Risk analysis procedure for MASS
FY 2023 Edition

Japan Ship Technology Research Association
National Maritime Research Institute

Table of Contents

1. Outline

MASS (Maritime Autonomous Surface Ships) have been developed in recent years and guidelines for MASS have been published by multiple classification societies and flag states. International Maritime Organization (IMO) has published interim guidelines for MASS trials to safely conduct the demonstration experiment. These guidelines require the implementation of risk analysis, but specific procedures are not indicated. Thus, in this manual, we present concrete steps of a risk analysis for MASS which carried out at the design and/or MASS trial. It contributes to better safety and promotion of development in regard to MASS.

2. Key Principles

2.1 Target ships of this manual

Though there is no international consensus on the definition of MASS and level of automation, this manual focuses on phase II and phase III autonomous ships of "Roadmap to Realize Autonomous Ships" by Maritime Bureau, Ministry of Land, Infrastructure, Transport and Tourism (phase II autonomous ships: ships on which sailors, the ultimate decision makers, are supported by the operation from land and/or the proposal by artificial intelligence (AI), phase III autonomous ships: ships with a high degree of autonomy and is designed for situations where the final decision-maker is not a sailor.).

2.2 Target risk analysis of this manual

As MASS, conventionally designed, built, and operated ships are partially redesigned or equipped with an automation system. Because ships that are conventionally designed, built, and operated are sufficiently safe, further risk analysis of the ship itself is unnecessary. Therefore, the risk analysis of the present manual analyzes hazards associated with parts and operations different from conventional ships.

2.3 Definition of terms

Table 2.1 shows the definition of main terms used in this manual.

Table 2.1. Definition of terms.

Terms	Definition
Risk	A measure of the likelihood that an undesirable event will occur together with a measure of the resulting consequence within a specified time, i.e., a combination of the frequency and severity of the consequence. [1]
Hazard	A factor leading to harm to life, health, property or environment. It is also referred to as the hazard factor. [2]

Accident scenario	When a series of stages up to harm is assumed from the initial condition in which the potential for hazard exists, its description is called a scenario. [2]
Risk treatment	Refers to a single or multiple measures taken to reduce risks. Measures include avoidance of hazard, reduction of consequences, and reduction of the likelihood of consequences from hazards.
HAZID	Acronym for HAZard IDentification.
FI	Initialism for frequency index. Frequency is converted to a common logarithm.
SI	Initialism for severity index. Severity is converted to a common logarithm.
RI	Initialism for risk index. Risk is converted to a common logarithm and obtained as a sum of FI and SI.
HAZID workshop	A workshop held to identify hazards. In addition to identifying hazards, FI, SI, and RI are often determined and risk treatments are considered, some of which are merely proposed while others provide estimates of their effects to decision makers for more effective risk treatment.
Task	Combination of operations and work that constitute ship operation according to the automation system design. “Tasks” vary depending on target, coverage area, and level of automation and remote control. [3]
Subtask	Operations and work that constitute a task. [3]
Decision-making subtask	The subtasks related to decision making by humans, such as situation awareness, decision, and action. [3]
Automated condition	A condition where computer systems control the execution of some or all the decision-making subtasks. [4]
Automated operation system (AOS)	A system that automates part or all of decision-making subtasks with a computer system or a combination of computer system and human. [3]
Remote operation system (ROS)	A system in which a part or all the decision-making subtasks can be operated by a remote operator (human) or a combination of an AOS and a remote operator (human).
Assumed conditions of use	Principal particulars of ships equipped with an automation system, a sea route, ship operation phase, and marine weather conditions for which an automation system is used.
Operational design domain (ODD)	Operational domain in which an automation system appropriately functions (ODD). [3] It may be expressed as a part of assumed conditions of use.
Fallback	Countermeasures to minimize risks when the AOS/ROS cannot work properly owing to unpredictable events such as malfunctions of the AOS/ROS and cyber-

	attack. This includes countermeasures when the AOS/ROS has deviated outside the ODD. [4]

3. Outline of risk analysis procedure

Let us explain the risk analysis procedure simply. It follows the flow shown in Figure 3.1. Please refer to the Section in this manual indicated in a bracket for detailed explanation of each item.

Risk analysis is performed for the initial and detailed designs. For a risk analysis of the initial design, documents necessary for confirming the analytical target scope and risk analysis are prepared. These documents are used to determine the analytical target scope and to summarize the information that must be confirmed for the risk analysis. Upon obtaining the consensus of those involved on the analytical conditions, such as risk assessment criteria, the analysis and assessment are performed. Finally, a report that summarizes the above results is prepared.

Next, a risk analysis is performed on the detailed design. For the detailed design that incorporates risk treatments recommended in the risk analysis on the initial design, specific machines and operations that were not yet determined in the initial design are assumed to analyze and assess risks in the same flow as the risk analysis of the initial design. Since the same preparation for the analysis and consensus on analytical conditions as that of the risk analysis on the initial design can be often used, these can be omitted. As the result of the risk assessment, recommended risk treatments are incorporated into the final detailed design, at which the risk analysis that is the target of the present manual is complete.

It is noted that, in the case of risk analysis on a demonstration experiment, depending on the demonstration experiment, the experiment may be conducted after risk analysis for the initial design.

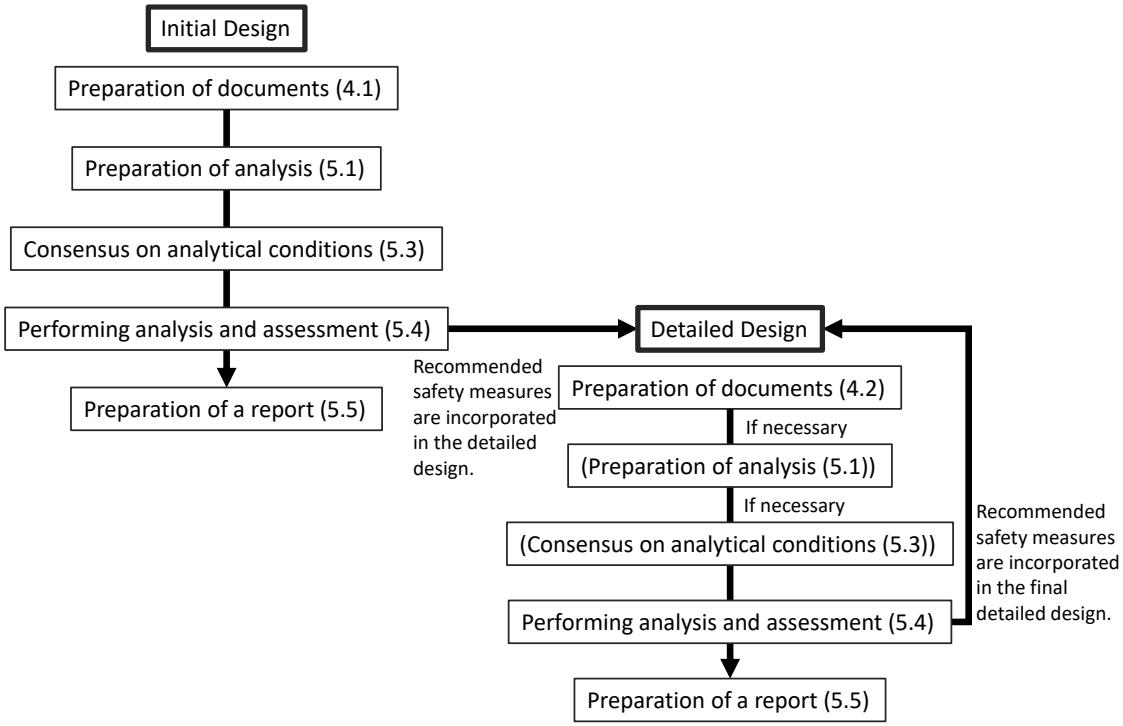

Figure 3.1. Flow chart of procedures used for risk analysis.

4. Documents to prepare

In this Section, we explain documents that are necessary in each step of an analysis.

4.1 Documents necessary for an analysis of the initial design

When analyzing the initial design, the following documents are necessary.

(1) Functional requirements for the automation system (target tasks and subtasks of the automation).

(2) System architecture that clarifies the entire image of the automation system (it is desirable to clarify the relation between the automation system and other systems on board the ship, and clarify sensors and nautical equipment as much as possible).

(3) Outline of the internal operation of the automation system.

(4) Outline of the division of roles for the automation system and humans (includes execution transfer between the automation system and humans and fallback process).

(5) ODD of an automation system.

In the case of risk analysis on a demonstration experiment, the following document is required addition to the above documents.

(6) Outline of a demonstration experiment (Objective of the experiment, Experimental route, Schedule, Experimental process, etc.)

4.2 Documents necessary for an analysis of the detailed design

Risk analysis of the detailed design requires changes in documents presented in the initial design and also documents for which parts that were unclear in the initial design are clarified.

5. Tasks performed at each step of a risk analysis

In this Section, we explain each task performed at each step of a risk analysis.

5.1 Preparation for an analysis

As the preparation of an analysis, parts of the target ship that are different from the conventional ships must be clarified. Information such as objective, role, composition, and method of new features of the analytical target ship and or new use of existing facilities is summarized. Based on this information, the analytical target is defined and the analytical target scope is confirmed.

First, features and usages of facilities with new features (hereafter referred to as the new facility), which are the analytical target, must be clarified. In addition, as the conditions of autonomous operation of the analytical target ship, the ODD, characteristics of the sea route, ship operation phase, conditions that must be maintained when deviating from the ODD, and response to such situations, must be summarized.

Furthermore, based on this information and specifications of the new facility, the analytical target is modeled. This is useful in defining the analytical target, confirming the analytical target scope, and supporting the analysis. As for modeling, elemental features for each module, such as hardware and software that constitute the new facility, are broken into a level that suits the analysis and then defined. As necessary, interaction (input, output, and so on) of elements is included in the definition. If information must be manually input or corrected, interaction between the feature and humans must be included as well. If the elements of the new system have an interaction with the existing ship facilities, these facilities are added to the model and the interaction between the new facility and the existing facilities are clarified to analyze the effect of the new facility on the existing facilities. Within the model prepared in the above procedure, the scope necessary for the objective of an analysis is defined as the analytical target scope. By using such model, understanding of the analytical target is promoted, supporting the analysis itself. See Appendices 1-3 for examples of modeling.

As for an analysis, if data on the failures or defects in each component included in the analytical target scope are available, such data must be gathered.

In summary, at the preparation stage of an analysis, the following information must be summarized. Example of the information is included in Appendices 1-3.

- Definition of the feature.
- Objective of the feature.

- Extent of automation and the relation between automation and the ship operator (crew on board/remote operator).
- Extent of remote control and the relation between automation and the ship operator (crew on board/remote operator).
- Assumed conditions of use (principal particulars of ships equipped with the new feature, sea route, ship operation phase, and marine weather conditions at which the new feature is used, and so on).
- ODD (external, internal, and communication conditions under which the new feature operates).
- Methods of autonomous navigation.
- Monitoring method of the relevant feature.
- Response procedure when autonomous navigation deviates from the ODD.
- Feature of each element, such as hardware and software, that constitutes the relevant new facility, interaction of elements, and so on (including information on the interaction between each element and humans and between each element and the existing systems).
- Data on failures and defects of each constituent element included in the analytical target scope.

5.2 Working group

Analysis is usually performed at a workshop attended by experts of different fields and attendees selected from experts in different fields. Below is a list of experts as an example:

Owners, ship builders, ship designers, experts with knowledge and experience of safety, design, and operation of the target system. And as necessary, ship inspectors, ship operators, safety engineers, experts of devices and human engineering, navigators, and marine engineers [5][6].

5.3 Consensus on the analytical conditions

Handling of the identified risks must be decided ahead of time. In other words, range at which risk reduction measures must be implemented for hazards with a risk of more than a certain level must be determined and those involved must reach a consensus. In addition, whether post-risk-treatment risks need to be estimated must be decided. To that end, (i) indexing of risks and (ii) setting of the criteria are necessary. Let us discuss these topics below.

(i) Indexing risks

For each accident scenario that starts with a hazard, the frequency of occurrence, the severity of consequences, and their product; i.e., risk, are semi-quantified (indexed). By expressing the frequency and severity of consequences with a logarithmic scale, semi-quantification (indexing) is performed. For determining the severity of consequences, generally, the level of effect on human life, environment, and asset is considered. Whether all of these are the targets or choose one must be determined a head

of time.

With risk denoted by R, occurrence frequency represented by F, and severity of consequences denoted by S, risk is obtained using Equation (1). By converting Equation (1) into a common logarithm, we obtain Equation (2).

$$R = F \cdot S \qquad (1)$$

$$\mathrm{Log}(R) = \mathrm{Log}(F) + \mathrm{Log}(S) \qquad (2)$$

We refer to risk, frequency, and severity of consequences converted to a common logarithm as risk index (RI), frequency index (FI), and severity index (SI), respectively. Here we present examples of FI, SI, and RI, which is a combination of FI and SI [7]. These are simply examples, and the same values are not required for an analysis. Thus, definition of FI and SI must be determined by those involved. Table 5.4 is called a risk matrix.

Table 5.1. Example of the definition of FI [7].

FI	Frequency	Definition	F (per ship year)
7	Frequent	Likely to occur once per month on one ship	10
5	Reasonably probable	Likely to occur once per year in a fleet of 10 ships	0.1
3	Remote	Likely to occur once per year in a fleet of 1,000 ships	10^{-3}
1	Extremely remote	Likely to occur once in the lifetime of a world fleet of 5,000 ships	10^{-5}

Table 5.2. Example of the definition of SI [7].

SI	Severity	Effects on human safety	Effects on ship	S (Equivalent fatalities)
1	Minor	Single or minor injuries	Local equipment damage	0.01
2	Significant	Multiple or severe injuries	Non-severe ship damage	0.1
3	Severe	Single fatality or multiple severe injuries	Severe damage	1
4	Catastrophic	Multiple fatalities	Total loss	10

Table 5.3. Example of the definition of SI (environment) [7].

SI	Severity	Definition
1	Category 1	Oil spill size < 1 tonne

2	Category 2	Oil spill size between 1–10 tonnes
3	Category 3	Oil spill size between 10–100 tonnes
4	Category 4	Oil spill size between 100–1,000 tonnes
5	Category 5	Oil spill size between 1,000–10,000 tonnes
6	Category 6	Oil spill size > 10,000 tonnes

Table 5.4. Example of the definition of RI (risk matrix) [7].

		Severity index (SI)			
		1	2	3	4
FI	Frequency	Minor	Significant	Severe	Catastrophic
7	Frequent	8	9	10	11
6		7	8	9	10
5	Reasonably probable	6	7	8	9
4		5	6	7	8
3	Remote	4	5	6	7
2		3	4	5	6
1	Extremely remote	2	3	4	5

(ii) Setting the criteria

Judgment criteria for indexed risks; in other words, criteria are set.

Thus, criteria are set on the risk matrix of (i) first. As shown in Figure 5.1, it is common to use three levels: “risk must be reduced,” “risk reduction must be considered,” and “no risk reduction necessary.” Risk is indexed for each hazard and accident scenario, and by comparing those with the criteria, need for risk treatment is determined.

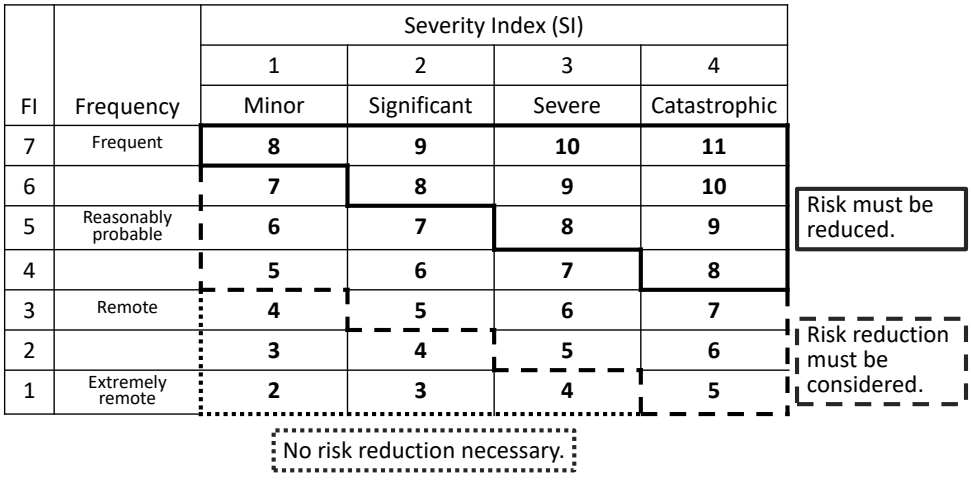

Figure 5.1. Example of judgment criteria.

- Consideration of risk treatment is unnecessary for hazards and accident scenarios under “no risk reduction necessary.”
- Risk treatment is considered for hazards and accident scenarios under “risk reduction must be considered.” Whether such risk treatment will be actually implemented is also examined. Because the introduction of a risk treatment is highly necessary for hazards and accident scenarios with high RI, risk treatments are implemented for hazards and accident scenarios with RI over a certain level. However, the level of RI at which risk treatments are implemented must be decided ahead of time. Even hazards and accident scenarios below this level of RI require at least some risk treatment efforts because they fall under “risk reduction must be considered.”
- Risk treatment is considered to be implemented for hazards and accident scenarios under “risk must be reduced.” Whether risk is indexed after an implementation of a risk treatment must be determined ahead of time. If yes, it is compared with the criteria of the risk matrix once again, and if it falls under “risk must be reduced” or “risk reduction must be considered,” further risk treatments are considered. These steps are repeated until hazard/accident scenario falls under “no risk reduction necessary” or “risk reduction must be considered.”

5.4 Performing analysis and assessment

Analysis is performed via common hazard identification methods (e.g., Structured What IF Technique (SWIFT), Failure Mode and Effects Analysis (FMEA), and HAZard and OPerability study (HAZOP)). It begins with identifying possible hazards for a new feature, followed by estimation of causes of hazards, consequence, severity of the consequence, and hazard frequency. These processes must be performed with experts mentioned in the previous Section. If necessary, risk treatment and so on that are recommended for high-risk hazards are identified. Similarly, if needed, risk following a risk treatment is estimated (it is desirable to also examine if a risk treatment leads to a new hazard and so on). The analysis process is recorded on a worksheet corresponding with the method as part of the report.

5.4.1 Identifying hazards

(i)General matters

Here, let us explain matters that are necessary to implement an analysis regardless of the identification method of hazards.

- Selection of experts

  Please refer to Section 5.2.
- Separating the phase

  Analysis must be performed for each phase that uses the target automation system. For

example, the following phases must be considered. Since this is simply an example, phases should be set according to the characteristics of the target automation system.

Berthing and unberthing, in-harbor navigation, navigation in congested waters, ocean navigation, emergencies (fire, flooding, and so on).

- Example of hazards that should be considered

Appendix 2 shows examples of hazards that should be considered. Because these are simply examples, hazards should be exhaustively identified beyond this list.

- Type of risk targets that should be considered (human life, environment, and asset)

As discussed in Section 5.3, in terms of the severity of consequence, it must be determined ahead of time which one or several of human life, environment, and property, will be considered as a target in analyzing the severity of consequence.

(ii) Outline of the risk analysis method

The outline of SWIFT, a method often used for risk analysis in the marine field, is presented below. Common methods other than SWIFT are listed in Appendix 3.

- SWIFT

At a workshop of designers, users, and experts of the target system led by a facilitator, questions are repeatedly asked about a situation that deviates from a normal one, "what if," and hazards are identified through brainstorming.

The analysis is technically easier than the other analysis methods and can be applied during a concept study or concept design stage. At the same time, it has disadvantages that the result depends on the experiences of participants and accident scenario is not explicitly presented as an analysis output.

Standard steps and worksheet of SWIFT are as follows:

Step 1: Define the target system and process.

Step 2: Prepare documents, such as design information and related data, and organize a working group.

Step 3: Hold a HAZID workshop and identify hazards, causes, results, FI, SI, RI, and existing safety measures through brainstorming.

Step 4: Record these discussions on the worksheet.

Worksheet example:

System: LNG carrier

Phase: In-harbor navigation

ID	Hazards	Causes	Consequences	Existing measures	necessary measures	FI	SI	RI	comments

1	Collision	- Dysfunction / damage to machines - Stormy weather - Operation error	- Dysfunction / damage to structural equipment - Secondary disaster - Injury or death to crew	- Preventive measures (alert system, double hull structure) - Mitigation measures (damage stability, lifesaving and rescue) - Inspection of machines - Education and training of operators		2	4	6	

Figure 5.2. Example of the SWIFT worksheet.

5.4.2 Indexing risks

Frequency and degree of severity for the identified hazards and accident scenarios are semi-quantified (indexed). Documents that can be referred for this indexing are shown below.

Documents necessary to set the frequency and severity: Data necessary to examine the frequency and seriousness.

- Data on the frequency and severity (level of damage and effect on human life, environment, and asset) of defects, failures, and accidents in each system that occurred in the past or are anticipated. If those are not available, reference the data for a similar system.
- Data on human life (number of death and injured), environment (marine pollution), and/or asset (damage to the ship).

Usable data should be used as much as possible for semi-quantification (indexing). However, in many cases, there is no usable datum. In such a case, semi-quantification (indexing) is performed based on the experience of experts. For example, by comparing the frequency and severity of hazards and/or accident scenarios without data to hazards and accident scenarios that have been semi-quantified (indexed) based on data, semi-quantification (indexing) of hazards and accident scenarios without data becomes possible.

Semi-quantified (indexed) risks are compared to the preset criteria, and a response to the risk is determined based on the predetermined judgment method used for determining risk acceptance, an examination method of risk treatment, and the judgment method for determining risk acceptance after risk treatment, in that if the risk is not acceptable, the risk with treatments is judged.

5.4.3 Risk analysis and assessment of the initial design

In a case of initial risk analysis based on a concept or basic design information, a focus is put on the role of the system and difference from existing ships due to the role in order to conduct a risk analysis and assessment.

Using the document shown in Section 4.1, the analytical target scope is determined with the method shown in Section 5.1 and the information shown in Section 5.1 is summarized. Then, attendees are chosen based on Section 5.2, reach a consensus on items shown in Section 5.3, and perform an analysis and assessment according to Sections 5.4.1 and 5.4.2.

From the following, hazards based on the concept design are considered.

(1) Risks originating from human–machine interface.

(2) Defects of sensors and control equipment linked to the automation system.

(3) Effect of the automation system on other systems on the ship.

(4) Cyber security.

(5) Defects during an operation of the automation system (including forgotten updates of related software and verification of the validity of emergency response).

5.4.4 Risk analysis and assessment of the detailed design

At this stage, following is confirmed.

- Recommendations of the initial risk analysis and assessment are definitely reflected in the detailed design.
- Accident scenarios and related features that were not considered in the initial risk analysis.

For the former, if it is found that the recommendations are not reflected, it will be ensured that they will be reflected in the detailed design. For the latter, if there are accident scenario or related feature not considered, analysis is performed in the same manner as in Section 5.4.3, and after updating the analysis, assessment is made.

5.5 Report

Details up to the previous Section must be recorded in a written form. An example of the table of contents for a record is shown below.

1. Risk analysis and assessment of the initial design
   1.1 Conceptual explanation of the system and documents necessary to perform a risk analysis on the initial design
   1.2 Information necessary to prepare for the analysis
   1.3 Working group
   1.4 Analytical conditions
   1.5 Analysis and assessment results
      1.5.1 Risk analysis procedure
      1.5.2 Analysis and assessment results (attached worksheet, explanation of the analysis and assessment results)
2. Risk analysis and assessment of the detailed design
   2.1 Explanation of the system and documents necessary to perform a risk analysis on the detailed design
   2.2 Information necessary to prepare for the analysis

2.3 Working group

2.4 Analytical conditions

2.5 Analysis and assessment results

2.5.1 Risk analysis procedure

2.5.2 Analysis and assessment results (attached worksheet, explanation of the analysis and assessment results)

Annex 1. An example of hazards to consider

Table A1.1 shows examples of hazards to consider by summarizing hazards from each class guide [4], [8], and [9] and existing studies [11]–[14].

Table A1.1. Examples of hazards to consider.

