime Research Institute, Risk analysis procedure for MASS, Report on MEGURI2040 (available only in Japanese), 2021.
13. M Minami et al, Development of the Comprehensive Simulation System for Autonomous Ships, MTEC-ICMASS-2022, Vol. 2311 (2022).
14. DNVGL, Autonomous and remotely operated ships, DNVGL-CG-0264, 2018.
15. BV, Guidelines for Autonomous Shipping, Guidance Note NI 641 DT R01 E, 2019.
16. ABS, ABS advisory on autonomous functionality, 2020.
17. National Institute of Standards and Technology, Frame work for Critical Infrastructure Cybersecurity Version 1.1, 2018, https://www.ipa.go.jp/files/000071204.pdf
18. National Institute of Standards and Technology, Computer Security Resource Centre, https://csrc.nist.gov/publications/sp
19. California Department of Motor Vehicles (DMV)：Article 3.7, Testing of Autonomous Vehicles, https://www.dmv.ca.gov/portal/file/adopted-regulatory-text-pdf/
20. California Department of Motor Vehicles (DMV)：Article 3.8, Deployment of Autonomous Vehicles, https://www.dmv.ca.gov/portal/file/adopted-regulatory-text-pdf/
21. International Civil Aviation Organization, Annex 13, To the Convention on International Civil Aviation, Aircraft Accident and Incident Investigation.
22. I Misra and L Maaten, Self-supervised learning for visual recognition, In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (2020), pp. 9565-9574.
23. M Caron et al., Deep clustering for unsupervised learning of visual features, In Proceedings of the European Conference on Computer Vision (2018), pp. 132-149.
24. X Chen et al., A simple framework for contrastive learning of visual representations with weak augmentations, In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (2021), pp. 6555-6564.
25. JY Zou et al., AI can be sexist and racist - it's time to make it fair, Nature, Vol. 559(2018), No. 7714, pp. 324-326.
26. 3GPP TR 38.821, Solutions for NR to support non-terrestrial networks (Release 16), 2021.
27. R1-2110604, LS on combination of open and closed loop TA control in NTN, in 3GPP TSG RAN WG1 Meeting #106-bis-e, 2021.
28. O Kodheli et al., Satellite Communications in the New Space Era: A Survey and Future Challenges, IEEE Communications Surveys & Tutorials, Vol. 23(2021), No. 1, pp. 70-109.
29. S Schaer and D Hood, Software defined networking architecture standardization, Computer Standards & Interfaces, Vol.54(2017), Part 4, pp. 197-202.
30. PK Sharma et al., SDN-based Platform Enabling Intelligent Routing within Transit Autonomous System Networks, In Proceedings of the IEEE 19th Annual Consumer Communications & Networking Conference, 2022.

Acknowledgement and Contact

This whitepaper is

Contributed by :

ClassNK MASS Project Team (Director: Yukihito Fujinami)

and written by

Main Authors :

Tomoaki Yamada	Research Institute
Makoto Ito	Research Institute
Yasuharu Adachi	Research Institute
Noriyuki Kajita	Digital Transformation Center
Rikiya Kuranobu	Technical Solution Department
Kohei Nakayama	Maritime Education and Training Certificate Department

based on our activities which we couldn't have done without the cooperation of the maritime community. We would like to thank the community.

Contact:

NIPPON KAIJI KYOKAI
MASS Project Team
Tel : +81-3-5226-2737
E-mail : ri@classnk.or.jp

ClassNK
CHARTING THE FUTURE

WHITE PAPER
Towards MASS social implementation
[English]

NIPPON KAIJI KYOKAI
MASS Project Team

3-3 Kioi-cho, Chiyoda-ku, Tokyo 102-0094, JAPAN
Tel : +81-3-5226-2737
Fax : +81-3-5226-2736
E-mail : ri@classnk.or.jp

www.classnk.com

April 2023