Classification	Hazards
External environment	Bad weather
	Poor visibility
	Congested waters
	Unexpected behavior of other ships
Failure of AOS and related equipment	Loss of signal from information collection devices
	Decrease of reliability or stability of information from information collection devices
	Failure of related equipment in the AOS
	Software bug in the AOS
	Inappropriate tuning of parameters according to ship specifications (e.g., the maneuverability of the ship is not correctly reflected in the AOS)
	Power loss of the AOS or related equipment
	Inappropriate human–machine interface (HMI), e.g., it is difficult to understand the reason for issuing an alarm, or there is insufficient time to execute transfer from the AOS to a human
	Improper interface between the AOS and other systems such as differences in situation awareness range, differences in kinetic performance models, mismatched parameters, system failures, and poor communication
Detection	Failure in detecting small objects (wreckage)
	Failure in detecting collision targets
	Failure in detecting navigational aids
	Failure in detecting ship lights, sounds, or shapes
	Failure in detecting semi-submerged towed or floating devices (e.g., seismic gauges and fishing trawls)
	Failure in detecting discrepancy between charted water depth and sounded water depth
	Failure in detecting discrepancy between weather forecast and actual weather situation

	Failure in detecting degrading performance of a sensor
	Failure in detecting degrading performance of the automation system
	Failure in detecting slamming or high vibration
Navigation	Collision with other ships or offshore infrastructures
	Collision with floating objects
	Collision with marine wildlife
	Collision with onshore infrastructure
	Loss of intact stability owing to unfavorable ship responses
	Loss of intact stability owing to icing
	Unexpected maneuvers and drive off
	Grounding owing to the loss of propulsion
	Grounding owing to the loss of steering control
	Grounding owing to deviation from the planned route
	Grounding owing to error in the planned route
	Fishing equipment/net becomes snagged on the sea route
	Loss of intact stability owing to shift/liquification of cargo
Improper operation	Omission of updating charts, atmospheric information, related software, etc. leading to misinformation
	Incorrect input of setting data and initial input data to the AOS, e.g., navigation plan data and reference values for collision avoidance decisions
	Replacement of related equipment with equipment that is not compatible with the AOS
	Too many alarms. Prioritization of alarms is not possible
Communication	Failure of electronic components in the communication links
	Less than ideal radio coverage for wireless links
	Error in transmission of data (also known as bit faults)
	Failure in data integrity (data transmission errors, etc.)
	Lack of acknowledgment of command(s)
	Wrong configuration of communication functions
	Unexpected reduction of available bandwidth
	Unexpected increase in latency
	Unstable data links over time
	Network storms
	Loss of power
Security	GNSS spoofing, AIS spoofing, etc.

	Jamming of RADAR, etc.
	Unauthorized access/hacking of the AOS and related systems
	The AOS or related systems infected with malware
Onboard crew (fallback)	Onboard crew dozing off
	Lack of proficiency and understanding of the AOS users, e.g., cannot understand the meaning of alarms and unsuitable use environment of the AOS
	Overconfidence of automation system users (onboard crew) in the automation system
	Inadequate human–machine interface
	Inability to understand incorrect input and unentered input of the voyage plan
	Conniving inappropriate sea routes
	Inability to understand unswitched operation modes (e.g., navigation mode for outside of a port navigation mode for inside of a port)
	Outside of the ODD and fallback is necessary, but onboard crew cannot respond
Emergency	Severe hull damage (structural damage, flooding due to failure of watertight equipment, etc.)
	Malfunction of ship equipment (propulsion, steering gear, radar, etc.)
	Fire
	Temporary or permanent power outage due to causes such as blackout
Remote control	Human errors by remote operators (falling asleep, leaving the position too long, incorrect interpretation of data, etc.)
	Ship losing communication with the remote control center
	Communication latency and failures
	Frozen screen, such as that for the remote control system
	Failure of remote operators to recognize the situation due to excessive or insufficient information
	Handover of responsibilities from one operator to another

Annex 2. Outline of common risk analysis methods

Below, we present the outline of risk analysis methods other than SWIFT, which was discussed in the main text and summarize their characteristics. Please refer to the references, e.g., [15]–[20], for more detailed descriptions of each method including SWIFT. Methods other than those presented in this manual can be applied to the risk analysis of an autonomous ship as well.

(1) Failure Mode and Effects Analysis (FMEA)

With a focus on the equipment that constitutes the system, possible modes of failure for the equipment are identified and their effects on the system are analyzed. This method is often used to identify the effect of failures.

It is advantageous in that a systematic and exhaustive analysis is possible. At the same time, its disadvantages include its difficulty in application during the concept design stage and the fact that it is labor and time intensive.

The standard steps and worksheet for FMEA are as follows:

Step 1: Define the target system and process.

Step 2: Prepare documents such as design information and related data and organize a working group.

Step 3: Hold a workshop and perform FMEA analysis. Select the components and perform the following for these components:

- Identifying features.
- Identifying the types of possible defects (failure mode).
- Identifying localized effect caused by the failure mode (local effect) and effect on the overall system (final effect).
- Identifying the measures to protect the system from the failure mode (a means, including alarms and error messages from the automated systems, to detect failures, corrective actions, etc.).

Step 4: Record these discussions on the worksheet.

Example of worksheet:

System:	Main engine system	Subsystem:	Fuel oil pipe system
Navigation mode:	Normal sailing at full speed	Block diagram:	Block diagram of fuel oil pipe system
Date:		Editor:	
Sheet number:		Approval by:	

Number	device name	feature	failure mode	cause of failure	effect of failure		failure detection	measures	severity	notes
					Local	final effect				
1	Main engine 1 (2, 3, 4)	Burn the fuel and convert the energy to mechanical work	Declined output (stopped output)	Damage to the piston of the main engine 1 (2, 3, 4)	Main engine 1 operation discontinued	Outer 2 axes cannot be operated	Unusual sound, vibration, various alarms	Outer 2 axes are stopped and sailing with inner 2 axes	Major impact	

Figure A2.1. Example of FMEA worksheet*.

*NMRI edition of the FMEA worksheet based on the HSC code.

Failure mode refers to the types of potential defects. The 2000 High-speed craft (HSC) Code, an international regulation for high-speed crafts [21], lists the following modes of failure: structural failure (damage), physical restraint or biting, vibration, inability to maintain position, inability to open or close, poor opening or closing, internal and external leakage, being above or below the tolerance level, accidental movements, intermittent movements, unstable movements, erroneous display, limited flow, erroneous movements, inability to stop or start, inability to switch, early movements, delayed movements, erroneous input (increase/decrease), erroneous output (increase/decrease), loss of input or output, short circuit, electric release, electric leakage, and other.

(2) HAZard and OPerability study (HAZOP)

This is a method that is often used to analyze hazards at process plants. It clarifies potential abnormalities in a process system and propagation mechanisms to assess validity of measures. Analysis begins by assuming “a deviation” from the design intent, and both cause and consequence are analyzed. Guide words are used to prepare questions to analyze potential risks of deviating from the design specifications, and causes and consequences are estimated on the basis of the answers to the questions.

While systematic and exhaustive analysis is possible, it is difficult to apply during the concept design stage and is labor and time intensive.

(3) Bow-Tie Diagram

Generally, a diagram in a bow-tie shape is used. The target phenomenon is the knot, while the left shows causes that could lead to the target phenomenon. The right side shows the consequences of the

phenomenon. This method combines the preventive measures of the target phenomenon and the preventive measures of the consequences of such a phenomenon. This method is often used to display an accident scenario in combination with SWIFT.

While this method can explicitly display an accident scenario, it does not support the identification of hazards, causes, or consequences and requires the use of other methods such as SWIFT.

(4) STAMP/STPA (Systems-Theoretic Accident Model and Processes/System-Theoretic Process Analysis)

This method was developed to analyze the safety of large-scale and complex systems that incorporate technologies such as AI/IoT, which focuses on defects in interactions between elements. While conventional methods such as FMEA assume accidents occur due to failure of constituting machines and operational errors, this method is characterized by its assumption that accidents occur due to interactions between elements.

Its advantages include the identification of abnormalities that cannot be discovered by conventional methods, analysis at a lower cost and with less labor than conventional methods [22], and its application to concept study and/or design stages. However, it does not support the detailed analysis of the cause of failure or perform semi-quantitative analysis [23]. As it is a relatively new method, examples of its application are limited when compared to conventional methods.

Table A2.1 shows a summary of the characteristics of the above methods and SWIFT.

Table A2.1. Characteristics of each method.

	SWIFT	FMEA	HAZOP	Bow-Tie	STAMP/STPA
Outline	Questions on a situation that deviates from normal, "what if," are repeatedly asked, and hazards are identified through brainstorming in this method	With a focus on machines that constitute a system, the failure modes possible for these machines are identified and their effects on the system are analyzed	Analysis begins by assuming "a deviation" from the design intent, and both causes and consequences are analyzed	A method of illustrating the process from a cause to the target phenomenon, and from a cause to the consequences, illustrated in a shape of a bow-tie	Developed to analyze the safety of a large-scale complex system that focuses on defects in the interaction between elements
Typical stage of application	Concept study, concept design, detailed design	Detailed design	Detailed design	Concept study, concept design, detailed design	Concept study, concept design, detailed design

Major advantages and disadvantages	・Analysis is relatively easy. ・Can be applied to the stage of concept study or design. ・Dependent on the experience of workshop participants. ・Accident scenario is not explicit	・ Systematic and exhaustive analysis is possible. ・Difficult to apply during the concept design stage. ・Labor and time intensive	・ Systematic and exhaustive analysis is possible. ・Difficult to apply during the concept design stage. ・Labor and time intensive	・Accident scenario is explicit. ・ Difficult to identify hazards, causes, and consequences using only this method, this requiring other methods such as SWIFT	・ Abnormalities that cannot be found using the conventional methods can be identified [22]. ・Analysis at a lower cost and with fewer man-hours than the conventional methods [22]. ・Can be applied to concept study and/or design stages. ・ Difficult to conduct a detailed analysis of the cause of failures. ・(Semi-) quantitative assessment is difficult [23] ・Fewer applications than the conventional method.

Appendix 1. A practical example of risk analysis on a phase II autonomous ship

A practical example of risk analysis on a phase II autonomous ship are shown in this Appendix. We assume two phases, that is, normal navigation and berthing/unberthing. It should be noted that risk analysis is desirable considering more phases to increase the comprehensiveness of hazards.

i. Preparation of documents

Examples of the documents mentioned in section 4.1 of this procedure are shown as follows:

(0) ConOps

Table 1.1 ConOps

● Definition of the feature This feature targets a given voyage plan, detects other ships and wreckage that the ship encounters, disturbances caused by marine weather, formulates a ship action plan according to a predetermined action policy, calculates engine output and steering commands to achieve the action plan, and outputs the speed and the course for the ship to achieve the voyage plan. The voyage plan consists of the departure point, departure date and time, arrival point, arrival date and time, and way point. The autonomous ship steering system onboard the ship will formulate a ship action plan based on the voyage plan and control the steering and engine output in accordance with the ship action plan using the ship control system. <Navigation Plan> Departure point: XXX Port Departure date and time: Month/date, XX:XX Arrival point: YYY Port Arrival date and time: Month/date, YY:YY Waypoint: ZZZ Port Waypoint arrival date and time: Month/date, ZZ:ZZ <Action Policy> Secure an appropriate time to begin avoidance and an appropriate distance to avoid interfering navigation of other ships or causing fear on sailor of other ships. Considering the voyage plan, in order to prevent a large delay, the time spent on avoidance navigation should be minimized while securing the above mentioned appropriate avoidance start time and distance.
● Objective of the feature The objective of this feature is to develop the ship steering plan that includes responses to external obstacles and disturbances that may act as impediments in the realization of the voyage plan and to control the ship according to that action plan approved by onboard crew.

● Extend of automation and relation of automation with operators (onboard crew/remote operators) Extent of automation of the present feature is equivalent to the Category I shown in the ClassNK Guidelines [4]. Collection of information on obstacles, integration of the collected information, and preparation of the action plan are performed with this feature. The action plan is presented to the onboard crew, and stands ready until the onboard crew approves. The action plan approved by the onboard crew is output to the steering and engine equipment by the present feature. Within the assumed conditions of use for this feature discussed below, autonomous navigation is performed with this feature. Outside these conditions, the crew on board steers in the conventional method.
● Extent of remote control and relation with operators (onboard crew/remote operators) This feature does not have remote control capability.
●Assumed range of use ship: Ship name: ○○○ Type of ship: Ferry Gross tonnage: 199 tons Loa: 45 m Width: 9 m Navigation area: Coasting area Route: Port XXX to Port YYY Phase of operation: normal navigation (including in-port and out-of-port); berthing and unberthing.
● Autonomous navigation methods Autonomous navigation of a ship equipped with this feature is performed by taking over the tasks from the onboard crew on the sea route within the assumed conditions of use and turning on the feature upon having the onboard crew confirming the operation. Completing the autonomous navigation along the sea route within the assumed conditions of use and hanging over the tasks to the onboard crew completes the extent of autonomous navigation. If the ship leaves the ODD during its route, even within the assumed conditions of use, autonomous navigation is stopped by handing over to the onboard crew."
● Means of monitoring relevant feature The sensor information collected and integrated into the present feature, the prepared action plan, and the position of the ship within the ODD are constantly provided to the onboard crew by the dedicated monitoring device on the ship.

● Response procedures in case of deviation from the ODD during the automatic operation

Deviation from the ODD is detected by this feature and the onboard crew are notified by the onboard alarm. After the crew switch from autonomous mode to manual mode in a defined procedure, the crew take over the control of the ship.

(1) Functional requirements for the automation system (target tasks and subtasks of the automation)

Table 1.2 Functional requirements for the automation system (Phase: Normal navigation)

ID	Element name	Task	Subtask
1	Autonomous ship steering system	· Establish action plan · Switch operation phase (normal navigation → berthing) · Diagnose own status	· Obtain integrated information on own ship · Obtain integrated information on other ships and drifting objects · Obtain integrated information on marine weather conditions · Calculate navigational safety and economic efficiency · Present ship action plans · Obtain information necessary to diagnose own status
2	Information integration system for own ship	· Integrate information on own ship · Diagnose own status · Diagnose sensor status	· Obtain information on own ship · Obtain information necessary to diagnose own status · Obtain information necessary to diagnose sensor status · Transmit integrated information, own status, and sensor status
3	Information integration system for other ships/ drifting objects	· Integrate information on other ships and drifting objects · Diagnose own status · Diagnose sensor status	· Obtain information on other ships and drifting objects · Obtain information necessary to diagnose own status · Obtain information necessary to diagnose sensor status · Transmit integrated information, own status, and sensor status

4	Information integration system for marine weather	· Integrate of the information on marine weather conditions · Diagnose own status · Diagnose sensor status	· Obtain information on marine weather conditions (current location) · Obtain marine weather condition forecast information · Obtain information necessary to diagnose own status · Obtain information necessary to diagnose sensor status · Transmit integrated information, own status, and sensor status
5	Ship control system	· Calculate control variables based on ship action plans · Rudder/engine control · Diagnose rudder/engine status · Diagnose own status	· Obtain ship action plans · Obtain actual ship's position · Calculate of the deviation between the ship action plans and the ship's position · Compare current situation with control threshold values · Transmit rudder/engine status and own status
6	Autonomous operation management system	· Control mode switching instructions · Diagnose own status	· Obtain information on own ship, other ships, drifting objects, marine weather conditions · Obtain information on the status of each system · Determine whether inside or outside ODD · Obtain information necessary to diagnose own status
7	Onboard crew	· Approve/revise the action plan · Switch the ship steering mode · Emergency response (forced switchover to manual mode)	· Check information on own ship, other ships, drifting objects, marine weather conditions · Check the action plan established by autonomous ship steering system · Check the instruction of switching the ship steering mode by autonomous operation management system · Constant monitoring of each system operation · Constant monitoring of surroundings of own ship

Table 1.3 Functional requirements for the automation system (Phase: Berthing/unberthing)

ID	Element name	Task	Subtask
1	Autonomous ship steering system	· Establish berthing/ unberthing action plan · Switch operation phase (unberthing → normal navigation) · Diagnose own status	· Obtain integrated information on own ship · Obtain integrated information on other ships and drifting objects · Obtain integrated information on marine weather conditions · Calculate navigational safety and economic efficiency · Present ship action plans for berthing/ unberthing · Obtain information necessary to diagnose own status
2	Information integration system for own ship	· Integrate information on own ship · Diagnose own status · Diagnose sensor status	· Obtain information on own ship · Obtain information necessary to diagnose own status · Obtain information necessary to diagnose sensor status · Transmit integrated information, own status, and sensor status
3	Measuring system for the distance from the berth	· Measure the distance between own ship and the berth · Activate an alarm in case of proximity · Diagnose own status · Diagnose sensor status	· Obtain the position of the berth · Obtain the position of own ship · Obtain information necessary to diagnose own status · Obtain information necessary to diagnose sensor status
4	Information integration system for other ships/ drifting objects	· Integrate information on other ships and drifting objects · Diagnose own status	· Obtain information on other ships and drifting objects · Obtain information necessary to diagnose own status · Obtain information necessary to diagnose sensor status

		· Diagnose sensor status	· Transmit integrated information, own status, and sensor status
5	Information integration system for marine weather	· Integrate of the information on marine weather conditions · Diagnose own status · Diagnose sensor status	· Obtain information on marine weather conditions (current location) · Obtain marine weather condition forecast information · Obtain information necessary to diagnose own status · Obtain information necessary to diagnose sensor status · Transmit integrated information, own status, and sensor status
6	Ship control system	· Calculate control variables based on ship action plans for berthing/unberthing · Rudder/engine control · Diagnose rudder/engine status · Diagnose own status	· Obtain ship action plans for berthing/ unberthing · Obtain actual ship's position · Calculate of the deviation between the ship action plans for berthing/ unberthing and the ship's position · Compare current situation with control threshold values · Transmit rudder/engine status and own status
7	Autonomous operation management system	· Control mode switching instructions · Diagnose own status	· Obtain information on own ship, other ships, drifting objects, marine weather conditions, and distance to the berth · Obtain information on the status of each system · Determine whether inside or outside ODD · Obtain information necessary to diagnose own status
8	Onboard crew	· Approve/revise the action plan for berthing/unberthing · Switch the ship steering mode	· Check information on own ship, other ships, drifting objects, marine weather conditions · Check the action plan for berthing/unberthing established by autonomous ship steering system

		· Emergency response (forced switchover to manual mode)	· Check the instruction of switching the ship steering mode by autonomous operation management system · Constant monitoring of each system operation · Constant monitoring of surroundings of own ship

(2) System architecture that clarifies the entire image of the automation system

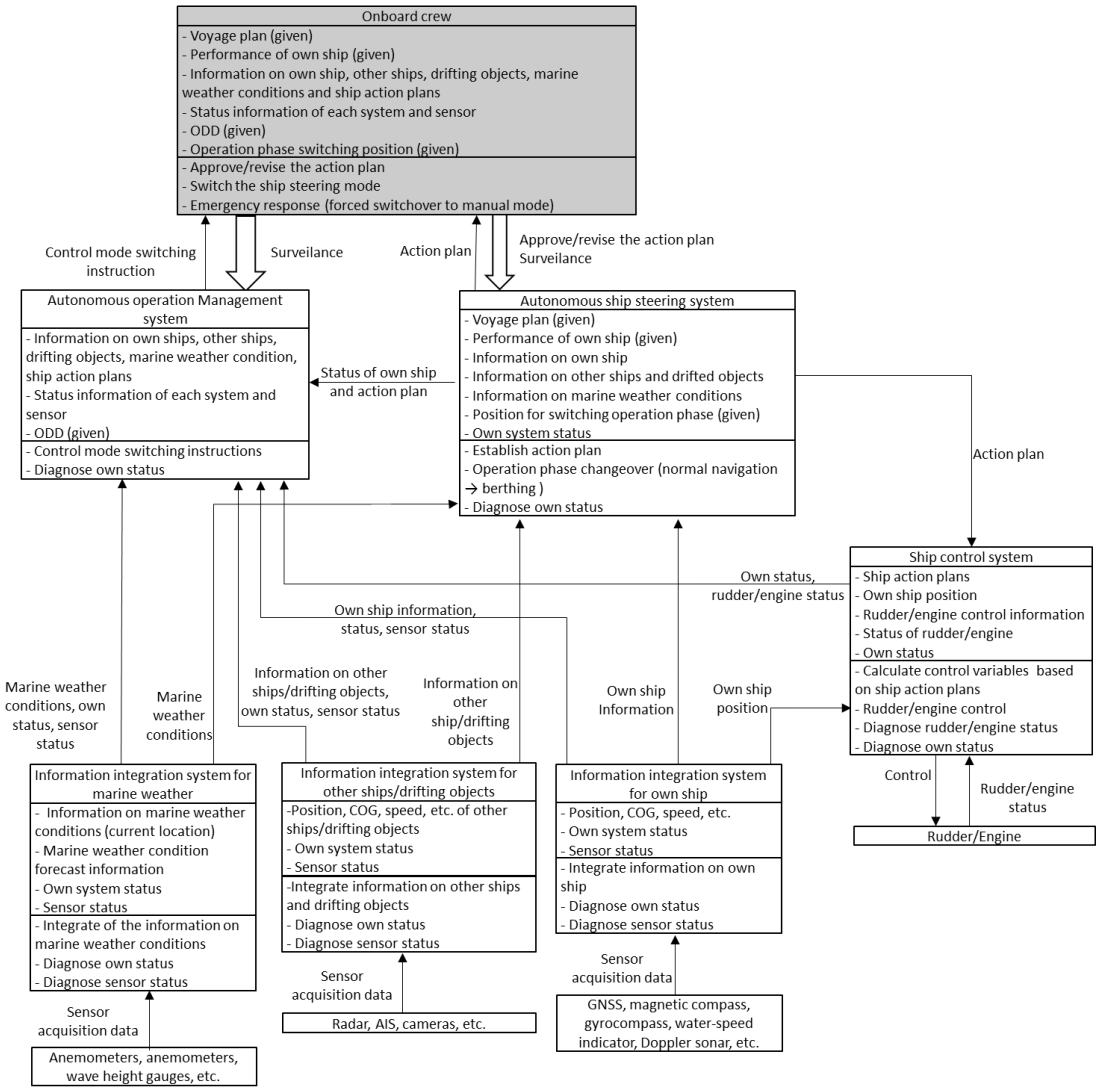

Figure 1.1 System architecture (Phase: Normal navigation)

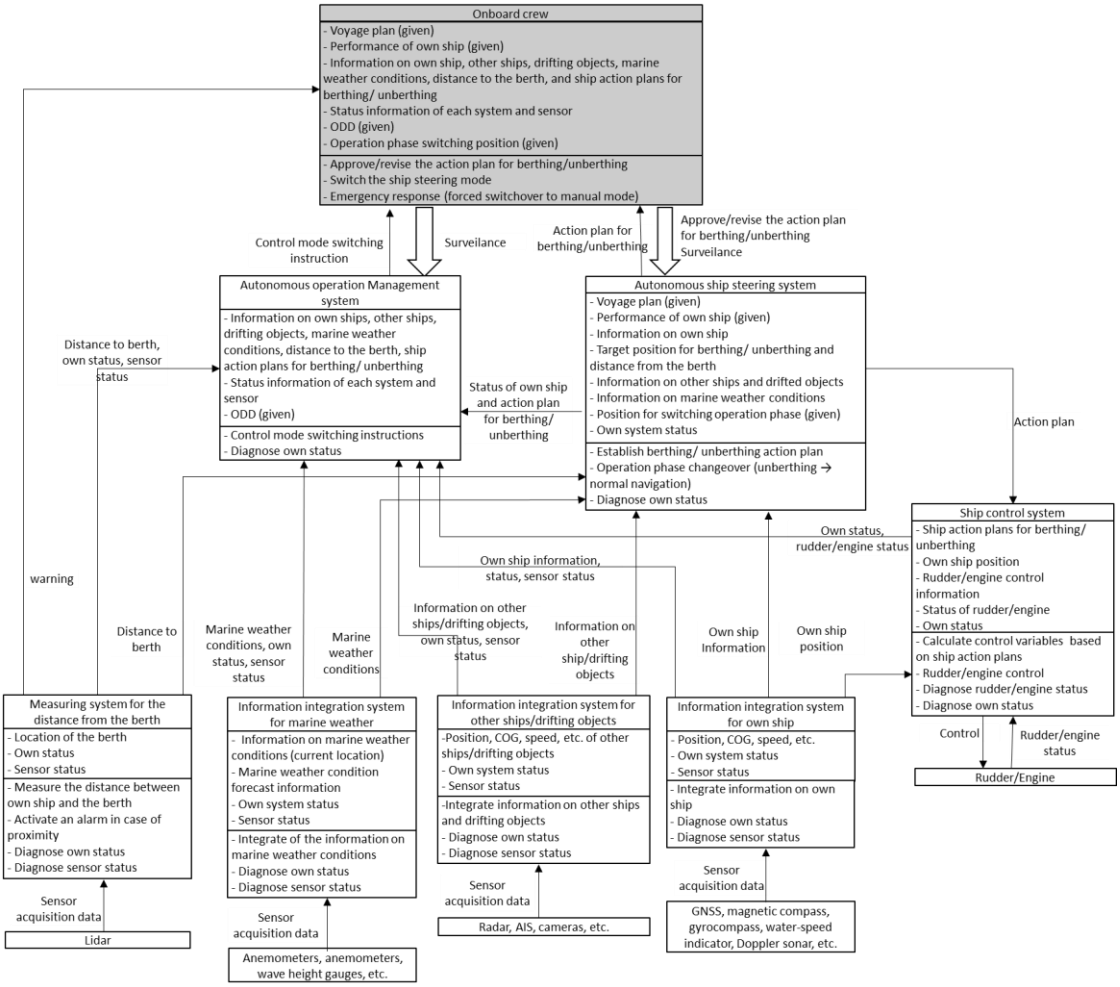

Figure 1.2 System architecture (Phase: Berthing/unberthing)

(3) Outline of the internal operation of the automation system

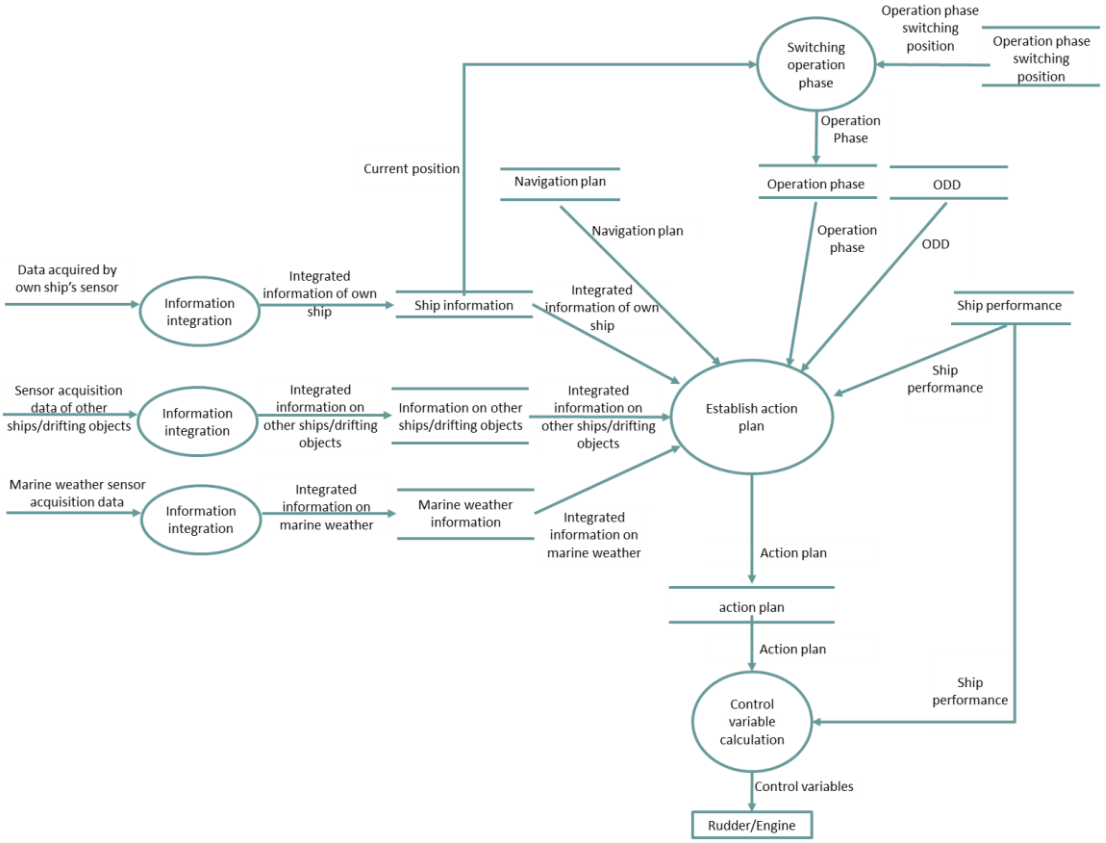

Figure 1.3 Outline of the internal operation regarding autonomous navigation (Phase: Normal navigation)

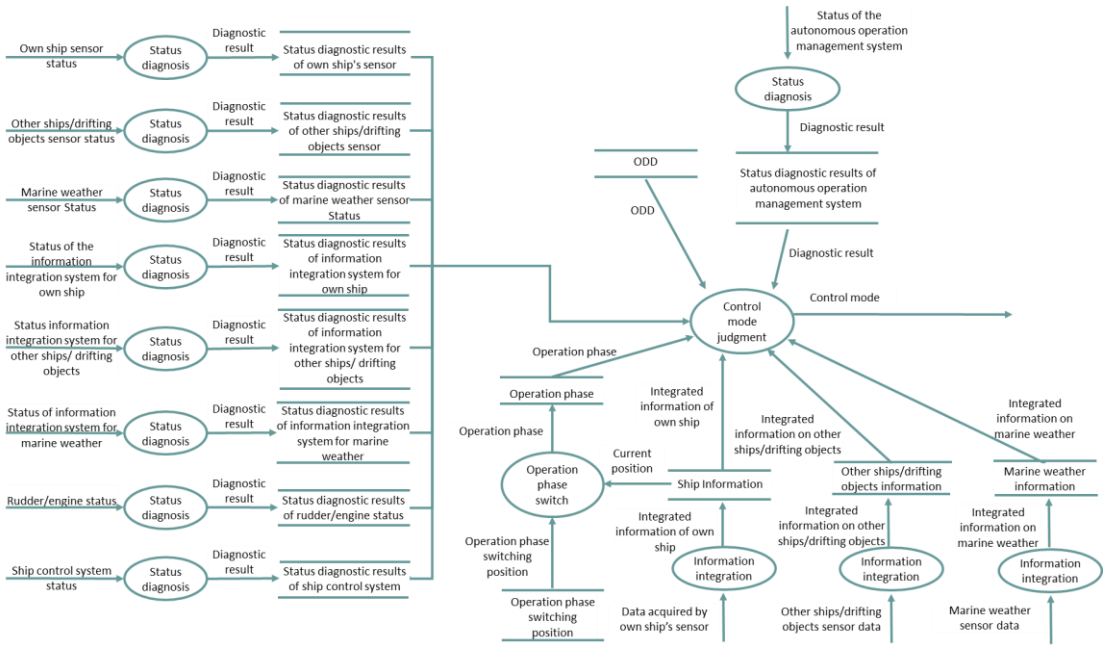

Figure 1.4 Outline of the internal operation regarding mode decision (Phase: Normal navigation)

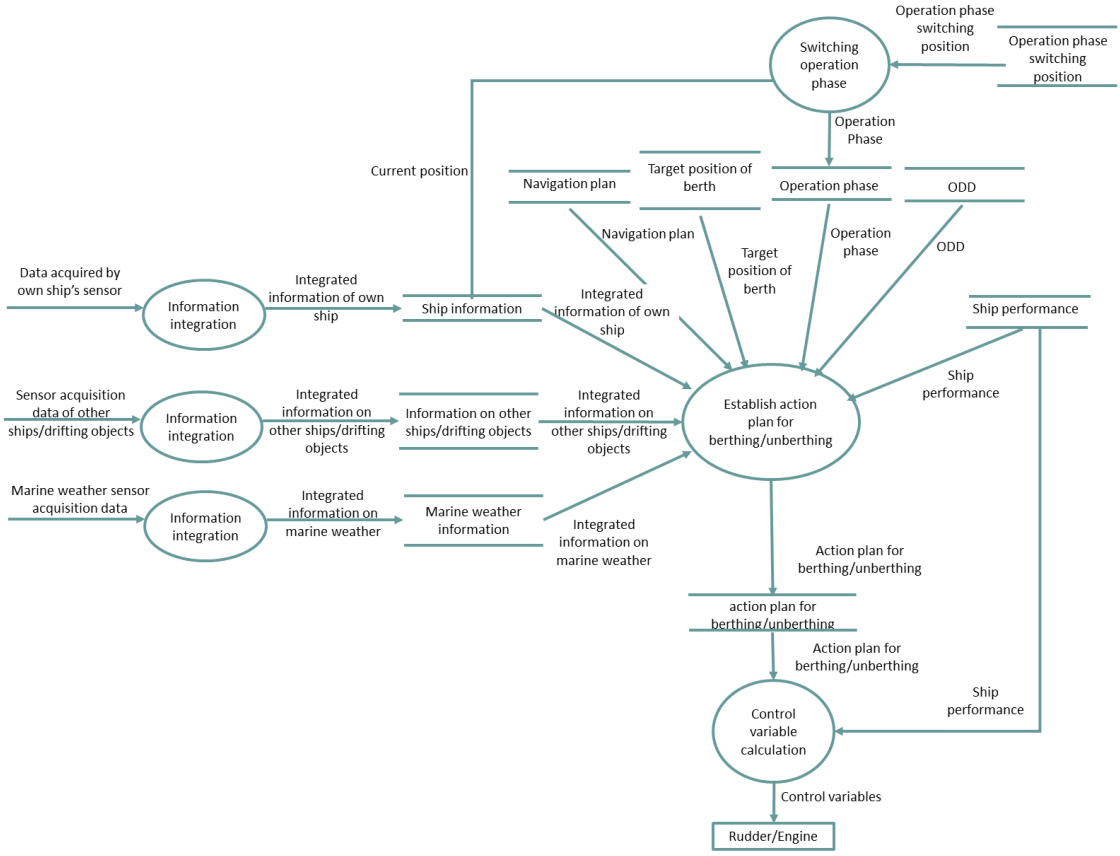

Figure 1.5 Outline of the internal operation regarding autonomous navigation (Phase: Berthing/unberthing)

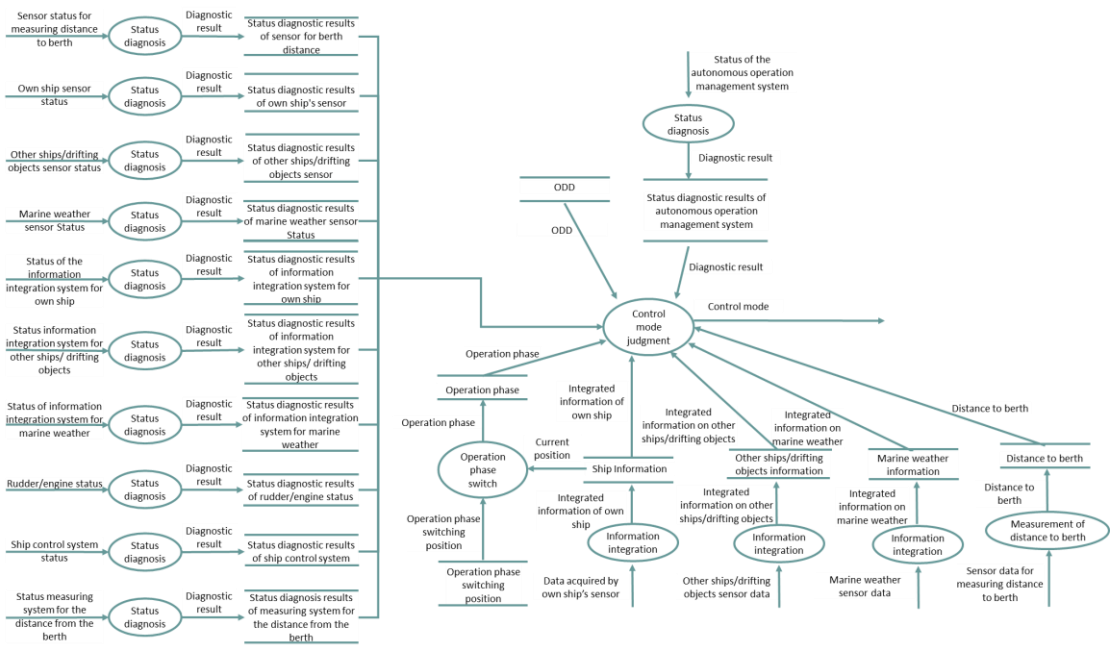

Figure 1.6 Outline of the internal operation regarding mode decision (Phase: Berthing/unberthing)

(4) Outline of the division of roles for the automation system and humans

Table 1.4 Outline of the division of roles for the automation system and humans (Phase: Normal navigation)

Task	Autonomous ship steering system	Information integration system for own ship	Information integration system for other ships/drifting objects	Information integration system for marine weather	Ship control system	Autonomous operation management system	Onboard crew
Switching operation phase	(1) Switching						(2) Surveillance
Obtaining information on own ship		(1) Acquiring and integrating information					(2) Surveillance
Obtaining information on other ships/drifting objects, etc.			(1) Acquiring and integrating information				(2) Surveillance
Obtaining marine weather information				(1) Acquiring and integrating information			(2) Surveillance

Establishing (avoidance) action plan	(1) Establishing						(2) Approving
Executing (avoidance) action plan					(1) Executing		(2) Surveillance
Diagnosis of related sensor status		(1) Diagnosis of conditions	(1) Diagnosis of conditions	(1) Diagnosis of conditions			(2) Surveillance
Diagnosis of own status	(1) Diagnosis of conditions	(1) Diagnosis of conditions	(1) Diagnosis of conditions	(1) Diagnosis of conditions	(1) Diagnosis of conditions	(1) Diagnosis of conditions	(2) Surveillance
Judging inside or outside the ODD and determining steering mode						(1) Judging and determining	(2) Surveillance
Control mode switching instructions and control mode switchover						(1) Control mode switching instructions	(2) Mode switching
Forced switchover to							(1) Surveillance (2)

manual mode							Switch-over to manual mode

Table 1.5 Outline of the division of roles for the automation system and humans (Phase: Berthing/unberthing)

Task	Autonomous ship steering system	Information integration system for own ship	Information integration system for other ships/drifting objects	Information integration system for marine weather	Measuring system for the distance from the berth	Ship control system	Autonomous operation management system	Onboard crew
Switching operation phase	(1) Switching							(2) Surveillance
Obtaining information on own ship		(1) Acquiring and integrating information						(2) Surveillance
Obtaining information on other ships/drifting objects, etc.			(1) Acquiring and integrating information					(2) Surveillance
Obtaining marine weather				(1) Acquiring and				(2) Surveillance

information				integrating information				
Measuring distance to berth					(1) Measuring			(2) Surveillance
Establishing action plan for berthing/unberthing	(1) Establishing							(2) Approving
Executing action plan for berthing/unberthing						(1) Executing		(2) Surveillance
Diagnosis of related sensor status		(1) Diagnosis of conditions	(1) Diagnosis of conditions	(1) Diagnosis of conditions	(1) Diagnosis of conditions			(2) Surveillance
Diagnosis of own status	(1) Diagnosis of conditions	(1) Diagnosis of conditions	(1) Diagnosis of conditions	(1) Diagnosis of conditions	(1) Diagnosis of conditions	(1) Diagnosis of conditions	(1) Diagnosis of conditions	(2) Surveillance
Judging inside or outside the ODD and determining steering mode							(1) Judging and determining	(2) Surveillance

Control mode switching instructions and control mode switchover							(1) Control mode switching instructions	(2) Mode switching
Forced switchover to manual mode								(1) Surveillance (2) Switchover to manual mode

(5) ODD of an automation system

Table 1.6 ODD of an automation system

Marine area conditions	
Navigation zone	Designated ship course
Waters within a departing/arriving harbor	There shall be occupied waters necessary for change of direction in the harbor: 3 L of occupied waters
Waters around a departing/arriving the berth	There shall be occupied waters necessary for departing from or arriving at the berth: 0.5 L of occupied waters
Degree of congestion	Low Congestion: Up to 8 ships within a 3 NM range
Ships not equipped with AIS and obstructions	No non-AIS equipped ships or obstacles that the system cannot detect: No dangerous obstacles of less than 1 m in size within 500 m
Environmental condition	
Marine weather	Calm condition: Wind: 7 m/s or less, wave height: 1.5 m or less, and visibility: 500 m or more
Time	All day
Internal state	

System state	Running normally: No error indication
Equipment required for operation	Running normally: No error indication
Ship motion	Within design constraints of the hull: No anomaly indicated
Other	No emergency events have occurred: No inboard fire, outboard fire, overboard, emergency signal interception, etc.

ii. Risk analysis

Examples of HAZID WS are shown in Tables 1.7 and 1.8. These are risk analysis results on Phase II autonomous ship which explained in the above i (Preparation of documents). The definitions of FI (Frequency Index), SI (Severity Index) and RI (Risk Index) are the same as those of section5.3 of this procedure document.

Table 1.7 HAZID WS (Phase: Normal navigation)

Sheet ID: 1
Phase: Normal navigation

ID	Hazard	Causes	Consequences	Existing Safeguards	Index(only existing safeguards)			Recommendation	Index(Include safeguards recommendation)			Comments
					SI	FI	RI		SI	FI	RI	
Autonomous ship steering system												
1	Error in establishing the action plan	C1.1 Input information not obtained or incorrect (information on own ship, other ships and drifting objects, marine weather, etc.) C1.2 Voyage plan (given) not obtained or incorrect C1.3 Faulty algorithm for establishing the ship action plan in the autonomous ship steering system C1.4 Failure or malfunction of the autonomous ship steering system C1.5 Malware infiltration or hacking	E1.1 Abnormal approach to other ships/objects, or areas with grounding risk E1.2 Collision, grounding, capsizing, and sinking	• Alarm for each system failure • Alarm when various information and voyage plans are not entered • Double-checking when entering voyage plans • Alarm when jumping position of own ship or other ships/drifts • Prior verification by simulations of action planning algorithms • Connect only to removable media with no viruses detected by virus detection software as well as no connection to external networks • Constant monitoring by the onboard crew • forced switchover to manual steering by onboard crew	1	5	6	• Improvement of the action planning algorithm • Consideration of measures to improve system reliability (redundancy, etc.) (including cost-benefit study)	1	5	6	* Recommendations to improve the safety more: • Verification of outputs and introduction of functions to deal with the verification results (implemented by human or machine, depending on the level of automation)

2	No implementation of the action plan	C2.1 Input information not obtained (information on own ship, other ships and drifting objects, marine weather, etc.) C2.2 Voyage plan (given) not obtained C2.3 Failure or malfunction of the autonomous ship steering system C2.4 Malware intrusion or hacking C2.5 Failure to receive inquiry (trigger for activating this function)	Same as ID1	• Alarm for each system failure • Alarm when various information and voyage plans are not entered • Alarm when a certain amount of time has elapsed • Pre verification through simulations • Connect only to removable media with no viruses detected by virus detection software as well as no connection to external networks • Constant monitoring by the onboard crew • forced switchover to manual steering by onboard crew	1	5	6	Same as ID1	1	5	6	* Recommendations to improve the safety more: • If there is no response, the inquiry source shall be made to ask again with new input information. • Introduce a function to deal with no response even after re querying (implemented by human or machine, depending on the level of automation)

3	Too late/too early implementation of the action plan	C3.1 Input information not obtained or obtained at the wrong time (information on own ship, other ships and drifting objects, marine weather, etc.) C3.2 Failure of the autonomous ship steering system's berthing/ unberthing action planning algorithm (too much time is spent on calculations for action planning) C3.3 Failure or malfunction of the autonomous ship steering system C3.4 Malware infiltration or hacking C3.5 Wrong timing of inquiry (trigger for activation of this function)	Same as ID1	Same as ID2	1	5	6	Same as ID1	1	5	6	* Recommendations to improve the safety more: • If the response is too late, the inquiry source shall be made to ask again with new input information. • Introduce a function to deal with cases where a response is not received in time (implemented by human or machine, depending on the level of automation)

4	Error in the switching operation phase (normal navigation phase to berthing phase)	C4.1 Incorrect input of the (given) position to switch the operation phase C4.2 Incorrect input information (own ship's position information) C4.3 Failure or malfunction of the autonomous ship steering system C4.4 Malware intrusion or hacking	E4.1 Deviation from course E4.2 Abnormal approach to other ships/objects, berth, or areas with grounding risk E4.3 Collision with other ships or berth, grounding, and capsizing or sinking	• Alarm for each system failure • Double check when inputting the operation phase switching position • Alarm at the time of position jump of own ship • Alarm at the time of route deviation • Pre verification through simulations • Connect only to removable media with no viruses detected by virus detection software as well as no connection to external networks • Constant monitoring by the onboard crew • forced switchover to manual steering by onboard crew	1	5	6	• Consideration of measures to improve system reliability (redundancy, etc.) (including cost-benefit study)	1	5	6	

5	No changeover of the operation phase (normal navigation phase to berthing phase)	C5.1 Incorrect input of the (given) position to switch the operation phase C5.2 Incorrect input or no input of input information (own ship's position information) C5.3 Failure or malfunction of the autonomous ship steering system C5.4 Malware intrusion or hacking C5.5 Failure to receive inquiry (trigger for activating this function)	Same as ID4	• Alarm for each system failure • Alarm if operation phase switching position or own position are not entered • Alarm at the time of position jump of own ship • Alarm at the time of route deviation • Pre verification through simulations • Activate alarm when a certain distance from the operation phase switching position is exceeded • Connect only to removable media with no viruses detected by virus detection software as well as no connection to external networks • Constant monitoring by the onboard crew • forced switchover to manual steering by onboard crew	1	5	6	Same as ID4	1	5	6	Same as ID2

6	Too late/too early to implement switching the operation phases (normal navigation phase to berthing phase)	C6.1 Wrong timing of obtaining input information (own ship's position) C6.2 Malfunction of the operation phase switching algorithm (switching operation takes too long) C6.3 Failure or malfunction of the autonomous ship steering system C6.4 Malware intrusion or hacking C6.5 Wrong timing of inquiry (trigger for activating this function)	Same as ID4	• System failure alarm • Alarm at the time of route deviation • Pre verification through simulations • Activate alarm when a certain distance from the operation phase switching position is exceeded • Connect only to removable media with no viruses detected by virus detection software as well as no connection to external networks • Constant monitoring by the onboard crew • forced switchover to manual steering by onboard crew	1	5	6	Same as ID4	1	5	6	Same as ID3
7	Error in diagnosis of own status	C7.1 Wrong algorithm for the self-diagnostic function of the autonomous ship steering system C7.2 Incorrect input information (information required for self-diagnosis) C7.3 Malware intrusion or hacking	• Misdiagnose as normal when abnormal → Same as ID4 • Misdiagnose as abnormal when normal → Switch to manual steering based on alarm	• Pre verification of the self-diagnostic function • Connect only to removable media with no viruses detected by virus detection software as well as no connection to external networks • Constant monitoring by the onboard crew • forced switchover to manual steering by onboard crew	1	5	6	Same as ID4	1	5	6	

8	No implementation of the diagnosis of own ship's status	C8.1 Failure, malfunction, or stoppage of the self-diagnostic function of the autonomous ship steering system C8.2 Input information (information necessary for self-diagnosis) not obtained C8.3 Malware intrusion or hacking	• Diagnosis not performed when normal → No problem (alarm will be activated when a certain period of time is exceeded) • Diagnosis not performed when abnormal → Same as ID4	• Pre verification of the self-diagnostic function • Alarm activated when a certain amount of time is exceeded • Connect only to removable media with no viruses detected by virus detection software as well as no connection to external networks • Constant monitoring by the onboard crew • forced switchover to manual steering by onboard crew	1	5	6	Same as ID4	1	5	6	

9	Too late/too early to implement the diagnosis of own status	C9.1 Failure or malfunction of the self-diagnostic function of the autonomous ship steering system C9.2 Malfunction of the self-diagnostic algorithm of the autonomous ship steering system (self-diagnostic operation takes too much time) C9.3 Incorrect timing for obtaining input information (information necessary for self-diagnosis) C9.4 Malware intrusion or hacking	• Too late to diagnose when normal → No problem (alarm will be activated when a certain period of time is exceeded) • Too late to diagnose as abnormal when abnormal → E9.1 Delay in switching to the manual operation E9.2 Autonomous operation outside ODD E9.3 Deviation from course E9.4 Abnormal approach to other ships/objects, or areas with grounding risk E9.5 Collision, grounding, capsizing, or sinking	Same as ID8	1	5	6	Same as ID4	1	5	6	
Information integration system for own ship												

10	Error in integration of own ship information	C10.1 Inconsistency in input information (e.g., different data between sensors of own ship, integration with old information, etc.) C10.2 Failure or malfunction of the information integration function and, error in the integration algorithm C10.3 Malware intrusion or hacking	E10.1 Establishment of the incorrect avoidance action plan E10.2 Incorrect calculation of the control variables E10.3 Incorrect/no switching of the operation phase E10.4 Deviation from course E10.5 Abnormal approach to other ships/objects or areas with grounding risk E10.6 Collision, grounding, capsizing, or sinking	• Advance verification of the information integration function • Integrating a method for dealing with discrepancies in data (which data should be prioritized) • Alarm for each system failure • Warnings when the same type of data differs • Connect only to removable media with no viruses detected by virus detection software as well as no connection to external networks • Constant monitoring by the onboard crew • forced switchover to manual steering by onboard crew	1	5	6	• Consideration of measures to improve system reliability (redundancy, etc.) (including cost-benefit study) • Improvement of the information integration algorithm	1	5	6	* Recommendations to improve the safety more: • Management of the reliability of integrated information (reliability evaluation and formulation of countermeasures in case of low reliability)

11	No implementation of integrating information of own ship	C11.1 Inconsistency in input information (different data between sensors of own ship) C11.2 Failure or malfunction of the information integration function and error in the integration algorithm C11.3 Malware intrusion or hacking C11.4 Failure to receive inquiry (trigger for activating this function)	Same as ID10	• Advance verification of the information integration function • Incorporating a method for dealing with discrepancies in data (which data should be prioritized) • Alarm for each system failure • Warnings when the same type of data differs • Alarm activated when a certain amount of time is exceeded • Connect only to removable media with no viruses detected by virus detection software as well as no connection to external networks • Constant monitoring by the onboard crew • forced switchover to manual steering by onboard crew	1	4	5	Same as ID10	1	4	5	* Recommendations to improve the safety more: • Introduce a function to deal with the absence of outputs (e.g., restarting the system in question; prepared separately from diagnosis of own to deal with the case of a stoppage of functionality)

12	Too late/too early to implement integrating own ship information	C12.1 Malfunction of the information integration function/algorithm (information integration takes too much time) C12.2 Wrong timing of information acquisition from different sensors C12.3 Malware intrusion or hacking C12.4 Wrong timing of inquiry (trigger for activating this function)	E12.1 Establishment of the incorrect avoidance action plan E12.2 Incorrect calculation of the control variables E12.3 Switch the operation phase at wrong position E12.4 Deviation from course E12.5 Abnormal approach to other ships/objects or areas with grounding risk E12.6 Collision, grounding, capsizing, or sinking	Same as ID11	1	5	6	Same as ID10	1	5	6	* Recommendations to improve the safety more: • Introduce a function to deal with large delays in output (e.g., restarting the system in question).
13	Error in the diagnosis of own status	C13.1 Failure or malfunction of the self-diagnostic function C13.2 Wrong algorithm for the self-diagnostic function C13.3 Incorrect input information (information required for self-	Same as ID7	Same as ID7	1	5	6	• Improvements in algorithm for self-diagnostic function	1	5	6	

14	No implementation of the diagnosis of own status	C14.1 Failure, malfunction, or stoppage of the self-diagnostic function C14.2 Input information (information necessary for self-diagnosis) not obtained C14.3 Malware intrusion	Same as ID8	Same as ID8	1	5	6	Same as ID13	1	5	6	
15	Too late/too early to implement the diagnosis of own status	C15.1 Failure or malfunction of the self-diagnostic function C15.2 Malfunction of the self-diagnostic algorithm (self-diagnostic operation takes too much time) C15.3 Incorrect timing for obtaining input information (information required for self-diagnosis) C15.4 Malware intrusion or hacking	Same as ID9	Same as ID9	1	6	7	Same as ID13	1	6	7	

16	Error in diagnosing sensor status	C16.1 Failure or malfunction of the status diagnostic function for the sensor C16.2 Wrong algorithm for the status diagnostic function for the sensors of own ship C16.3 Incorrect input information (information required for sensor status diagnosis) C16.4 Malware intrusion or hacking	• Misdiagnose as normal when abnormal → Same as ID10 • Misdiagnose as abnormal when normal → Switch to manual steering based on alarm	• Pre verification of the status diagnostic function and algorithm for the sensor • Connect only to removable media with no viruses detected by virus detection software as well as no connection to external networks	1	5	6	• Improvements in algorithm for the diagnostic function of the sensor status	1	5	6	
17	No implementation of the diagnosis of sensor status	C17.1 Failure or malfunction of the status diagnostic function for the sensors of own ship C17.2 Input information (information necessary for sensor status diagnosis) not obtained C17.3 Malware intrusion or hacking	• Diagnosis not performed when abnormal → Same as ID10 • Diagnosis not performed when normal → No problem (alarm will be activated when a certain period of time is exceeded)	• Pre verification of the status diagnostic function for the sensors • Alarm activated when a certain amount of time is exceeded • Connect only to removable media with no viruses detected by virus detection software as well as no connection to external networks	1	5	6	Same as ID16	1	5	6	

18	Too late/too early to implement the diagnosis of sensor status	C18.1 Failure or malfunction of the status diagnostic function for the sensors of own ship C18.2 Malfunction of the sensor status diagnosis algorithm (status diagnosis operation takes too much time) C18.3 Wrong timing of obtaining input information (information required for sensor status diagnosis) C18.4 Malware intrusion or hacking	• Too late to diagnose as normal when normal → No problem (alarm will be activated when a certain period of time is exceeded) • Too late to diagnose as abnormal when abnormal → Same as ID12	• Pre verification of the status diagnostic function and algorithm for the sensors • Alarm activated when a certain amount of time is exceeded • Connect only to removable media with no viruses detected by virus detection software as well as no connection to external networks	1	5	6	Same as ID16	1	5	6	
Information integration system for other ships and drifting objects												
19	Error in integration information of other ships and drifting objects	C19.1 Inconsistency in input information (e.g., different data between sensors, integration with old information) C19.2 Failure or malfunction of the information integration function as well as errors in the integration algorithm	E19.1 Establishment of the incorrect avoidance action plan E19.2 Abnormal approach to other ships/objects or areas with grounding risk E19.3 Collision	Same as ID10	1	5	6	Same as ID10	1	5	6	Same as ID10

20	No implementation of integration information of other ships and drifting objects	C20.1 Inconsistency in input information (e.g., different data between sensors) C20.2 Failure or malfunction of the information integration function as well as errors in the integration algorithm C20.3 Malware intrusion or hacking C20.4 Failure to receive inquiry (trigger for activating this function)	Same as ID19	Same as ID11	1	4	5	Same as ID10	1	4	5	Same as ID11
21	Too late/too early implementation of integration information of other ships and drifting objects	C21.1 Failure of information integration function/algorithm (information integration takes too much time) C21.2 Wrong timing of information acquisition from different sensors C21.3 Malware intrusion or hacking C21.4 Wrong timing of inquiry (trigger for activation of this function)	Same as ID19	Same as ID11	1	5	6	Same as ID10	1	5	6	Same as ID12

22	Error in diagnosing own status	C22.1 Failure or malfunction of the self-diagnostic function C22.2 Wrong algorithm for the self-diagnostic function C22.3 Incorrect input information (information necessary for self-diagnosis) C22.4 Malware intrusion or hacking	Same as ID7	Same as ID7	1	5	6	Same as ID13	1	5	6	
23	No implementation of diagnosing own status	C23.1 Failure or malfunction of the self-diagnostic function C23.2 Input information (information necessary for self-diagnosis) not obtained C23.3 Malware intrusion or hacking	Same as ID8	Same as ID8	1	5	6	Same as ID13	1	5	6	

24	Too late/too early implementation of diagnosing own status	C24.1 Failure or malfunction of the self-diagnostic function C24.2 Malfunction of the self-diagnostic algorithm (self-diagnostic operation takes too much time) C24.3 Wrong timing of obtaining input information (information required for self-diagnosis) C24.4 Malware intrusion or hacking	Same as ID9	Same as ID9	1	6	7	Same as ID13	1	6	7	
25	Error in diagnosing sensor status	C25.1 Failure or malfunction of the status diagnostic function for the sensors C25.2 Wrong algorithm for the status diagnostic function for the sensors C25.3 Incorrect input information (information necessary for sensor status diagnosis) C25.4 Malware intrusion or hacking	• Misdiagnose as normal when abnormal → Same as ID19 • Misdiagnose as abnormal when normal → Switch to manual steering based on alarm	Same as ID16	1	5	6	Same as ID16	1	5	6	

26	No implementation of diagnosing sensor status	C26.1 Failure or malfunction of the status diagnostic function for the sensors C26.2 Input information (information necessary for sensor status diagnosis) not obtained C26.3 Malware intrusion or hacking	• Diagnosis not performed when abnormal → Same as ID19 • Diagnosis not performed when normal → No problem (alarm will be activated when a certain period of time is exceeded)	Same as ID17	1	5	6	Same as ID16	1	5	6	
27	Too late/too early implementation of diagnosing sensor status	C27.1 Failure or malfunction of the status diagnostic function for the sensors C27.2 Malfunction of the algorithm for the sensor status diagnosis (status diagnosis operation takes too much time) C27.3 Wrong timing of obtaining input information (information required for sensor status diagnosis) C27.4 Malware intrusion or hacking	• Too late diagnosis as normal when normal → No problem (alarm will be activated when a certain period of time is exceeded) • Too late diagnosis as abnormal when abnormal → Same as ID19	Same as ID18	1	5	6	Same as ID16	1	5	6	
Information integration system for marine weather												

28	Error in integration of marine weather information	C28.1 Inconsistency in input information (e.g., different data between sensors, integration with old information) C28.2 Failure or malfunction of the information integration function as well as error in integration algorithm C28.3 Malware intrusion or hacking	Same as ID19	Same as ID10	1	5	6	Same as ID10	1	5	6	Same as ID10
29	No implementation of integrating marine weather information	C29.1 Inconsistency in input information (e.g., different data between sensors) C29.2 Failure or malfunction of the information integration function as well as error in integration algorithm C29.3 Malware intrusion or hacking C29.4 Failure to receive inquiry (trigger for activating this function)	Same as ID19	Same as ID11	1	4	5	Same as ID10	1	4	5	Same as ID11

30	Too late/too early implementation of integrating marine weather information	C30.1 Failure or malfunction of the information integration function/algorithm (information integration takes too much time) C30.2 Wrong timing of information acquisition from different sensors C30.3 Malware intrusion or hacking C30.4 Wrong timing of inquiry (trigger for activation of this function)	Same as ID19	Same as ID11	1	5	6	Same as ID10	1	5	6	Same as ID12
31	Error in diagnosing own status	C31.1 Failure or malfunction of the self-diagnostic function C31.2 Wrong algorithm for the self-diagnostic function C31.3 Incorrect input information (information necessary for self-diagnosis) C31.4 Malware intrusion or hacking	Same as ID7	Same as ID7	1	5	6	Same as ID13	1	5	6	

32	No implementation of diagnosing own status	C32.1 Failure or malfunction of the self-diagnostic function C32.2 Input information (information necessary for self-diagnosis) not obtained C32.3 Malware intrusion or hacking	Same as ID8	Same as ID8	1	5	6	Same as ID13	1	5	6	
33	Too late/too early implementation of diagnosing own status	C33.1 Failure or malfunction of the self-diagnostic function C33.2 Malfunction of the self-diagnostic algorithm (self-diagnostic operation takes too much time) C33.3 Wrong timing of obtaining input information (information required for self-diagnosis) C33.4 Malware intrusion or hacking	Same as ID9	Same as ID9	1	6	7	Same as ID13	1	6	7	

34	Error in diagnosing sensor status	C34.1 Failure or malfunction of the status diagnostic function for the sensors C34.2 Wrong algorithm for the status diagnostic function for the sensors C34.3 Incorrect input information (information necessary for sensor status diagnosis) C34.4 Malware intrusion or hacking	• Misdiagnose as normal when abnormal → Same as ID19 • Misdiagnose as abnormal when normal → Switch to manual steering based on alarm	Same as ID16	1	5	6	Same as ID16	1	5	6	
35	No implementation of diagnosing sensor status	C35.1 Failure or malfunction of the status diagnostic function for the sensors C35.2 Input information (information necessary for sensor status diagnosis) not obtained C35.3 Malware intrusion or hacking	• Diagnosis not performed when abnormal → Same as ID19 • Diagnosis not performed when normal → No problem (alarm will be activated when a certain period of time is exceeded)	Same as ID17	1	5	6	Same as ID16	1	5	6	

36	Too late/too early implementation of diagnosing sensor status	C36.1 Failure or malfunction of the status diagnostic function for the sensors C36.2 Malfunction of the algorithm for the sensor status diagnosis (status diagnosis operation takes too much time) C36.3 Wrong timing of obtaining input information (information required for sensor status diagnosis) C36.4 Malware intrusion or hacking	• Too late diagnosis as normal when normal → No problem (alarm will be activated when a certain period of time is exceeded) • Too late diagnosis as abnormal when abnormal → Same as ID19	Same as ID18	1	5	6	Same as ID16	1	5	6	
Ship control system												
37	Error in calculation of the control variables based on the action plan	C37.1 Error in the action plan C37.2 Incorrect input information (information required for control variables calculation) C37.3 Error in the control variables calculation algorithm C37.4 Failure or malfunction of the ship control system C37.5 Malware intrusion or hacking	E37.1 Deviation from course E37.2 Abnormal approach to other ships/objects or areas with grounding risk E37.3 Collision, grounding, capsizing, or sinking	• System failure alarm • Pre verification of the control variables calculation algorithm through simulations • Connect only to removable media with no viruses detected by virus detection software as well as no connection to external networks • Constant monitoring by the onboard crew • forced switchover to manual steering by onboard crew	1	5	6	• Improvement of the control variables calculation algorithm • Consideration of measures to improve system reliability (redundancy, etc.) (including cost-benefit study)	1	5	6	

38	No implementation of calculating the control variables based on the action plan	C38.1 Action plan not obtained C38.2 Input information (information required for control variables calculation) not obtained C38.3 Failure or malfunction of the ship control system C38.4 Malware intrusion or hacking C38.5 Failure to receive inquiry (trigger for activating this function)	Same as ID37	• System failure alarm • Alarm at the time when various information is not obtained • Pre verification through simulations • Alarm activated when a certain amount of time is exceeded • Connect only to removable media with no viruses detected by virus detection software as well as no connection to external networks • Constant monitoring by the onboard crew	1	5	6	• Consideration of measures to improve system reliability (redundancy, etc.) (including cost-benefit study)	1	5	6	Same as ID2

39	Too late/too early to implement control variables calculations based on the action plan	C39.1 Wrong timing of obtaining the action plan C39.2 Wrong timing of acquiring input information (information required for control variables calculation) C39.3 Malfunction in the control variables calculation algorithm (excessive time required for control variables calculation) C39.4 Failure or malfunction in the ship control system C39.5 Malware intrusion C39.6 Wrong timing of inquiry (trigger for activation of this function)	Same as ID37	• System failure alarm • Pre verification through simulations • Warning activated when a certain period of time has elapsed • Alarm activated when a certain amount of time is exceeded • Connect only to removable media with no viruses detected by virus detection software as well as no connection to external networks • Constant monitoring by the onboard crew • forced switchover to manual steering by onboard crew	1	5	6	Same as ID38	1	5	6	Same as ID3
40	Error in control of the rudder or engine	C40.1 Error in control variables calculation C40.2 Actuator malfunction or failure	E40.1 Unable to navigate E40.2 Deviation from course E40.3 Abnormal approach to other ships/objects, or areas with grounding risk E40.4 Collision, grounding, capsizing, or sinking	• Pre verification of the system • Alarms in case of actuator failure or malfunction • Constant monitoring by the onboard crew • forced switchover to manual steering by onboard crew	1	5	6	• Consideration of measures to improve system reliability (redundancy, etc.) (including cost-benefit study)	1	5	6	* Recommendations to improve the safety more: • Introduction of a function to deal with incorrect rudder/engine status (e.g., restarting the system in question)

41	No implementation of control of the rudder or engine	C41.1 Input information (control variables) not obtained C41.2 Malfunction or failure of the actuator C41.3 Failure to receive inquiry (trigger for activating this function)	Same as ID40	• Alarms in case of actuator failure or malfunction • Alarm when control variables not obtained • Alarm activated when a certain amount of time is exceeded • Constant monitoring by the onboard crew • forced switchover to manual steering by onboard crew	1	5	6	Same as ID40	1	5	6	* Recommendations to improve the safety more: • Introduction of a function to deal with cases where the rudder/engine is not under control (e.g., restarting the system in question) • If there is no response, the inquiry source shall be made to ask again with new input information. • Introduce a function to deal with no response even after re querying (implemented by human or machine, depending on the level of automation)

42	Too late/too early to implement controlling the rudder or engine	C42.1 Wrong timing of obtaining input information (control variables) C42.2 Malfunction or failure of the actuator C42.3 Wrong timing of inquiry (trigger for activation of this function)	Same as ID40	Same as ID41	1	5	6	Same as ID40	1	5	6	* Recommendations to improve the safety more: • Introduction of a function to deal with rudder/engine control delays exceeding a certain level (e.g., restarting the system in question). • If the response is too late, the inquiry source shall be made to ask again with new input information. • Introduce a function to deal with cases where a response is not received in time (implemented by human or machine, depending on the level of automation)

43	Error in diagnosis of rudder/engine conditions	C43.1 Failure or malfunction of the rudder/engine condition diagnostic function C43.2 Wrong algorithm for the rudder/engine condition diagnostic function C43.3 Incorrect input information (information required for rudder/engine condition diagnosis) C43.4 Malware intrusion or hacking	Same as ID7	Same as ID7	1	5	6	• Improved algorithms for rudder/engine condition diagnostic functions	1	5	6	
44	No implementation of diagnosis of rudder/engine conditions	C44.1 Failure or malfunction of the rudder/engine condition diagnostic function C44.2 Input information (information required for rudder/engine condition diagnosis) not obtained C44.3 Malware intrusion or hacking	Same as ID8	Same as ID8	1	5	6	Same as ID43	1	5	6	

45	Too late/too early to implement diagnosis of rudder/engine conditions	C45.1 Failure or malfunction of the rudder/engine condition diagnostic function C45.2 Malfunction of the rudder/engine condition diagnostic algorithm (self-diagnostic operation takes too much time) C45.3 Wrong timing of obtaining input information (information required for rudder/engine condition diagnosis) C45.4 Malware intrusion or hacking	Same as ID9	Same as ID9	1	6	7	Same as ID43	1	6	7	
46	Error in diagnosing own status	C46.1 Failure or malfunction of the self-diagnostic function C46.2 Wrong algorithm for the self-diagnostic function C46.3 Incorrect input information (information required for self-diagnosis) C46.4 Malware intrusion or hacking	Same as ID7	Same as ID7	1	5	6	Same as ID13	1	5	6	

47	No implementation of diagnosing own status	C47.1 Failure, malfunction, or stoppage of the self-diagnostic function C47.2 Input information (information necessary for self-diagnosis) not obtained C47.3 Malware intrusion or hacking	Same as ID8	Same as ID8	1	5	6	Same as ID13	1	5	6	
48	Too late/too early implementation of diagnosing own status	C48.1 Failure or malfunction of the self-diagnostic function C48.2 Malfunction of the self-diagnostic algorithm (self-diagnostic operation takes too much time) C48.3 Incorrect timing of obtaining input information (information required for self-diagnosis) C48.4 Malware intrusion or hacking	Same as ID9	Same as ID9	1	6	7	Same as ID13	1	6	7	
Autonomous Operation Management System												

49	Error in instructions for switching the ship steering mode	C49.1 Failure or malfunction of the autonomous operation management system C49.2 Error in the algorithm to switch the operation mode C49.3 Error in input information (information required for making the operation mode switching decision) C49.4 Malware intrusion or hacking	E49.1 Autonomous steering outside ODD E49.2 Deviation from course E49.3 Abnormal approach to other ships/objects or areas with grounding risk E49.4 Collision, grounding, capsizing, or sinking	• Alarm for each system failure • Double-checking at the time of ODD input • Alarm at the time of route deviation • Prior verification of the instruction function to switch the ship steering mode through simulations • Connect only to removable media with no viruses detected by virus detection software as well as no connection to external networks • Constant monitoring by the onboard crew • forced switchover to manual steering by onboard crew	1	5	6	• Improvement of the ship steering mode switching algorithm • Consideration of measures to improve system reliability (redundancy, etc.) (including cost-benefit study)	1	5	6	

50	No implementation of the ship steering mode switching instructions	C50.1 Failure or malfunction of the autonomous operation management system C50.2 Error in the algorithm to switch the operation mode C50.3 Error in input information (information required for making the operation mode switching decision) C50.4 Malware intrusion or hacking C50.5 Failure to receive inquiry (trigger for activating this function)	Same as ID49	• Alarm for each system failure • Alarm activated when a certain amount of time is exceeded • Double-checking at the time of ODD input • Alarm at the time of route deviation • Prior verification of the instruction function to switch the ship steering mode through simulations • Connect only to removable media with no viruses detected by virus detection software as well as no connection to external networks	1	5	6	Same as ID49	1	5	6	Same as ID2

51	Too late/too early to give the ship steering mode switching instructions	C51.1 Failure or malfunction of the autonomous operation management system C51.2 Malfunction of the algorithm to switch the operation mode (calculating the decision to switch the operation mode takes too much time) C51.3 Wrong timing of obtaining input information (information necessary to decide whether to switch the operation mode) C51.4 Malware infiltration or hacking C51.5 Wrong timing of inquiry (trigger for activation of this function)	Same as ID49	Same as ID50	1	5	6	Same as ID49	1	5	6	Same as ID3

52	Error in diagnosing own status	C52.1 Failure or malfunction of the self-diagnostic function C52.2 Wrong algorithm for the self-diagnostic function C52.3 Incorrect input information (information required for self-diagnosis) C52.4 Malware intrusion or hacking	Same as ID7	Same as ID7	1	5	6	Same as ID13	1	5	6	
53	No implementation of diagnosing own status	C53.1 Failure, malfunction, or stoppage of the self-diagnostic function C53.2 Input information (information necessary for self-diagnosis) not obtained C53.3 Malware intrusion or hacking	Same as ID8	Same as ID8	1	5	6	Same as ID13	1	5	6	

54	Too late/too early implementation of diagnosing own status	C54.1 Failure or malfunction of the self-diagnostic function C54.2 Malfunction of the self-diagnostic algorithm (self-diagnostic operation takes too much time) C54.3 Incorrect timing of obtaining input information (information required for self-diagnosis) C54.4 Malware intrusion or hacking	Same as ID9	Same as ID9	1	6	7	Same as ID13	1	6	7	
Onboard crew												

55	Error in approving /revising of action plan	C55.1 Overconfidence in the autonomous ship steering system C55.2 Insufficient understanding of the operation method C55.3 HMI that makes it difficult to understand the intention of action plan C55.4 Misperception of their own ship's performance or current information on their ship/surrounding/environment, etc. C55.5 Failure or malfunction of the autonomous ship steering system C55.6 Operation mistake C55.7 Distraction due to concurrent tasks and time pressure	Same as ID1	• Preparation of manuals on how to operate the sutonomous ship steering system • Advance training of the onboard crew • Appropriate HMI design and verification • Alarm for failure or malfunction of the autonomous ship steering system • Setting confirmation notification	1	5	6	• Establishment of advance training method of the onboard crew	1	5	6	* Recommendations to improve the safety more: • Workload management of the onboard crew (ensuring the enough number of the onboard crews for the amount of tasks and replenishing resources by introducing available automation)

56	No implamentation of approving/revising of action plan	C56.1 Sudden illness, napping, or no crews in bridge, etc. C56.2 Insufficient understanding of the need for the approving/revising of action plan C56.3 HMI that makes it difficult to understand the need for the approving/revising of action plan C56.4 Failure or malfunction of the autonomous ship steering system C56.5 Operation mistake C56.6 Restraint by other tasks C56.7 No notification of the need for approving action plan (and no alarm)	Same as ID1	• Preparation of manuals on how to operate the sutonomous ship steering system • Advance training of the onboard crew • Appropriate HMI design and verification • Alarm for failure or malfunction of the autonomous ship steering system • Setting confirmation notification • Alarm when a certain amount of time has elapsed	1	5	6	Same as ID55	1	4	5	* Recommendations to improve the safety more: • Consider introducing a crew monitoring system • Consider and implement how to operate when the crew does not respond (MRM/MRC) • Workload management of the onboard crew (limiting the work they can perform)

57	Too late/too early implamentation of approving/revising of action plan	C57.1 Insufficient understanding of the operation method C57.2 HMI that makes it difficult to understand the intention of action plan and thus takes time to approve/revise the action plan C57.3 Understanding of their own ship's performance or current information on their ship/surrounding/environment, etc. takes time, and result in being late to approve/revise action plan C57.4 Failure or malfunction of the autonomous ship steering system C57.5 Takes time to release from other tasks C57.6 No notification of the need for approving action plan (and no alarm)	Same as ID1	• Preparation of manuals on how to operate the sutonomous ship steering system • Advance training of the onboard crew • Appropriate HMI design and verification • Alarm for failure or malfunction of the autonomous ship steering system • Issue of approving request in appropriate timing • Alarm when a certain amount of time has elapsed	1	5	6	• Establishment of advance training method of the onboard crew • Improving of requesting argorithm for approving of action plan	1	5	6	* Recommendations to improve the safety more: • Consider and implement how to operate when the crew does not respond after a certain period of time (MRM/MRC) • Workload management of the onboard crew (limiting the work they can perform)

58	Error in switching the steering mode	C58.1 Failure or malfunction of the ship steering mode switching function C58.2 The crew is not familiar with the procedure C58.3 Distraction due to concurrent tasks and time pressure	Same as ID49	• Preparation of manuals on how to switch the steering mode • Advance training of the onboard crew • Alarm for failure or malfunction of the autonomous ship steering system	1	6	7	Same as ID55	1	5	6	Same as ID55
59	No implementation of switching the steering mode	C59.1 Sudden illness, napping, or no crews in bridge, etc. C59.2 Insufficient understanding of the need for the ship steering mode switching operation C59.3 HMI finding it difficult to understand the ship steering mode C59.4 Failure or malfunction of the ship steering mode switching function C59.5 Ship operation mode switching instruction not activated C59.6 Forgetting due to concurrent tasks	Same as ID49	• Preparation of manuals on how to operate the sutonomous ship steering system • Advance training of the onboard crew • Appropriate HMI design and verification • Alarm for failure or malfunction of the autonomous ship steering system • Alarm when a certain amount of time has elapsed	1	5	6	Same as ID55	1	5	6	Same as ID56

60	Too late/too early to implement switching of the steering mode	C60.1 Insufficient understanding of the operation method C60.2 HMI finding it difficult to understand the necessity of switching the ship steering mode, thus taking time to switch C60.3 Failure or malfunction of the ship steering mode switching function C60.4 Too late issuance of the ship steering mode switching instruction C60.5 Lack of resources due to concurrent tasks	Same as ID49	Same as ID59	1	6	7	Same as ID55	1	5	6	Same as ID57
61	Error in emergency response (forced switchover to manual steering)	C61.1 Failure of the ship steering mode switching function C61.2 The onboard crew is not familiar with the ship steering mode switching method C61.3 Distraction due to other tasks and time pressure	Same as ID1	• Preparation of the manual on how to switch the steering mode • Advance training of the onboard crew	1	6	7	Same as ID55	1	6	7	Same as ID55

62	Failure to implement the emergency response (forced switchover to manual steering)	C62.1 Overconfidence in the autonomous ship steering system C62.2 The onboard crew does not understand that the current situation is an emergency (misperception of their own ship's performance or current information on their ship/surrounding/environment, etc.). C62.3 The onboard crew is not familiar with how to switch the ship steering mode C62.4 The onboard crew's sudden illness, napping, or engaging in other tasks, among other factors	Same as ID1	• Advance training of the onboard crew • Appropriate HMI design that the crew can understand current situations well and the verification	1	6	7	Same as ID55	1	5	6	* Recommendations to improve the safety more: • Consider introducing a crew monitoring system • Workload management for onboard crew members (limiting the work they can perform)
63	Too late/too early to implement emergency response (forced switchover to manual steering)	Same as ID61	Same as ID1	Same as ID61	1	6	7	Same as ID55	1	6	7	Same as ID55

Table 1.8 HAZID WS (Phase: Berthing/unberthing)

Sheet ID: 2
Phase: Berthing/unberthing

ID	Hazard	Causes	Consequences	Existing Safeguards	Index(only existing safeguards)			Recommendation	Index(Include safeguards recommendation)			Comments
					SI	FI	RI		SI	FI	RI	
Autonomous ship steering system												
1	Error in establishing the action plan for berthing/ unberthing	C1.1 Input information not obtained or incorrect (information on own ship, other ships and drifting objects, marine weather, target positions of berthing/ unberthing, etc.) C1.2 Voyage plan (given) not obtained or incorrect C1.3 Faulty algorithm for establishing the ship action plan for berthing/ unberthing in the autonomous ship steering system C1.4 Failure or malfunction of the autonomous ship steering system C1.5 Malware infiltration or hacking	E1.1 Abnormal approach to the berth, other ships/objects, or areas with grounding risk E1.2 Collision, contact, grounding, capsizing, and sinking	• Alarm for each system failure • Alarm when various information and voyage plans are not entered • Double-checking when entering voyage plans • Alarm when jumping position of own ship or other ships/drifts • Prior verification by simulations of berthing/ unberthing action planning algorithms • Connect only to removable media with no viruses detected by virus detection software as well as no connection to external networks • Constant monitoring by the onboard crew • forced switchover to manual steering by onboard crew	2	5	7	• Improvement of the action planning algorithm for berthing/ unberthing • Consideration of measures to improve system reliability (redundancy, etc.) (including cost–benefit study)	2	5	7	* Recommendations to improve the safety more: • Verification of outputs and introduction of functions to deal with the verification results (implemented by human or machine, depending on the level of automation)

2	No implementation of the berthing/ unberthing action plan	C2.1 Input information not obtained (information on own ship, other ships and drifting objects, marine weather, target position of berthing/ unberthing, etc.) C2.2 Voyage plan (given) not obtained C2.3 Failure or malfunction of the autonomous ship steering system C2.4 Malware intrusion or hacking C2.5 Failure to receive inquiry (trigger for activating this function)	Same as ID1	• Alarm for each system failure • Alarm when various information and voyage plans are not entered • Alarm when a certain amount of time has elapsed • Pre verification through simulations • Connect only to removable media with no viruses detected by virus detection software as well as no connection to external networks • Constant monitoring by the onboard crew • forced switchover to manual steering by onboard crew	2	4	6	Same as ID1	2	4	6	* Recommendations to improve the safety more: • If there is no response, the inquiry source shall be made to ask again with new input information. • Introduce a function to deal with no response even after re querying (implemented by human or machine, depending on the level of automation)

3	Too late/too early implementation of the berthing/ unberthing action plan	C3.1 Input information not obtained or obtained at the wrong time (information on own ship, other ships and drifting objects, marine weather, target positions of berthing/ unberthing, etc.) C3.2 Failure of the autonomous ship steering system's berthing/ unberthing action planning algorithm (too much time is spent on calculations for berthing/ unberthing action planning) C3.3 Failure or malfunction of the autonomous ship steering system C3.4 Malware infiltration or hacking C3.5 Wrong timing of inquiry (trigger for activation of this function)	Same as ID1	Same as ID2	2	5	7	Same as ID1	2	5	7	* Recommendations to improve the safety more: • If the response is too late, the inquiry source shall be made to ask again with new input information. • Introduce a function to deal with cases where a response is not received in time (implemented by human or machine, depending on the level of automation)

4	Error in the switching operation phase (unberthing phase to normal navigation phase)	C4.1 Incorrect input of the (given) position to switch the operation phase C4.2 Incorrect input information (own ship's position information) C4.3 Failure or malfunction of the autonomous ship steering system C4.4 Malware intrusion or hacking	E4.1 Deviation from course E4.2 Abnormal approach to other ships/objects, berth, or areas with grounding risk E4.3 Collision with other ships or berth, grounding, and capsizing or sinking	• Alarm for each system failure • Double check when inputting the operation phase switching position • Alarm at the time of position jump of own ship • Alarm at the time of route deviation • Pre verification through simulations • Connect only to removable media with no viruses detected by virus detection software as well as no connection to external networks • Constant monitoring by the onboard crew • forced switchover to manual steering by onboard crew	2	5	7	• Consideration of measures to improve system reliability (redundancy, etc.) (including cost–benefit study)	2	5	7	

5	No changeover of the operation phase (unberthing phase to normal navigation phase)	C5.1 Incorrect input of the (given) position to switch the operation phase C5.2 Incorrect input or no input of input information (own ship's position information) C5.3 Failure or malfunction of the autonomous ship steering system C5.4 Malware intrusion or hacking C5.5 Failure to receive inquiry (trigger for activating this function)	Same as ID4	• Alarm for each system failure • Alarm if operation phase switching position or own position are not entered • Alarm at the time of position jump of own ship • Alarm at the time of route deviation • Pre verification through simulations • Activate alarm when a certain distance from the operation phase switching position is exceeded • Connect only to removable media with no viruses detected by virus detection software as well as no connection to external networks • Constant monitoring by the onboard crew • forced switchover to manual steering by onboard crew	2	4	6	Same as ID4	2	4	6	Same as ID2

6	Too late/too early to implement switching the operation phases (unberthing phase to normal navigation phase)	C6.1 Wrong timing of obtaining input information (own ship's position) C6.2 Malfunction of the operation phase switching algorithm (switching operation takes too long) C6.3 Failure or malfunction of the autonomous ship steering system C6.4 Malware intrusion or hacking C6.5 Wrong timing of inquiry (trigger for activating this function)	Same as ID4	• System failure alarm • Alarm at the time of route deviation • Pre verification through simulations • Activate alarm when a certain distance from the operation phase switching position is exceeded • Connect only to removable media with no viruses detected by virus detection software as well as no connection to external networks • Constant monitoring by the onboard crew • forced switchover to manual steering by onboard crew	2	5	7	Same as ID4	2	5	7	Same as ID3
7	Error in diagnosis of own status	C7.1 Wrong algorithm for the self-diagnostic function of the autonomous ship steering system C7.2 Incorrect input information (information required for self-diagnosis) C7.3 Malware intrusion or hacking	• Misdiagnose as normal when abnormal → Same as ID4 • Misdiagnose as abnormal when normal → Switch to manual steering based on alarm	• Pre verification of the self-diagnostic function • Connect only to removable media with no viruses detected by virus detection software as well as no connection to external networks • Constant monitoring by the onboard crew • forced switchover to manual steering by onboard crew	2	5	7	Same as ID4	2	5	7	

8	No implementation of the diagnosis of own ship's status	C8.1 Failure, malfunction, or stoppage of the self-diagnostic function of the autonomous ship steering system C8.2 Input information (information necessary for self-diagnosis) not obtained C8.3 Malware intrusion or hacking	E8.1 Difficult to judge wheter autonomous operation is being conducted appropriately • Diagnosis not performed when normal → No problem (alarm will be activated when a certain period of time is exceeded) • Diagnosis not performed when abnormal → Same as ID4	• Pre verification of the self-diagnostic function • Alarm activated when a certain amount of time is exceeded • Connect only to removable media with no viruses detected by virus detection software as well as no connection to external networks • Constant monitoring by the onboard crew • forced switchover to manual steering by onboard crew	2	4	6	Same as ID4	2	4	6	

9	Too late/too early to implement the diagnosis of own status	C9.1 Failure or malfunction of the self-diagnostic function of the autonomous ship steering system C9.2 Malfunction of the self-diagnostic algorithm of the autonomous ship steering system (self-diagnostic operation takes too much time) C9.3 Incorrect timing for obtaining input information (information necessary for self-diagnosis) C9.4 Malware intrusion or hacking	• Too late to diagnose when normal → No problem (alarm will be activated when a certain period of time is exceeded) • Too late to diagnose as abnormal when abnormal → E9.1 Delay in switching to the manual operation E9.2 Autonomous operation outside ODD E9.3 Route deviation E9.4 Abnormal approach to berth, other ships/objects, or areas with grounding risk E9.5 Collision, contact, grounding, capsizing, or sinking	Same as ID8	2	5	7	Same as ID4	2	5	7	
Information integration system for own ship												

10	Error in integration of own ship information	C10.1 Inconsistency in input information (e.g., different data between sensors of own ship, integration with old information, etc.) C10.2 Failure or malfunction of the information integration function and, error in the integration algorithm C10.3 Malware intrusion or hacking	E10.1 Establishment of the incorrect action plan for berthing/ unberthing E10.2 Incorrect calculation of the control variables E10.3 Incorrect/no switching of the operation phase E10.4 Deviation from course E10.5 Abnormal approach to other ships/objects, berth, or areas with grounding risk E10.6 Collision, grounding, capsizing, or sinking	• Advance verification of the information integration function • Integrating a method for dealing with discrepancies in data (which data should be prioritized) • Alarm for each system failure • Warnings when the same type of data differs • Connect only to removable media with no viruses detected by virus detection software as well as no connection to external networks • Constant monitoring by the onboard crew • forced switchover to manual steering by onboard crew	2	4	6	• Consideration of measures to improve system reliability (redundancy, etc.) (including cost–benefit study) • Improvement of the information integration algorithm	2	4	6	* Recommendations to improve the safety more: • Management of the reliability of integrated information (reliability evaluation and formulation of countermeasures in case of low reliability)

11	No implementation of integrating information of own ship	C11.1 Inconsistency in input information (different data between sensors of own ship) C11.2 Failure or malfunction of the information integration function and error in the integration algorithm C11.3 Malware intrusion or hacking C11.4 Failure to receive inquiry (trigger for activating this function)	Same as ID10	• Advance verification of the information integration function • Incorporating a method for dealing with discrepancies in data (which data should be prioritized) • Alarm for each system failure • Warnings when the same type of data differs • Alarm activated when a certain amount of time is exceeded • Connect only to removable media with no viruses detected by virus detection software as well as no connection to external networks	2	4	6	Same as ID10	2	4	6	* Recommendations to improve the safety more: • Introduce a function to deal with the absence of outputs (e.g., restarting the system in question; prepared separately from diagnosis of own to deal with the case of a stoppage of functionality)

12	Too late/too early to implement integrating own ship information	C12.1 Malfunction of the information integration function/algorithm (information integration takes too much time) C12.2 Wrong timing of information acquisition from different sensors C12.3 Malware intrusion or hacking C12.4 Wrong timing of inquiry (trigger for activating this function)	E12.1 Establishment of the incorrect action plan for beathing/ unberthing E12.2 Incorrect calculation of the control variables E12.3 Switch the operation phase at wrong position E12.4 Deviation from course E12.5 Abnormal approach to other ships/objects, berth, or areas with grounding risk E12.6 Collision, grounding, capsizing, or sinking	Same as ID11	2	4	6	Same as ID10	2	4	6	* Recommendations to improve the safety more: • Introduce a function to deal with large delays in output (e.g., restarting the system in question).

13	Error in the diagnosis of own status	C13.1 Failure or malfunction of the self-diagnostic function C13.2 Wrong algorithm for the self-diagnostic function C13.3 Incorrect input information (information required for self-diagnosis) C13.4 Malware intrusion or hacking	Same as ID7	Same as ID7	2	5	7	• Improvements in algorithm for self-diagnostic function	2	5	7	
14	No implementation of the diagnosis of own status	C14.1 Failure, malfunction, or stoppage of the self-diagnostic function C14.2 Input information (information necessary for self-diagnosis) not obtained C14.3 Malware intrusion or hacking	Same as ID8	Same as ID8	2	4	6	Same as ID13	2	4	6	

15	Too late/too early to implement the diagnosis of own status	C15.1 Failure or malfunction of the self-diagnostic function C15.2 Malfunction of the self-diagnostic algorithm (self-diagnostic operation takes too much time) C15.3 Incorrect timing for obtaining input information (information required for self-diagnosis) C15.4 Malware intrusion or hacking	Same as ID9	Same as ID9	2	5	7	Same as ID13	2	5	7	
16	Error in diagnosing sensor status	C16.1 Failure or malfunction of the status diagnostic function for the sensor C16.2 Wrong algorithm for the status diagnostic function for the sensors of own ship C16.3 Incorrect input information (information required for sensor status diagnosis) C16.4 Malware intrusion or hacking	• Misdiagnose as normal when abnormal → Same as ID10 • Misdiagnose as abnormal when normal → Switch to manual steering based on alarm	• Pre verification of the status diagnostic function and algorithm for the sensor • Connect only to removable media with no viruses detected by virus detection software as well as no connection to external networks	2	5	7	• Improvements in algorithm for the diagnostic function of the sensor status	2	5	7	

17	No implementation of the diagnosis of sensor status	C17.1 Failure or malfunction of the status diagnostic function for the sensors of own ship C17.2 Input information (information necessary for sensor status diagnosis) not obtained C17.3 Malware intrusion or hacking	• Diagnosis not performed when abnormal → Same as ID10 • Diagnosis not performed when normal → No problem (alarm will be activated when a certain period of time is exceeded)	• Pre verification of the status diagnostic function for the sensors • Alarm activated when a certain amount of time is exceeded • Connect only to removable media with no viruses detected by virus detection software as well as no connection to external networks	2	4	6	Same as ID16	2	4	6	
18	Too late/too early to implement the diagnosis of sensor status	C18.1 Failure or malfunction of the status diagnostic function for the sensors of own ship C18.2 Malfunction of the sensor status diagnosis algorithm (status diagnosis operation takes too much time) C18.3 Wrong timing of obtaining input information (information required for sensor status diagnosis) C18.4 Malware intrusion or hacking	• Too late to diagnose as normal when normal → No problem (alarm will be activated when a certain period of time is exceeded) • Too late to diagnose as abnormal when abnormal → Same as ID12	• Pre verification of the status diagnostic function and algorithm for the sensors • Alarm activated when a certain amount of time is exceeded • Connect only to removable media with no viruses detected by virus detection software as well as no connection to external networks	2	5	7	Same as ID16	2	5	7	

Measuring system for the distance from the berth												
19	Error in measuring the distance to the berth from own ship	C19.1 Failure or malfunction of the sensors for measuring the distance to the berth C19.2 Failure or malfunction of the system for measuring the distance to the berth C19.3 Communication failure or malfunction between the distance sensor and the measurement system C19.4 Malware intrusion or hacking	E19.1 Abnormal approach to the berth E19.2 Collision with the berth	• Alarm for each system failure • Connect only to removable media with no viruses detected by virus detection software as well as no connection to external networks • Constant monitoring by the onboard crew • forced switchover to manual steering by onboard crew	2	4	6	• Consideration of measures to improve system reliability (redundancy, etc.) (including cost–benefit study)	2	4	6	
20	No implementation of measuring the distance to the berth	Same as ID19	Same as ID19	Same as ID19	2	4	6	Same as ID19	2	4	6	

21	Too late/too early to implement the measurement of the distance to the berth	Same as ID19	Same as ID19	Same as ID19	2	5	7	Same as ID19	2	5	7	
22	Error in activating the close-proximity alarm	C22.1 Failure or malfunction of the system for measuring the distance to the berth C22.2 Error in the alarm activating algorithm of the system for measuring the distance to the berth C22.3 Wrong input information (information necessary for alarm activating decisions) C22.4 Malware intrusion or hacking	E22.1 Alarm activated but not actually close (see ID 23 and 24 when alarm not activated but the berth is actually close)	Same as ID19	2	4	6	Same as ID19	2	4	6	

23	No implementation of activating close-proximity alarm	Same as ID22	(Alarm not activated but the berth is actually close) E23.1 Delay or failure in switching the ship steering mode E23.2 Abnormal approach to the berth E23.3 Collision with the berth	Same as ID19	2	4	6	Same as ID19	2	4	6	

24	Too late/too early to activate close-proximity alarm	C24.1 Failure or malfunction of the system for measuring the distance to the berth C24.2 Malfunction of the alarm activating algorithm for measuring the distance to the berth (calculating the decision to activate the alarm takes too much time) C24.3 Wrong timing of obtaining input information (information required to make alarm activating decision) C24.4 Malware intrusion or hacking	(Alarm delayed when the berth is actually close) E24.1 Delay or failure in switching the ship steering mode E24.2 Abnormal approach to the berth E24.3 Collision with the berth	• Verification of appropriate timing for activating the alarm • Alarm for each system failure • Connect only to removable media with no viruses detected by virus detection software as well as no connection to external networks • Constant monitoring by the onboard crew • forced switchover to manual steering by onboard crew	2	4	6	Same as ID19	2	4	6	
25	Error in diagnosis of own status	C25.1 Failure or malfunction of the self-diagnostic function C25.2 Wrong algorithm for the self-diagnostic function C25.3 Incorrect input information (information required for self-diagnosis) C25.4 Malware intrusion or hacking	Same as ID7	Same as ID7	2	5	7	Same as ID13	2	5	7	

26	No implementation of diagnosis of own status	C26.1 Failure or malfunction of the self-diagnostic function C26.2 Input information (information necessary for self-diagnosis) not obtained C26.3 Malware intrusion or hacking	Same as ID8	Same as ID8	2	4	6	Same as ID13	2	4	6	
27	Too late/too early to implement diagnosis of own status	C27.1 Failure or malfunction of the self-diagnostic C27.2 Malfunction of the self-diagnostic algorithm of the system (self-diagnostic operation takes too much time) C27.3 Incorrect timing of obtaining input information (information required for self-diagnosis) C27.4 Malware intrusion or hacking	Same as ID9	Same as ID9	2	5	7	Same as ID13	2	5	7	

28	Error in diagnosing sensor status	C28.1 Wrong algorithm for the status diagnostic function for the sensors C28.2 Incorrect input information (information required for sensor status diagnosis) C28.3 Malware intrusion or hacking	• Misdiagnose as normal when abnormal →Same as ID19 • Misdiagnose as abnormal when normal →Switch to manual steering based on alarm	Same as ID16	2	5	7	Same as ID16	2	5	7	
29	No implementation of diagnosis of sensor status	C29.1 Failure of the status diagnostic function for the sensors C29.2 Input information (information required for sensor status diagnosis) not obtained C29.3 Malware intrusion or hacking	• Diagnosis not performed when abnormal → Same as ID19 • Diagnosis not performed when normal → No problem (alarm will be activated when a certain period of time is exceeded)	Same as ID17	2	4	6	Same as ID16	2	4	6	

30	Too late/too early to implement diagnosis of sensor status	C30.1 Failure or malfunction of the status diagnostic function for the sensors C30.2 Malfunction of the sensor status diagnosis algorithm of the system (status diagnosis operation takes too much time) C30.3 Wrong timing of obtaining input information (information required for sensor status diagnosis) C30.4 Malware intrusion or hacking	• Too late diagnosis as normal when normal → No problem (alarm will be activated when a certain period of time is exceeded) • Too late diagnosis as abnormal when abnormal → Same as ID19	Same as ID18	2	5	7	Same as ID16	2	5	7	
Information integration system for other ships and drifting objects												

31	Error in integration information of other ships and drifting objects	C31.1 Inconsistency in input information (e.g., different data between sensors, integration with old information) C31.2 Failure or malfunction of the information integration function as well as errors in the integration algorithm C31.3 Malware intrusion or hacking	E31.1 Establishment of the incorrect action plan berthing/ unberthing. E31.2 Abnormal approach to other ships/objects or areas with grounding risk E31.3 Collision, grounding, capsizing, or sinking	Same as ID10	2	4	6	Same as ID10	2	4	6	Same as ID10
32	No implementation of integration information of other ships and drifting objects	C32.1 Inconsistency in input information (e.g., different data between sensors) C32.2 Failure or malfunction of the information integration function as well as errors in the integration algorithm C32.3 Malware intrusion or hacking C32.4 Failure to receive inquiry (trigger for activating this function)	Same as ID31	Same as ID11	2	4	6	Same as ID10	2	4	6	Same as ID11

33	Too late/too early implementation of integration information of other ships and drifting objects	C33.1 Failure of information integration function/algorithm (information integration takes too much time) C33.2 Wrong timing of information acquisition from different sensors C33.3 Malware intrusion or hacking C33.4 Wrong timing of inquiry (trigger for activation of this function)	Same as ID31	Same as ID10	2	4	6	Same as ID10	2	4	6	Same as ID12
34	Error in diagnosing own status	C34.1 Failure or malfunction of the self-diagnostic function C34.2 Wrong algorithm for the self-diagnostic function C34.3 Incorrect input information (information necessary for self-diagnosis) C34.4 Malware intrusion or hacking	Same as ID7	Same as ID7	2	5	7	Same as ID13	2	5	7	

35	No implementation of diagnosing own status	C35.1 Failure or malfunction of the self-diagnostic function C35.2 Input information (information necessary for self-diagnosis) not obtained C35.3 Malware intrusion or hacking	Same as ID8	Same as ID8	2	4	6	Same as ID13	2	4	6	
36	Too late/too early implementation of diagnosing own status	C36.1 Failure or malfunction of the self-diagnostic function C36.2 Malfunction of the self-diagnostic algorithm (self-diagnostic operation takes too much time) C36.3 Wrong timing of obtaining input information (information required for self-diagnosis) C36.4 Malware intrusion or hacking	Same as ID9	Same as ID9	2	5	7	Same as ID13	2	5	7	

37	Error in diagnosing sensor status	C37.1 Failure or malfunction of the status diagnostic function for the sensors C37.2 Wrong algorithm for the status diagnostic function for the sensors C37.3 Incorrect input information (information necessary for sensor status diagnosis) C37.4 Malware intrusion or hacking	• Misdiagnose as normal when abnormal → Same as ID31 • Misdiagnose as abnormal when normal → Switch to manual steering based on alarm	Same as ID16	2	5	7	Same as ID16	2	5	7	
38	No implementation of diagnosing sensor status	C38.1 Failure or malfunction of the status diagnostic function for the sensors C38.2 Input information (information necessary for sensor status diagnosis) not obtained C38.3 Malware intrusion or hacking	• Diagnosis not performed when abnormal → Same as ID31 • Diagnosis not performed when normal → No problem (alarm will be activated when a certain period of time is exceeded)	Same as ID17	2	4	6	Same as ID16	2	4	6	

39	Too late/too early implementation of diagnosing sensor status	C39.1 Failure or malfunction of the status diagnostic function for the sensors C39.2 Malfunction of the algorithm for the sensor status diagnosis (status diagnosis operation takes too much time) C39.3 Wrong timing of obtaining input information (information required for sensor status diagnosis) C39.4 Malware intrusion or hacking	• Too late diagnosis as normal when normal → No problem (alarm will be activated when a certain period of time is exceeded) • Too late diagnosis as abnormal when abnormal → Same as ID31	Same as ID18	2	5	7	Same as ID16	2	5	7	
Information integration system for marine weather												
40	Error in integration of marine weather information	C40.1 Inconsistency in input information (e.g., different data between sensors, integration with old information) C40.2 Failure or malfunction of the information integration function as well as error in integration algorithm C40.3 Malware intrusion or hacking	Same as ID31	Same as ID10	2	4	6	Same as ID10	2	4	6	Same as ID10

41	No implementation of integrating marine weather information	C41.1 Inconsistency in input information (e.g., different data between sensors) C41.2 Failure or malfunction of the information integration function as well as error in integration algorithm C41.3 Malware intrusion or hacking C41.4 Failure to receive inquiry (trigger for activating this function)	Same as ID31	Same as ID11	2	4	6	Same as ID10	2	4	6	Same as ID11
42	Too late/too early implementation of integrating marine weather information	C42.1 Failure or malfunction of the information integration function/algorithm (information integration takes too much time) C42.2 Wrong timing of information acquisition from different sensors C42.3 Malware intrusion or hacking C42.4 Wrong timing of inquiry (trigger for activation of this function)	Same as ID31	Same as ID11	2	4	6	Same as ID10	2	4	6	Same as ID12

43	Error in diagnosing own status	C43.1 Failure or malfunction of the self-diagnostic function C43.2 Wrong algorithm for the self-diagnostic function C43.3 Incorrect input information (information necessary for self-diagnosis) C43.4 Malware intrusion or hacking	Same as ID7	Same as ID7	2	5	7	Same as ID13	2	5	7	
44	No implementation of diagnosing own status	C44.1 Failure or malfunction of the self-diagnostic function C44.2 Input information (information necessary for self-diagnosis) not obtained C44.3 Malware intrusion or hacking	Same as ID8	Same as ID8	2	4	6	Same as ID13	2	4	6	

45	Too late/too early implementation of diagnosing own status	C45.1 Failure or malfunction of the self-diagnostic function C45.2 Malfunction of the self-diagnostic algorithm (self-diagnostic operation takes too much time) C45.3 Wrong timing of obtaining input information (information required for self-diagnosis) C45.4 Malware intrusion or hacking	Same as ID9	Same as ID9	2	5	7	Same as ID13	2	5	7	
46	Error in diagnosing sensor status	C46.1 Failure or malfunction of the status diagnostic function for the sensors C46.2 Wrong algorithm for the status diagnostic function for the sensors C46.3 Incorrect input information (information necessary for sensor status diagnosis) C46.4 Malware intrusion or hacking	• Misdiagnose as normal when abnormal → Same as ID31 • Misdiagnose as abnormal when normal → Switch to manual steering based on alarm	Same as ID16	2	5	7	Same as ID16	2	5	7	

47	No implementation of diagnosing sensor status	C47.1 Failure or malfunction of the status diagnostic function for the sensors C47.2 Input information (information necessary for sensor status diagnosis) not obtained C47.3 Malware intrusion or hacking	• Diagnosis not performed when abnormal → Same as ID31 • Diagnosis not performed when normal → No problem (alarm will be activated when a certain period of time is exceeded)	Same as ID17	2	4	6	Same as ID16	2	4	6	
48	Too late/too early implementation of diagnosing sensor status	C48.1 Failure or malfunction of the status diagnostic function for the sensors C48.2 Malfunction of the algorithm for the sensor status diagnosis (status diagnosis operation takes too much time) C48.3 Wrong timing of obtaining input information (information required for sensor status diagnosis) C48.4 Malware intrusion or hacking	• Too late diagnosis as normal when normal → No problem (alarm will be activated when a certain period of time is exceeded) • Too late diagnosis as abnormal when abnormal → Same as ID31	Same as ID18	2	5	7	Same as ID16	2	5	7	
Ship control system												

49	Error in calculation of the control variables based on the action plan for berthing/ unberthing	C49.1 Error in the action plan for berthing/ unberthing C49.2 Incorrect input information (information required for control variables calculation) C49.3 Error in the control variables calculation algorithm C49.3-2 Poor accuracy of the steering motion model of own ship C49.4 Failure or malfunction of the ship control system C49.5 Malware intrusion or hacking	E49.1 Deviation from course E49.2 Abnormal approach to other ships/objects or areas with grounding risk E49.3 Collision, grounding, capsizing, or sinking	• System failure alarm • Pre verification of the control variables calculation algorithm through simulations • Connect only to removable media with no viruses detected by virus detection software as well as no connection to external networks • Constant monitoring by the onboard crew • forced switchover to manual steering by onboard crew	2	5	7	• Improvement of the control variables calculation algorithm • Ensure accuracy of the steering motion model of own ship • Consideration of measures to improve system reliability (redundancy, etc.) (including cost–benefit study)	2	5	7	

50	No implementation of calculating the control variables based on the action plan for berthing/ unberthing	C50.1 Action plan for berthing/ unberthing not obtained C50.2 Input information (information required for control variables calculation) not obtained C50.3 Failure or malfunction of the ship control system C50.4 Malware intrusion or hacking C50.5 Failure to receive inquiry (trigger for activating this function)	Same as ID49	• System failure alarm • Alarm at the time when various information is not obtained • Pre verification through simulations • Alarm activated when a certain amount of time is exceeded • Connect only to removable media with no viruses detected by virus detection software as well as no connection to external networks • Constant monitoring by the onboard crew • forced switchover to manual steering by onboard crew	2	4	6	• Consideration of measures to improve system reliability (redundancy, etc.) (including cost–benefit study)	2	4	6	* Recommendations to improve the safety more: • Introduction of mechanisms to verify ship behavior (e.g., watch for berthing speed) • If there is no response, the inquiry source shall be made to ask again with new input information. • Introduce a function to deal with no response even after re querying (implemented by human or machine, depending on the level of automation)

51	Too late/too early to implement control variables calculations based on the action plan for berthing/ unberthing	C51.1 Wrong timing of obtaining the action plan for berthing/ unberthing C51.2 Wrong timing of acquiring input information (information required for control variables calculation) C51.3 Malfunction in the control variables calculation algorithm (excessive time required for control variables calculation) C51.4 Failure or malfunction in the ship control system C51.5 Malware intrusion C51.6 Wrong timing of inquiry (trigger for activation of this function)	Same as ID49	• System failure alarm • Pre verification through simulations • Warning activated when a certain period of time has elapsed • Alarm activated when a certain amount of time is exceeded • Connect only to removable media with no viruses detected by virus detection software as well as no connection to external networks	2	5	7	Same as ID50	2	5	7	* Recommendations to improve the safety more: • Introduction of mechanisms to verify behavior (e.g., watch for berthing speed) • If the response is too late, the inquiry source shall be made to ask again with new input information. • Introduce a function to deal with cases where a response is not received in time (implemented by human or machine, depending on the level of automation)

52	Error in control of the rudder or engine	C52.1 Error in control variables calculation C52.2 Actuator malfunction or failure	E52.1 Unable to navigate E52.2 Deviation from course E52.3 Abnormal approach to other ships/objects, or areas with grounding risk E52.4 Collision, grounding, capsizing, or sinking	• Pre verification of the system • Alarms in case of actuator failure or malfunction • Constant monitoring by the onboard crew • forced switchover to manual steering by onboard crew	2	4	6	• Consideration of measures to improve system reliability (redundancy, etc.) (including cost–benefit study)	2	4	6	* Recommendations to improve the safety more: • Introduction of a function to deal with incorrect rudder/engine status (e.g., restarting the system in question)

53	No implementation of control of the rudder or engine	C53.1 Input information (control variables) not obtained C53.2 Malfunction or failure of the actuator C53.3 Failure to receive inquiry (trigger for activating this function)	Same as ID52	• Alarms in case of actuator failure or malfunction • Alarm when control variables not obtained • Alarm activated when a certain amount of time is exceeded • Constant monitoring by the onboard crew • forced switchover to manual steering by onboard crew	2	4	6	Same as ID52	2	4	6	* Recommendations to improve the safety more: • Introduction of a function to deal with cases where the rudder/engine is not under control (e.g., restarting the system in question) • If there is no response, the inquiry source shall be made to ask again with new input information. • Introduce a function to deal with no response even after re querying (implemented by human or machine, depending on the level of automation)

54	Too late/too early to implement controlling the rudder or engine	C54.1 Wrong timing of obtaining input information (control variables) C54.2 Malfunction or failure of the actuator C54.3 Wrong timing of inquiry (trigger for activation of this function)	Same as ID52	Same as ID53	2	5	7	Same as ID52	2	5	7	* Recommendations to improve the safety more: • Introduction of a function to deal with rudder/engine control delays exceeding a certain level (e.g., restarting the system in question). • If the response is too late, the inquiry source shall be made to ask again with new input information. • Introduce a function to deal with cases where a response is not received in time (implemented by human or machine, depending on the level of automation)

55	Error in diagnosis of rudder/engine conditions	C55.1 Failure or malfunction of the rudder/engine condition diagnostic function C55.2 Wrong algorithm for the rudder/engine condition diagnostic function C55.3 Incorrect input information (information required for rudder/engine condition diagnosis) C55.4 Malware intrusion or hacking	Same as ID7	Same as ID7	2	5	7	• Improved algorithms for rudder/engine condition diagnostic functions	2	5	7	
56	No implementation of diagnosis of rudder/engine conditions	C56.1 Failure or malfunction of the rudder/engine condition diagnostic function C56.2 Input information (information required for rudder/engine condition diagnosis) not obtained C56.3 Malware intrusion or hacking	Same as ID8	Same as ID8	2	4	6	Same as ID55	2	4	6	

57	Too late/too early to implement diagnosis of rudder/engine conditions	C57.1 Failure or malfunction of the rudder/engine condition diagnostic function C57.2 Malfunction of the rudder/engine condition diagnostic algorithm (self-diagnostic operation takes too much time) C57.3 Wrong timing of obtaining input information (information required for rudder/engine condition diagnosis) C57.4 Malware intrusion or hacking	Same as ID9	Same as ID9	2	5	7	Same as ID55	2	5	7	
58	Error in diagnosing own status	C58.1 Failure or malfunction of the self-diagnostic function C58.2 Wrong algorithm for the self-diagnostic function C58.3 Incorrect input information (information required for self-diagnosis) C58.4 Malware intrusion or hacking	Same as ID7	Same as ID7	2	5	7	Same as ID13	2	5	7	

59	No implementation of diagnosing own status	C59.1 Failure, malfunction, or stoppage of the self-diagnostic function C59.2 Input information (information necessary for self-diagnosis) not obtained C59.3 Malware intrusion or hacking	Same as ID8	Same as ID8	2	4	6	Same as ID13	2	4	6	
60	Too late/too early implementation of diagnosing own status	C60.1 Failure or malfunction of the self-diagnostic function C60.2 Malfunction of the self-diagnostic algorithm (self-diagnostic operation takes too much time) C60.3 Incorrect timing of obtaining input information (information required for self-diagnosis) C60.4 Malware intrusion or hacking	Same as ID9	Same as ID9	2	5	7	Same as ID13	2	5	7	
Autonomous Operation Management System												

61	Error in instructions for switching the ship steering mode	C61.1 Failure or malfunction of the autonomous operation management system C61.2 Error in the algorithm to switch the operation mode C61.3 Error in input information (information required for making the operation mode switching decision) C61.4 Malware intrusion or hacking	E61.1 Autonomous steering for berthing/ unberthing outside ODD E61.2 Deviation from course E61.3 Abnormal approach to other ships/objects or areas with grounding risk E61.4 Collision, stranding, capsizing or sinking	• Alarm for each system failure • Double-checking at the time of ODD input • Alarm at the time of route deviation • Prior verification of the instruction function to switch the ship steering mode through simulations • Connect only to removable media with no viruses detected by virus detection software as well as no connection to external networks • Constant monitoring by the onboard crew • forced switchover to manual steering by onboard crew	2	5	7	• Improvement of the ship steering mode switching algorithm • Consideration of measures to improve system reliability (redundancy, etc.) (including cost–benefit study)	2	5	7	

62	No implementation of the ship steering mode switching instructions	C62.1 Failure or malfunction of the autonomous operation management system C62.2 Error in the algorithm to switch the operation mode C62.3 Error in input information (information required for making the operation mode switching decision) C62.4 Malware intrusion or hacking C62.5 Failure to receive inquiry (trigger for activating this function)	Same as ID61	• Alarm for each system failure • Alarm activated when a certain amount of time is exceeded • Double-checking at the time of ODD input • Alarm at the time of route deviation • Prior verification of the instruction function to switch the ship steering mode through simulations • Connect only to removable media with no viruses detected by virus detection software as well as no connection to external networks	2	4	6	Same as ID61	2	4	6	Same as ID2

63	Too late/too early to give the ship steering mode switching instructions	C63.1 Failure or malfunction of the autonomous operation management system C63.2 Malfunction of the algorithm to switch the operation mode (calculating the decision to switch the operation mode takes too much time) C63.3 Wrong timing of obtaining input information (information necessary to decide whether to switch the operation mode) C63.4 Malware infiltration or hacking C63.5 Wrong timing of inquiry (trigger for activation of this function)	Same as ID61	Same as ID62	2	5	7	Same as ID61	2	5	7	Same as ID3

64	Error in diagnosing own status	C64.1 Failure or malfunction of the self-diagnostic function C64.2 Wrong algorithm for the self-diagnostic function C64.3 Incorrect input information (information required for self-diagnosis) C64.4 Malware intrusion or hacking	Same as ID7	Same as ID7	2	5	7	Same as ID13	2	5	7	
65	No implementation of diagnosing own status	C65.1 Failure, malfunction, or stoppage of the self-diagnostic function C65.2 Input information (information necessary for self-diagnosis) not obtained C65.3 Malware intrusion or hacking	Same as ID8	Same as ID8	2	4	6	Same as ID13	2	4	6	

66	Too late/too early implementation of diagnosing own status	C66.1 Failure or malfunction of the self-diagnostic function C66.2 Malfunction of the self-diagnostic algorithm (self-diagnostic operation takes too much time) C66.3 Incorrect timing of obtaining input information (information required for self-diagnosis) C66.4 Malware intrusion or hacking	Same as ID9	Same as ID9	2	5	7	Same as ID13	2	5	7	
Onboard crew												

67	Error in approving /revising of action plan for berthing/unberthing	C67.1 Overconfidence in the autonomous ship steering system C67.2 Insufficient understanding of the operation method C67.3 HMI that makes it difficult to understand the intention of action plan for berthing/unberthing C67.4 Misperception of their own ship's performance or current information on their ship/surrounding/environment, etc. C67.5 Failure or malfunction of the autonomous ship steering system C67.6 Operation mistake C67.7 Distraction due to concurrent tasks and time pressure	Same as ID1	• Preparation of manuals on how to operate the sutonomous ship steering system • Advance training of the onboard crew • Appropriate HMI design and verification • Alarm for failure or malfunction of the autonomous ship steering system • Setting confirmation notification	2	5	7	• Establishment of advance training method of the onboard crew	2	4	6	* Recommendations to improve the safety more: • Workload management of the onboard crew (ensuring the enough number of the onboard crews for the amount of tasks and replenishing resources by introducing available automation)

68	No implamentation of approving/revising of action plan for berthing/unberthing	C68.1 Sudden illness, napping, or no crews in bridge, etc. C68.2 Insufficient understanding of the need for the approving/revising of action plan for berthing/unberthing C68.3 HMI that makes it difficult to understand the need for the approving/revising of action plan for berthing/unberthing C68.4 Failure or malfunction of the autonomous ship steering system C68.5 Operation mistake C68.6 Restraint by other tasks C68.7 No notification of the need for approving action plan (and no alarm)	Same as ID1	• Preparation of manuals on how to operate the sutonomous ship steering system • Advance training of the onboard crew • Appropriate HMI design and verification • Alarm for failure or malfunction of the autonomous ship steering system • Setting confirmation notification • Alarm when a certain amount of time has elapsed	2	4	6	Same as ID67	2	4	6	* Recommendations to improve the safety more: • Consider introducing a crew monitoring system • Consider and implement how to operate when the crew does not respond (MRM/MRC) • Workload management of the onboard crew (limiting the work they can perform)

69	Too late/too early implamentation of approving/revising of action plan for berthing/unberthing	C69.1 Insufficient understanding of the operation method C69.2 HMI that makes it difficult to understand the intention of action plan and thus takes time to approve/revise the action plan for berhing/unberthing C69.3 Understanding of their own ship's performance or current information on their ship/surrounding/environment, etc. takes time, and result in being late to approve/revise action plan C69.4 Failure or malfunction of the autonomous ship steering system C69.5 Takes time to release from other tasks C69.6 No notification of the need for approving action plan (and no alarm)	Same as ID1	• Preparation of manuals on how to operate the sutonomous ship steering system • Advance training of the onboard crew • Appropriate HMI design and verification • Alarm for failure or malfunction of the autonomous ship steering system • Issue of approving request in appropriate timing • Alarm when a certain amount of time has elapsed	2	5	7	• Establishment of advance training method of the onboard crew • Improving of requesting argorithm for approving of action plan for berthing/unberthing	2	5	7	* Recommendations to improve the safety more: • Consider and implement how to operate when the crew does not respond after a certain period of time (MRM/MRC) • Workload management of the onboard crew (limiting the work they can perform)

70	Error in switching the steering mode	C70.1 Failure or malfunction of the ship steering mode switching function C70.2 The crew is not familiar with the procedure C70.3 Distraction due to concurrent tasks and time pressure	Same as ID61	• Preparation of manuals on how to switch the steering mode • Advance training of the onboard crew • Alarm for failure or malfunction of the autonomous ship steering system	2	5	7	Same as ID67	2	5	7	Same as ID67
71	No implementation of switching the steering mode	C71.1 Sudden illness, napping, or no crews in bridge, etc. C71.2 Insufficient understanding of the need for the ship steering mode switching operation C71.3 HMI finding it difficult to understand the ship steering mode C71.4 Failure or malfunction of the ship steering mode switching function C71.5 Ship operation mode switching instruction not activated C71.6 Forgetting due to concurrent tasks	Same as ID61	• Preparation of manuals on how to operate the sutonomous ship steering system • Advance training of the onboard crew • Appropriate HMI design and verification • Alarm for failure or malfunction of the autonomous ship steering system • Alarm when a certain amount of time has elapsed	2	5	7	Same as ID67	2	4	6	Same as ID68

72	Too late/too early to implement switching of the steering mode	C72.1 Insufficient understanding of the operation method C72.2 HMI finding it difficult to understand the necessity of switching the ship steering mode, thus taking time to switch C72.3 Failure or malfunction of the ship steering mode switching function C72.4 Too late issuance of the ship steering mode switching instruction C72.5 Lack of resources due to concurrent tasks	Same as ID61	Same as ID71	2	5	7	Same as ID67	2	5	7	Same as ID69
73	Error in emergency response (forced switchover to manual steering)	C73.1 Failure of the ship steering mode switching function C73.2 The onboard crew is not familiar with the ship steering mode switching method C73.3 Distraction due to other tasks and time pressure	Same as ID1	• Preparation of the manual on how to switch the steering mode • Advance training of the onboard crew	2	6	8	Same as ID67	2	5	7	Same as ID67

74	Failure to implement the emergency response (forced switchover to manual steering)	C74.1 Overconfidence in the autonomous ship steering system C74.2 The onboard crew does not understand that the current situation is an emergency (misperception of their own ship's performance or current information on their ship/surrounding/environment, etc.). C74.3 The onboard crew is not familiar with how to switch the ship steering mode C74.4 The onboard crew's sudden illness, napping, or engaging in other tasks, among other factors	Same as ID1	• Advance training of the onboard crew • Appropriate HMI design that the crew can understand current situations well and the verification	2	5	7	Same as ID67	2	5	7	* Recommendations to improve the safety more: • Consider introducing a crew monitoring system • Workload management for onboard crew members (limiting the work they can perform)

75	Too late/too early to implement emergency response (forced switchover to manual steering)	Same as ID61	Same as ID1	Same as ID73	2	6	8	Same as ID67	2	5	7	Same as ID67

Appendix 2. A practical example of risk analysis on a demonstration experiment of phase III autonomous ship

A practical example of risk analysis on a demonstration experiment of phase III autonomous ship are shown in this Appendix. We assume two phases, that is, normal navigation and berthing/unberthing. It should be noted that risk analysis is desirable considering more phases to increase the comprehensiveness of hazards.

i. Preparation of documents

Examples of the documents mentioned in section 4.1 of this procedure are shown as follows:

(0) ConOps

Table 2.1 ConOps

● Definition of the feature This feature targets a given voyage plan, detects other ships and wreckage that the ship encounters, disturbances caused by marine weather, formulates a ship action plan according to a predetermined action policy, calculates engine output and steering commands to achieve the action plan, and outputs the speed and the course for the ship to achieve the voyage plan. The voyage plan consists of the departure point, departure date and time, arrival point, arrival date and time, and way point. The autonomous ship steering system onboard the ship will formulate a ship action plan based on the voyage plan and control the steering and engine output in accordance with the ship action plan using the ship control system. <Navigation Plan> Departure point: XXX Port Departure date and time: Month/date, XX:XX Arrival point: YYY Port Arrival date and time: Month/date, YY:YY Waypoint: ZZZ Port Waypoint arrival date and time: Month/date, ZZ:ZZ <Action Policy> Secure an appropriate time to begin avoidance and an appropriate distance to avoid interfering navigation of other ships or causing fear on sailor of other ships. Considering the voyage plan, in order to prevent a large delay, the time spent on avoidance navigation should be minimized while securing the above mentioned appropriate avoidance start time and distance.
● Objective of the feature The objective of this feature is to develop the ship steering plan that includes responses to external

obstacles and disturbances that may act as impediments in the realization of the voyage plan and to control the ship according to that action plan.
● Extend of automation and relation of automation with operators (onboard crew/remote operators) Extent of automation of the present feature is equivalent to the Category II shown in the ClassNK Guidelines [4]. Collection of information on obstacles, integration of the collected information, and preparation of the action plan are performed with this feature. The action plan is output to the steering and engine equipment by the present feature. Within the assumed conditions of use for this feature discussed below, autonomous navigation is performed with this feature. Outside these conditions, the crew on board steers in the conventional method.
● Extent of remote control and relation with operators (onboard crew/remote operators) This feature does not have remote control capability.
●Assumed range of use ship: Ship name: ○○○ Type of ship: Ferry Gross tonnage: 199 tons Loa: 45 m Width: 9 m Navigation area: Coasting area Route: Port XXX to Port YYY Phase of operation: normal navigation (including in-port and out-of-port); berthing and unberthing.
● Autonomous navigation methods Autonomous navigation of a ship equipped with this feature is performed by taking over the tasks from the onboard crew on the sea route within the assumed conditions of use and turning on the feature upon having the onboard crew confirming the operation. t Completing the autonomous navigation along the sea route within the assumed conditions of use and hanging over the tasks to the onboard crew completes the extent of autonomous navigation. If the ship leaves the ODD during its route, even within the assumed conditions of use, autonomous navigation is stopped by handing over to the onboard crew.
● Means of monitoring relevant feature The sensor information collected and integrated into the present feature, the prepared action plan, and the position of the ship within the ODD are constantly provided to the onboard crew by the

dedicated monitoring device on the ship.
● Response procedures in case of deviation from the ODD during the automatic operation Deviation from the ODD is detected by this feature and the onboard crew are notified by the onboard alarm. After the crew switch from autonomous mode to manual mode in a defined procedure, the crew take over the control of the ship.

(1) Functional requirements for the automation system (target tasks and subtasks of the automation)

Table 2.2 Functional requirements for the automation system (Phase: Normal navigation)

ID	Element name	Task	Subtask
1	Autonomous ship steering system	· Establish action plan · Switch operation phase (normal navigation → berthing) · Diagnose own status	· Obtain integrated information on own ship · Obtain integrated information on other ships and drifting objects · Obtain integrated information on marine weather conditions · Calculate navigational safety and economic efficiency · Present ship action plans · Obtain information necessary to diagnose own status
2	Information integration system for own ship	· Integrate information on own ship · Diagnose own status · Diagnose sensor status	· Obtain information on own ship · Obtain information necessary to diagnose own status · Obtain information necessary to diagnose sensor status · Transmit integrated information, own status, and sensor status
3	Information integration system for other ships/ drifting objects	· Integrate information on other ships and drifting objects · Diagnose own status · Diagnose sensor status	· Obtain information on other ships and drifting objects · Obtain information necessary to diagnose own status · Obtain information necessary to diagnose sensor status · Transmit integrated information, own status, and sensor status

4	Information integration system for marine weather	· Integrate of the information on marine weather conditions · Diagnose own status · Diagnose sensor status	· Obtain information on marine weather conditions (current location) · Obtain marine weather condition forecast information · Obtain information necessary to diagnose own status · Obtain information necessary to diagnose sensor status · Transmit integrated information, own status, and sensor status
5	Ship control system	· Calculate control variables based on ship action plans · Rudder/engine control · Diagnose rudder/engine status · Diagnose own status	· Obtain ship action plans · Obtain actual ship's position · Calculate of the deviation between the ship action plans and the ship's position · Compare current situation with control threshold values · Transmit rudder/engine status and own status
6	Autonomous operation management system	· Control mode switching instructions · Diagnose own status	· Obtain information on own ship, other ships, drifting objects, marine weather conditions · Obtain information on the status of each system · Determine whether inside or outside ODD · Obtain information necessary to diagnose own status
7	Onboard crew	(Immediately before going to the bridge) · Go to the bridge based on instructions from the autonomous operation management system (After arriving at the bridge) · Identify current situation	· Confirm the operation mode switching instructions of the autonomous operation management system · Confirm information on own ship, other ships/drifting objects, weather/sea conditions

		· Switch the ship steering mode based on instructions from the system · Manual operation	
8	Shadow crew	· Constant monitoring of each system, surrounding conditions, etc. · Emergency response (forced switchover to manual mode)	

Table 2.3 Functional requirements for the automation system (Phase: Berthing/unberthing)

ID	Element name	Task	Subtask
1	Autonomous ship steering system	• Establish berthing/ unberthing action plan • Switch operation phase (unberthing → normal navigation) • Diagnose own status	• Obtain integrated information on own ship • Obtain integrated information on other ships and drifting objects • Obtain integrated information on marine weather conditions • Calculate navigational safety and economic efficiency • Present ship action plans for berthing/ unberthing • Obtain information necessary to diagnose own status
2	Information integration system for own ship	• Integrate information on own ship • Diagnose own status • Diagnose sensor status	• Obtain information on own ship • Obtain information necessary to diagnose own status • Obtain information necessary to diagnose sensor status • Transmit integrated information, own status, and sensor status
3	Measuring system for the distance	• Measure the distance between own ship and the berth • Activate an alarm in case	• Obtain the position of the berth • Obtain the position of own ship • Obtain information necessary to diagnose own status

	from the berth	of proximity • Diagnose own status • Diagnose sensor status	• Obtain information necessary to diagnose sensor status
4	Information integration system for other ships/ drifting objects	• Integrate information on other ships and drifting objects • Diagnose own status • Diagnose sensor status	• Obtain information on other ships and drifting objects • Obtain information necessary to diagnose own status • Obtain information necessary to diagnose sensor status • Transmit integrated information, own status, and sensor status
5	Information integration system for marine weather	• Integrate of the information on marine weather conditions • Diagnose own status • Diagnose sensor status	• Obtain information on marine weather conditions (current location) • Obtain marine weather condition forecast information • Obtain information necessary to diagnose own status • Obtain information necessary to diagnose sensor status • Transmit integrated information, own status, and sensor status
6	Ship control system	• Calculate control variables based on ship action plans for berthing/unberthing • Rudder/engine control • Diagnose rudder/engine status • Diagnose own status	• Obtain ship action plans for berthing/ unberthing • Obtain actual ship’s position • Calculate of the deviation between the ship action plans for berthing/ unberthing and the ship’s position • Compare current situation with control threshold values • Transmit rudder/engine status and own status
7	Autonomous operation management system	• Control mode switching instructions • Diagnose own status	• Obtain information on own ship, other ships, drifting objects, marine weather conditions, and distance to the berth • Obtain information on the status of each system • Determine whether inside or outside ODD

			• Obtain information necessary to diagnose own status
8	Onboard crew	(Immediately before going to the bridge) • Go to the bridge based on instructions from the autonomous operation management system (After arriving at the bridge) • Identify current situation • Switch the ship steering mode based on instructions from the system • Manual operation	• Confirm the operation mode switching instructions of the autonomous operation management system • Confirm information on own ship, other ships/drifting objects, weather/sea conditions, and distance to the berth
9	Shadow crew	• Constant monitoring of each system, surrounding conditions, etc. • Emergency response (forced switchover to manual mode)	

(2) System architecture that clarifies the entire image of the automation system

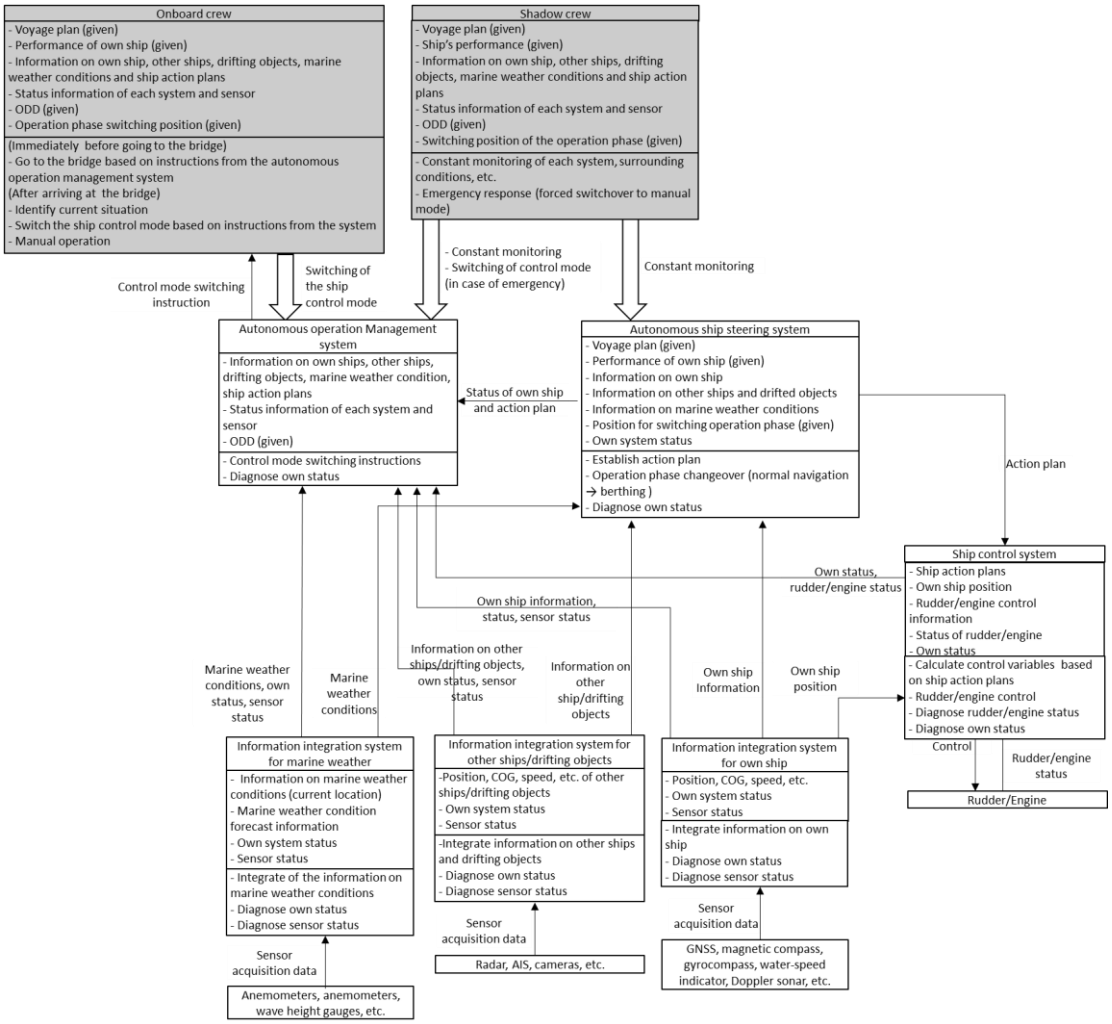

Figure 2.1 System architecture (Phase: Normal navigation)

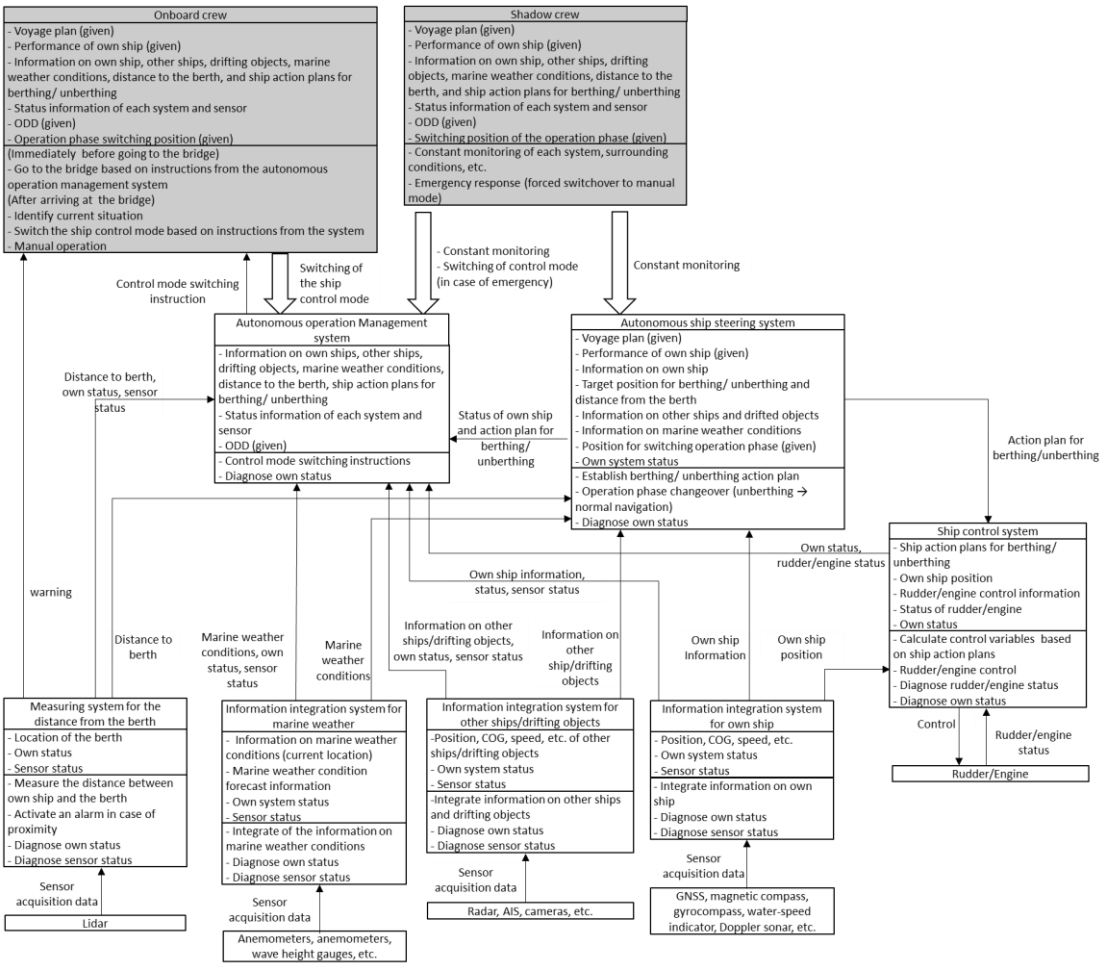

Figure 2.2 System architecture (Phase: Berthing/unberthing)

(3) Outline of the internal operation of the automation system

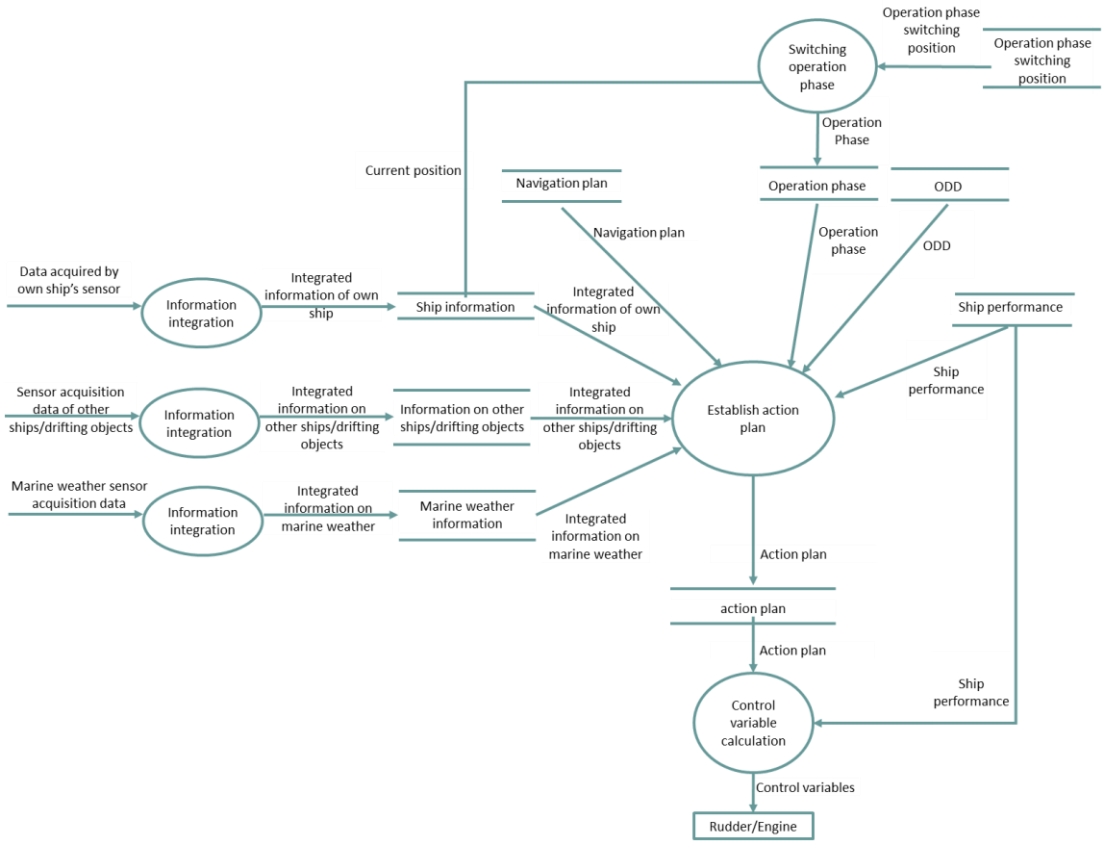

Figure 2.3 Outline of the internal operation regarding autonomous navigation (Phase: Normal navigation)

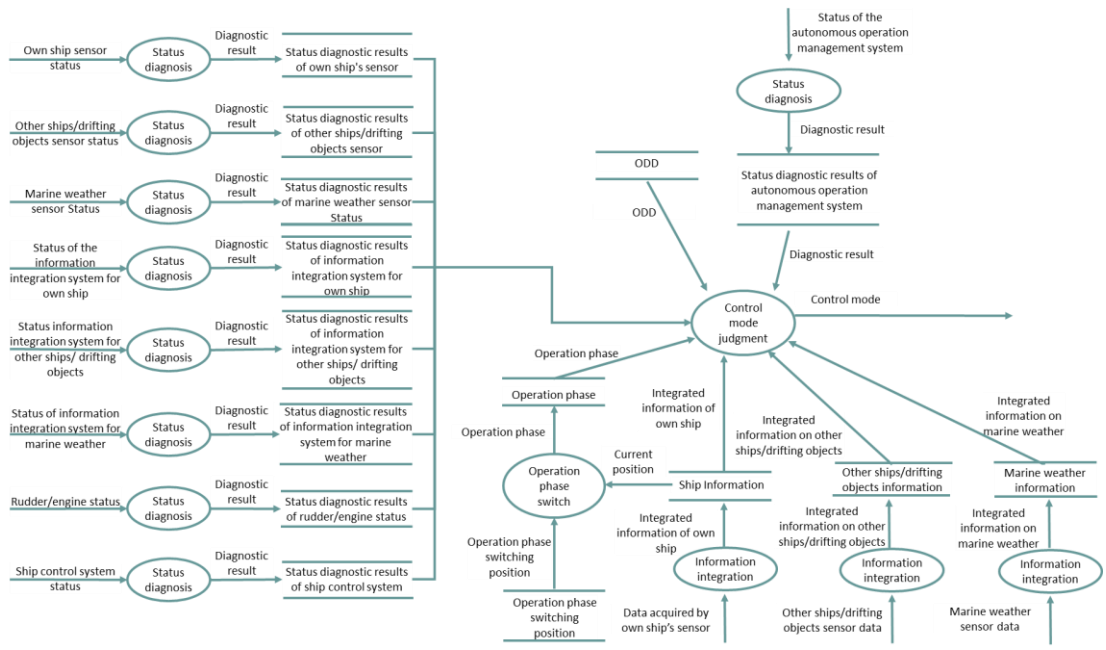

Figure 2.4 Outline of the internal operation regarding mode decision (Phase: Normal navigation)

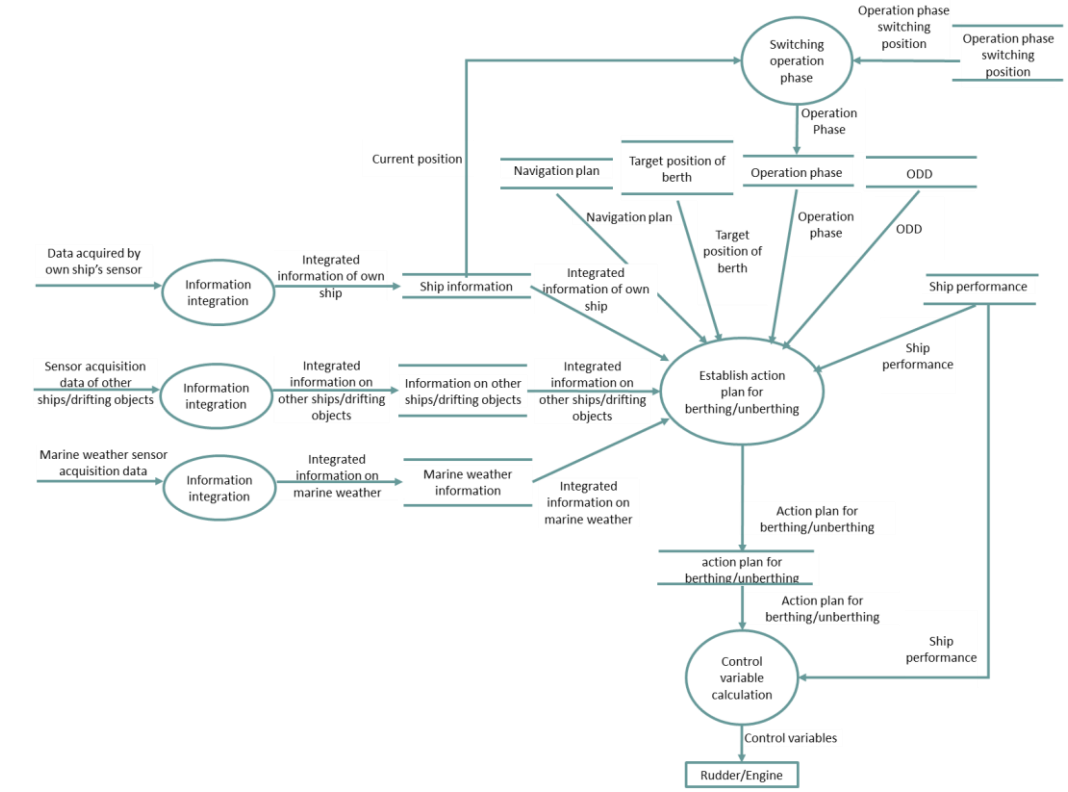

Figure 2.5 Outline of the internal operation regarding autonomous navigation (Phase: Berthing/unberthing)

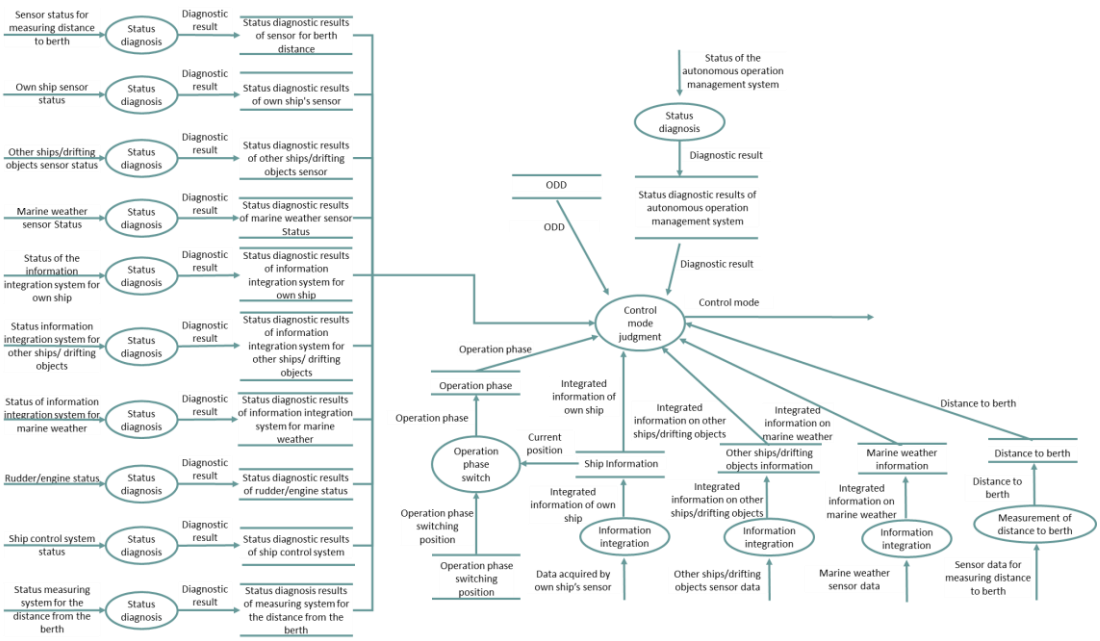

Figure 2.6 Outline of the internal operation regarding mode decision (Phase: Berthing/unberthing)

(4) Outline of the division of roles for the automation system and humans

Table 2.4 Outline of the division of roles for the automation system and humans (Phase: Normal navigation)

Task	Autonomous ship steering system	Information integration system for own ship	Information integration system for other ships/drifting objects	Information integration system for marine weather	Ship control system	Autonomous operation management system	Onboard crew	Shadow crew
Switching operation phase	(1) Switching							(2) Monitoring
Obtaining information on own ship		(1) Acquiring and integrating information						(2) Monitoring
Obtaining information on other ships/drifting objects, etc.			(1) Acquiring and integrating information					(2) Monitoring
Obtaining marine				(1) Acquiring and				(2) Monitoring

weather information				integrating information				
Establishing (avoidance) action plan	(1) Establishing							(2) Monitoring
Executing (avoidance) action plan					(1) Executing			(2) Monitoring
Diagnosis of related sensor status		(1) Diagnosis of conditions	(1) Diagnosis of conditions	(1) Diagnosis of conditions				(2) Monitoring
Diagnosis of own status	(1) Diagnosis of conditions	(1) Diagnosis of conditions	(1) Diagnosis of conditions	(1) Diagnosis of conditions	(1) Diagnosis of conditions	(1) Diagnosis of conditions		(2) Monitoring
Judging inside or outside the ODD and determining steering mode						(1) Judging and determining		(2) Monitoring
Control mode switching						(1) Control mode switching	(2) Going to the bridge	(5) Monitoring

instructions and control mode switch-over						instructions	(3) Identifying current status (4) Mode switching	
Forced switch-over to manual mode								(1) Monitoring (2) Switch-over to manual mode

Table 2.5 Outline of the division of roles for the automation system and humans (Phase: Berthing/unberthing)

Task	Autonomous ship steering system	Information integration system for own ship	Information integration system for other ships/drifting objects	Information integration system for marine weather	Measuring system for the distance from the berth	Ship control system	Autonomous operation management system	Onboard crew	Shadow crew
Switching operation phase	(1) Switching								(2) Monitoring

Obtaining information on own ship		(1) Acquiring and integrating information							(2) Monitoring
Obtaining information on other ships/drifting objects, etc.			(1) Acquiring and integrating information						(2) Monitoring
Obtaining marine weather information				(1) Acquiring and integrating information					(2) Monitoring
Measuring distance to berth					(1) Measuring				(2) Monitoring
Establishing action plan for berthing/unberthing	(1) Establishing								(2) Monitoring
Executing action plan						(1) Executing			(2) Monitoring

for berthing/ unberthing									
Diagnosis of related sensor status		(1) Diagnosis of conditions	(1) Diagnosis of conditions	(1) Diagnosis of conditions	(1) Diagnosis of conditions				(2) Monitoring
Diagnosis of own status	(1) Diagnosis of conditions	(1) Diagnosis of conditions	(1) Diagnosis of conditions	(1) Diagnosis of conditions	(1) Diagnosis of conditions	(1) Diagnosis of conditions	(1) Diagnosis of conditions		(2) Monitoring
Judging inside or outside the ODD and determining steering mode							(1) Judging and determining		(2) Monitoring
Control mode switching instructions and control mode switchover							(1) Control mode switching instructions	(2) Going to the bridge (3) Identifying current status (4) Mode switching	(5) Monitoring

Forced switch-over to manual mode									(1) Moni-toring (2) Switch over to manual mode

(5) ODD of an automation system

Table 2.6 ODD of an automation system

Marine area conditions	
Navigation zone	Designated ship course
Waters within a departing/arriving harbor	There shall be occupied waters necessary for change of direction in the harbor: 3 L of occupied waters
Waters around a departing/arriving the berth	There shall be occupied waters necessary for departing from or arriving at the berth: 0.5 L of occupied waters
Degree of congestion	Low Congestion: Up to 5 ships within a 3 NM range
Ships not equipped with AIS and obstructions	No non-AIS equipped ships or obstacles that the system cannot detect: No dangerous obstacles of less than 1 m in size within 700 m
Environmental condition	
Marine weather	Calm condition: Wind: 7 m/s or less, wave height: 1.5 m or less, and visibility: 500 m or more
Time	All day
Internal state	
System state	Running normally: No error indication
Equipment required for operation	Running normally: No error indication
Ship motion	Within design constraints of the hull: No anomaly indicated
Other	No emergency events have occurred: No inboard fire, outboard fire, overboard, emergency signal interception, etc.

(6) Outline of a demonstration experiment

· Objective of the experiment: To identify points that need to be improved in the automatic navigation

system by operating a ship equipped with the system under development in actual seas.

· Experimental route: Port XXX to Port YYY

· Date of experiment: YYYY/MM/DD

· Shadow crew: Keep a constant watch and check the operation of the ship during automatic ship steering using this function and perform a fallback operation when any abnormality is detected. Shadow crew shall be present on the bridge at all times.

· Onboard crew: Onboard crew remain in their cabins during automatic ship steering. When an alarm from the autonomous operation Management system is triggered, they shall go to the bridge, switch to manual ship steering, and steer the ship.

· Passenger: The ship is a passenger ship; however, the experiment will be conducted without passengers on board.

ii. Risk analysis

Examples of HAZID WS are shown in Tables 2.7 and 2.8. These are risk analysis results on the demonstration experiment of Phase III autonomous ship which explained in the above i (Preparation of documents). The definitions of FI (Frequency Index), SI (Severity Index) and RI (Risk Index) are the same as those of section5.3 of this procedure document.

Table 2.7 HAZID WS (Phase: Normal navigation)

Sheet ID: 1
Phase: Normal navigation

ID	Hazard	Causes	Consequences	Existing Safeguards	Index(only existing safeguards)			Safeguards at Trial	Index(Include safeguards at trial)			Emergency Plan	Comments (safety measures for commercial operation, etc.)
					SI	FI	RI		SI	FI	RI		
Autonomous ship steering system													
1	Error in establishing the action plan	C1.1 Input information not obtained or incorrect (information on own ship, other ships and drifting objects, marine weather, etc.) C1.2 Voyage plan (given) not obtained or incorrect C1.3 Faulty algorithm for establishing the ship action plan in the autonomous ship steering system C1.4 Failure or malfunction of the autonomous ship steering system C1.5 Malware infiltration or hacking	E1.1 Abnormal approach to other ships/objects, or areas with grounding risk E1.2 Collision, grounding, capsizing, and sinking	• Alarm for each system failure • Alarm when various information and voyage plans are not entered • Double-checking when entering voyage plans • Alarm when jumping position of own ship or other ships/drifts • Prior verification by simulations of action planning algorithms • Connect only to removable media with no viruses detected by virus detection software as well as no connection to external networks	1	5	6	• Constant monitoring by the shadow crews • Takeover by the shadow crews • training of the shadow crews regarding switching to the ship steering mode, etc. • Terminate experiments in case of malfunctions or abnormalities.	1	5	6	(1) Activate alarm in case of failure or abnormality. Moreover, abnormality or failure is detected through constant monitoring by the shadow crews. (2) Switch to manual steering at the discretion of the shadow crews. *If necessary, prepare details of the emergency plan separately	• Improvement of the action planning algorithm • Consideration of measures to improve system reliability (redundancy, etc.) (including cost–benefit study) • Verification of outputs and introduction of functions to deal with the verification results (implemented by human or machine, depending on the level of automation)

2	No implementation of the action plan	C2.1 Input information not obtained (information on own ship, other ships and drifting objects, marine weather, etc.) C2.2 Voyage plan (given) not obtained C2.3 Failure or malfunction of the autonomous ship steering system C2.4 Malware intrusion or hacking C2.5 Failure to receive inquiry (trigger for activating this function)	Same as ID1	• Alarm for each system failure • Alarm when various information and voyage plans are not entered • Alarm when a certain amount of time has elapsed • Pre verification through simulations • Connect only to removable media with no viruses detected by virus detection software as well as no connection to external networks	1	5	6	Same as ID1	1	5	6	Same as ID1	• Consideration of measures to improve system reliability (redundancy, etc.) (including cost–benefit study) • If there is no response, the inquiry source shall be made to ask again with new input information. • Introduce a function to deal with no response even after re querying (implemented by human or machine, depending on the level of automation)

3	Too late/too early implementation of the action plan	C3.1 Input information not obtained or obtained at the wrong time (information on own ship, other ships and drifting objects, marine weather, etc.) C3.2 Failure of the autonomous ship steering system's berthing/ unberthing action planning algorithm (too much time is spent on calculations for action planning) C3.3 Failure or malfunction of the autonomous ship steering system C3.4 Malware infiltration or hacking C3.5 Wrong timing of inquiry (trigger for activation of this function)	Same as ID1	Same as ID2	1	5	6	Same as ID1	1	5	6	Same as ID1	• Consideration of measures to improve system reliability (redundancy, etc.) (including cost–benefit study) • If the response is too late, the inquiry source shall be made to ask again with new input information. • Introduce a function to deal with cases where a response is not received in time (implemented by human or machine, depending on the level of automation)

4	Error in the switching operation phase (normal navigation phase to berthing phase)	C4.1 Incorrect input of the (given) position to switch the operation phase C4.2 Incorrect input information (own ship's position information) C4.3 Failure or malfunction of the autonomous ship steering system C4.4 Malware intrusion or hacking	E4.1 Deviation from course E4.2 Abnormal approach to other ships/objects, berth, or areas with grounding risk E4.3 Collision with other ships or berth, grounding, and capsizing or sinking	• Alarm for each system failure • Double check when inputting the operation phase switching position • Alarm at the time of position jump of own ship • Alarm at the time of route deviation • Pre verification through simulations • Connect only to removable media with no viruses detected by virus detection software as well as no connection to external networks	1	5	6	Same as ID1	1	5	6	Same as ID1	• Consideration of measures to improve system reliability (redundancy, etc.) (including cost–benefit study)

5	No changeover of the operation phase (normal navigation phase to berthing phase)	C5.1 Incorrect input of the (given) position to switch the operation phase C5.2 Incorrect input or no input of input information (own ship's position information) C5.3 Failure or malfunction of the autonomous ship steering system C5.4 Malware intrusion or hacking C5.5 Failure to receive inquiry (trigger for activating this function)	Same as ID4	• Alarm for each system failure • Alarm if operation phase switching position or own position are not entered • Alarm at the time of position jump of own ship • Alarm at the time of route deviation • Pre verification through simulations • Activate alarm when a certain distance from the operation phase switching position is exceeded • Connect only to removable media with no viruses detected by virus detection software as well as no connection to external networks	1	5	6	Same as ID1	1	5	6	Same as ID1	Same as ID2

6	Too late/too early to implement switching the operation phases (normal navigation phase to berthing phase)	C6.1 Wrong timing of obtaining input information (own ship's position) C6.2 Malfunction of the operation phase switching algorithm (switching operation takes too long) C6.3 Failure or malfunction of the autonomous ship steering system C6.4 Malware intrusion or hacking C6.5 Wrong timing of inquiry (trigger for activating this function)	Same as ID4	• System failure alarm • Alarm at the time of route deviation • Pre verification through simulations • Activate alarm when a certain distance from the operation phase switching position is exceeded • Connect only to removable media with no viruses detected by virus detection software as well as no connection to external networks	1	5	6	Same as ID1	1	5	6	Same as ID1	Same as ID3
7	Error in diagnosis of own status	C7.1 Wrong algorithm for the self-diagnostic function of the autonomous ship steering system C7.2 Incorrect input information (information required for self-diagnosis) C7.3 Malware intrusion or hacking	• Misdiagnose as normal when abnormal → Same as ID4 • Misdiagnose as abnormal when normal → Switch to manual steering based on alarm	• Pre verification of the self-diagnostic function • Connect only to removable media with no viruses detected by virus detection software as well as no connection to external networks	1	5	6	Same as ID1	1	5	6	Same as ID1	Same as ID4

8	No implementation of the diagnosis of own ship's status	C8.1 Failure, malfunction, or stoppage of the self-diagnostic function of the autonomous ship steering system C8.2 Input information (information necessary for self-diagnosis) not obtained C8.3 Malware intrusion or hacking	• Diagnosis not performed when normal → No problem (alarm will be activated when a certain period of time is exceeded) • Diagnosis not performed when abnormal → Same as ID4	• Pre verification of the self-diagnostic function • Alarm activated when a certain amount of time is exceeded • Connect only to removable media with no viruses detected by virus detection software as well as no connection to external networks	1	5	6	Same as ID1	1	5	6	Same as ID1	ID4と同じ

9	Too late/too early to implement the diagnosis of own status	C9.1 Failure or malfunction of the self-diagnostic function of the autonomous ship steering system C9.2 Malfunction of the self-diagnostic algorithm of the autonomous ship steering system (self-diagnostic operation takes too much time) C9.3 Incorrect timing for obtaining input information (information necessary for self-diagnosis) C9.4 Malware intrusion or hacking	• Too late to diagnose when normal → No problem (alarm will be activated when a certain period of time is exceeded) • Too late to diagnose as abnormal when abnormal → E9.1 Delay in switching to the manual operation E9.2 Autonomous operation outside ODD E9.3 Deviation from course E9.4 Abnormal approach to other ships/objects, or areas with grounding risk E9.5 Collision, grounding, capsizing, or sinking	Same as ID8	1	5	6	Same as ID1	1	5	6	Same as ID1	Same as ID4
Information integration system for own ship														

10	Error in integration of own ship information	C10.1 Inconsistency in input information (e.g., different data between sensors of own ship, integration with old information, etc.) C10.2 Failure or malfunction of the information integration function and, error in the integration algorithm C10.3 Malware intrusion or hacking	E10.1 Establishment of the incorrect avoidance action plan E10.2 Incorrect calculation of the control variables E10.3 Incorrect/no switching of the operation phase E10.4 Deviation from course E10.5 Abnormal approach to other ships/objects or areas with grounding risk E10.6 Collision, grounding, capsizing, or sinking	• Advance verification of the information integration function • Integrating a method for dealing with discrepancies in data (which data should be prioritized) • Alarm for each system failure • Warnings when the same type of data differs • Connect only to removable media with no viruses detected by virus detection software as well as no connection to external networks	1	5	6	Same as ID1	1	5	6	Same as ID1	• Consideration of measures to improve system reliability (redundancy, etc.) (including cost–benefit study) • Improvement of the information integration algorithm • Management of the reliability of integrated information (reliability evaluation and formulation of countermeasures in case of low reliability)

11	No implementation of integrating information of own ship	C11.1 Inconsistency in input information (different data between sensors of own ship) C11.2 Failure or malfunction of the information integration function and error in the integration algorithm C11.3 Malware intrusion or hacking C11.4 Failure to receive inquiry (trigger for activating this function)	Same as ID10	• Advance verification of the information integration function • Incorporating a method for dealing with discrepancies in data (which data should be prioritized) • Alarm for each system failure • Warnings when the same type of data differs • Alarm activated when a certain amount of time is exceeded • Connect only to removable media with no viruses detected by virus detection software as well as no connection to external networks	1	4	5	Same as ID1	1	4	5	Same as ID1	• Consideration of measures to improve system reliability (redundancy, etc.) (including cost–benefit study) • Improvement of the information integration algorithm • Introduce a function to deal with the absence of outputs (e.g., restarting the system in question; prepared separately from diagnosis of own to deal with the case of a stoppage of functionality)

12	Too late/too early to implement integrating own ship information	C12.1 Malfunction of the information integration function/algorithm (information integration takes too much time) C12.2 Wrong timing of information acquisition from different sensors C12.3 Malware intrusion or hacking C12.4 Wrong timing of inquiry (trigger for activating this function)	E12.1 Establishment of the incorrect avoidance action plan E12.2 Incorrect calculation of the control variables E12.3 Switch the operation phase at wrong position E12.4 Deviation from course E12.5 Abnormal approach to other ships/objects or areas with grounding risk E12.6 Collision, grounding, capsizing, or sinking	Same as ID11	1	5	6	Same as ID1	1	5	6	Same as ID1	• Consideration of measures to improve system reliability (redundancy, etc.) (including cost–benefit study) • Improvement of the information integration algorithm • Introduce a function to deal with large delays in output (e.g., restarting the system in question).
13	Error in the diagnosis of own status	C13.1 Failure or malfunction of the self-diagnostic function C13.2 Wrong algorithm for the self-diagnostic function C13.3 Incorrect input information (information required for self-diagnosis) C13.4 Malware intrusion or hacking	Same as ID7	Same as ID7	1	5	6	Same as ID1	1	5	6	Same as ID1	• Improvements in algorithm for self-diagnostic function

14	No implementation of the diagnosis of own status	C14.1 Failure, malfunction, or stoppage of the self-diagnostic function C14.2 Input information (information necessary for self-diagnosis) not obtained C14.3 Malware intrusion or hacking	Same as ID8	Same as ID8	1	5	6	Same as ID1	1	5	6	Same as ID1	Same as ID13
15	Too late/too early to implement the diagnosis of own status	C15.1 Failure or malfunction of the self-diagnostic function C15.2 Malfunction of the self-diagnostic algorithm (self-diagnostic operation takes too much time) C15.3 Incorrect timing for obtaining input information (information required for self-diagnosis) C15.4 Malware intrusion or hacking	Same as ID9	Same as ID9	1	5	6	Same as ID1	1	5	6	Same as ID1	Same as ID13

16	Error in diagnosing sensor status	C16.1 Failure or malfunction of the status diagnostic function for the sensor C16.2 Wrong algorithm for the status diagnostic function for the sensors of own ship C16.3 Incorrect input information (information required for sensor status diagnosis) C16.4 Malware intrusion or hacking	• Misdiagnose as normal when abnormal → Same as ID10 • Misdiagnose as abnormal when normal → Switch to manual steering based on alarm	• Pre verification of the status diagnostic function and algorithm for the sensor • Connect only to removable media with no viruses detected by virus detection software as well as no connection to external networks	1	5	6	Same as ID1	1	5	6	Same as ID1	• Improvements in algorithm for the diagnostic function of the sensor status
17	No implementation of the diagnosis of sensor status	C17.1 Failure or malfunction of the status diagnostic function for the sensors of own ship C17.2 Input information (information necessary for sensor status diagnosis) not obtained C17.3 Malware intrusion or hacking	• Diagnosis not performed when abnormal → Same as ID10 • Diagnosis not performed when normal → No problem (alarm will be activated when a certain period of time is exceeded)	• Pre verification of the status diagnostic function for the sensors • Alarm activated when a certain amount of time is exceeded • Connect only to removable media with no viruses detected by virus detection software as well as no connection to external networks	1	5	6	Same as ID1	1	5	6	Same as ID1	Same as ID16

18	Too late/too early to implement the diagnosis of sensor status	C18.1 Failure or malfunction of the status diagnostic function for the sensors of own ship C18.2 Malfunction of the sensor status diagnosis algorithm (status diagnosis operation takes too much time) C18.3 Wrong timing of obtaining input information (information required for sensor status diagnosis) C18.4 Malware intrusion or hacking	• Too late to diagnose as normal when normal → No problem (alarm will be activated when a certain period of time is exceeded) • Too late to diagnose as abnormal when abnormal → Same as ID12	• Pre verification of the status diagnostic function and algorithm for the sensors • Alarm activated when a certain amount of time is exceeded • Connect only to removable media with no viruses detected by virus detection software as well as no connection to external networks	1	5	6	Same as ID1	1	5	6	Same as ID1	Same as ID16
Information integration system for other ships and drifting objects														

19	Error in integration information of other ships and drifting objects	C19.1 Inconsistency in input information (e.g., different data between sensors, integration with old information) C19.2 Failure or malfunction of the information integration function as well as errors in the integration algorithm C19.3 Malware intrusion or hacking	E19.1 Establishment of the incorrect avoidance action plan E19.2 Abnormal approach to other ships/objects or areas with grounding risk E19.3 Collision, grounding, capsizing, or sinking	Same as ID10	1	5	6	Same as ID1	1	5	6	Same as ID1	Same as ID10
20	No implementation of integration information of other ships and drifting objects	C20.1 Inconsistency in input information (e.g., different data between sensors) C20.2 Failure or malfunction of the information integration function as well as errors in the integration algorithm C20.3 Malware intrusion or hacking C20.4 Failure to receive inquiry (trigger for activating this function)	Same as ID19	Same as ID11	1	4	5	Same as ID1	1	4	5	Same as ID1	Same as ID11

21	Too late/too early implementation of integration information of other ships and drifting objects	C21.1 Failure of information integration function/algorithm (information integration takes too much time) C21.2 Wrong timing of information acquisition from different sensors C21.3 Malware intrusion or hacking C21.4 Wrong timing of inquiry (trigger for activation of this function)	Same as ID19	Same as ID11	1	5	6	Same as ID1	1	5	6	Same as ID1	Same as ID12
22	Error in diagnosing own status	C22.1 Failure or malfunction of the self-diagnostic function C22.2 Wrong algorithm for the self-diagnostic function C22.3 Incorrect input information (information necessary for self-diagnosis) C22.4 Malware intrusion or hacking	Same as ID7	Same as ID7	1	5	6	Same as ID1	1	5	6	Same as ID1	Same as ID13

23	No implementation of diagnosing own status	C23.1 Failure or malfunction of the self-diagnostic function C23.2 Input information (information necessary for self-diagnosis) not obtained C23.3 Malware intrusion or hacking	Same as ID8	Same as ID8	1	5	6	Same as ID1	1	5	6	Same as ID1	Same as ID13
24	Too late/too early implementation of diagnosing own status	C24.1 Failure or malfunction of the self-diagnostic function C24.2 Malfunction of the self-diagnostic algorithm (self-diagnostic operation takes too much time) C24.3 Wrong timing of obtaining input information (information required for self-diagnosis) C24.4 Malware intrusion or hacking	Same as ID9	Same as ID9	1	5	6	Same as ID1	1	5	6	Same as ID1	Same as ID13

25	Error in diagnosing sensor status	C25.1 Failure or malfunction of the status diagnostic function for the sensors C25.2 Wrong algorithm for the status diagnostic function for the sensors C25.3 Incorrect input information (information necessary for sensor status diagnosis) C25.4 Malware intrusion or hacking	• Misdiagnose as normal when abnormal → Same as ID19 • Misdiagnose as abnormal when normal → Switch to manual steering based on alarm	Same as ID16	1	5	6	Same as ID1	1	5	6	Same as ID1	Same as ID16
26	No implementation of diagnosing sensor status	C26.1 Failure or malfunction of the status diagnostic function for the sensors C26.2 Input information (information necessary for sensor status diagnosis) not obtained C26.3 Malware intrusion or hacking	• Diagnosis not performed when abnormal → Same as ID19 • Diagnosis not performed when normal → No problem (alarm will be activated when a certain period of time is exceeded)	Same as ID17	1	5	6	Same as ID1	1	5	6	Same as ID1	Same as ID16

27	Too late/too early implementation of diagnosing sensor status	C27.1 Failure or malfunction of the status diagnostic function for the sensors C27.2 Malfunction of the algorithm for the sensor status diagnosis (status diagnosis operation takes too much time) C27.3 Wrong timing of obtaining input information (information required for sensor status diagnosis) C27.4 Malware intrusion or hacking	• Too late diagnosis as normal when normal → No problem (alarm will be activated when a certain period of time is exceeded) • Too late diagnosis as abnormal when abnormal → Same as ID19	Same as ID18	1	5	6	Same as ID1	1	5	6	Same as ID1	Same as ID16
Information integration system for marine weather														
28	Error in integration of marine weather information	C28.1 Inconsistency in input information (e.g., different data between sensors, integration with old information) C28.2 Failure or malfunction of the information integration function as well as error in integration algorithm C28.3 Malware intrusion or hacking	Same as ID19	Same as ID10	1	5	6	Same as ID1	1	5	6	Same as ID1	Same as ID10

29	No implementation of integrating marine weather information	C29.1 Inconsistency in input information (e.g., different data between sensors) C29.2 Failure or malfunction of the information integration function as well as error in integration algorithm C29.3 Malware intrusion or hacking C29.4 Failure to receive inquiry (trigger for activating this function)	Same as ID19	Same as ID11	1	4	5	Same as ID1	1	4	5	Same as ID1	Same as ID11
30	Too late/too early implementation of integrating marine weather information	C30.1 Failure or malfunction of the information integration function/algorithm (information integration takes too much time) C30.2 Wrong timing of information acquisition from different sensors C30.3 Malware intrusion or hacking C30.4 Wrong timing of inquiry (trigger for activation of this function)	Same as ID19	Same as ID11	1	5	6	Same as ID1	1	5	6	Same as ID1	Same as ID12

31	Error in diagnosing own status	C31.1 Failure or malfunction of the self-diagnostic function C31.2 Wrong algorithm for the self-diagnostic function C31.3 Incorrect input information (information necessary for self-diagnosis) C31.4 Malware intrusion or hacking	Same as ID7	Same as ID7	1	5	6	Same as ID1	1	5	6	Same as ID1	Same as ID13
32	No implementation of diagnosing own status	C32.1 Failure or malfunction of the self-diagnostic function C32.2 Input information (information necessary for self-diagnosis) not obtained C32.3 Malware intrusion or hacking	Same as ID8	Same as ID8	1	5	6	Same as ID1	1	5	6	Same as ID1	Same as ID13

33	Too late/too early implementation of diagnosing own status	C33.1 Failure or malfunction of the self-diagnostic function C33.2 Malfunction of the self-diagnostic algorithm (self-diagnostic operation takes too much time) C33.3 Wrong timing of obtaining input information (information required for self-diagnosis) C33.4 Malware intrusion or hacking	Same as ID9	Same as ID9	1	5	6	Same as ID1	1	5	6	Same as ID1	Same as ID13
34	Error in diagnosing sensor status	C34.1 Failure or malfunction of the status diagnostic function for the sensors C34.2 Wrong algorithm for the status diagnostic function for the sensors C34.3 Incorrect input information (information necessary for sensor status diagnosis) C34.4 Malware intrusion or hacking	• Misdiagnose as normal when abnormal → Same as ID19 • Misdiagnose as abnormal when normal → Switch to manual steering based on alarm	Same as ID16	1	5	6	Same as ID1	1	5	6	Same as ID1	Same as ID16

35	No implementation of diagnosing sensor status	C35.1 Failure or malfunction of the status diagnostic function for the sensors C35.2 Input information (information necessary for sensor status diagnosis) not obtained C35.3 Malware intrusion or hacking	• Diagnosis not performed when abnormal → Same as ID19 • Diagnosis not performed when normal → No problem (alarm will be activated when a certain period of time is exceeded)	Same as ID17	1	5	6	Same as ID1	1	5	6	Same as ID1	Same as ID16
36	Too late/too early implementation of diagnosing sensor status	C36.1 Failure or malfunction of the status diagnostic function for the sensors C36.2 Malfunction of the algorithm for the sensor status diagnosis (status diagnosis operation takes too much time) C36.3 Wrong timing of obtaining input information (information required for sensor status diagnosis) C36.4 Malware intrusion or hacking	• Too late diagnosis as normal when normal → No problem (alarm will be activated when a certain period of time is exceeded) • Too late diagnosis as abnormal when abnormal → Same as ID19	Same as ID18	1	5	6	Same as ID1	1	5	6	Same as ID1	Same as ID16
Ship control system														

37	Error in calculation of the control variables based on the action plan	C37.1 Error in the action plan C37.2 Incorrect input information (information required for control variables calculation) C37.3 Error in the control variables calculation algorithm C37.4 Failure or malfunction of the ship control system C37.5 Malware intrusion or hacking	E37.1 Deviation from course E37.2 Abnormal approach to other ships/objects or areas with grounding risk E37.3 Collision, grounding, capsizing, or sinking	• System failure alarm • Pre verification of the control variables calculation algorithm through simulations • Connect only to removable media with no viruses detected by virus detection software as well as no connection to external networks	1	5	6	Same as ID1	1	5	6	Same as ID1	• Improvement of the control variables calculation algorithm • Consideration of measures to improve system reliability (redundancy, etc.) (including cost–benefit study)

38	No implementation of calculating the control variables based on the action plan	C38.1 Action plan not obtained C38.2 Input information (information required for control variables calculation) not obtained C38.3 Failure or malfunction of the ship control system C38.4 Malware intrusion or hacking C38.5 Failure to receive inquiry (trigger for activating this function)	Same as ID37	• System failure alarm • Alarm at the time when various information is not obtained • Pre verification through simulations • Alarm activated when a certain amount of time is exceeded • Connect only to removable media with no viruses detected by virus detection software as well as no connection to external networks	1	5	6	Same as ID1	1	5	6	Same as ID1	Same as ID2

39	Too late/too early to implement control variables calculations based on the action plan	C39.1 Wrong timing of obtaining the action plan C39.2 Wrong timing of acquiring input information (information required for control variables calculation) C39.3 Malfunction in the control variables calculation algorithm (excessive time required for control variables calculation) C39.4 Failure or malfunction in the ship control system C39.5 Malware intrusion C39.6 Wrong timing of inquiry (trigger for activation of this function)	Same as ID37	• System failure alarm • Pre verification through simulations • Warning activated when a certain period of time has elapsed • Alarm activated when a certain amount of time is exceeded • Connect only to removable media with no viruses detected by virus detection software as well as no connection to external networks	1	5	6	Same as ID1	1	5	6	Same as ID1	Same as ID3

40	Error in control of the rudder or engine	C40.1 Error in control variables calculation C40.2 Actuator malfunction or failure	E40.1 Unable to navigate E40.2 Deviation from course E40.3 Abnormal approach to other ships/objects, or areas with grounding risk E40.4 Collision, grounding, capsizing, or sinking	• Pre verification of the system • Alarms in case of actuator failure or malfunction	1	5	6	Same as ID1	1	5	6	Same as ID1	• Consideration of measures to improve reliability (redundancy, etc.) (including cost–benefit study) • Introduction of a function to deal with incorrect rudder/engine status (e.g., restarting the system in question)

41	No implementation of control of the rudder or engine	C41.1 Input information (control variables) not obtained C41.2 Malfunction or failure of the actuator C41.3 Failure to receive inquiry (trigger for activating this function)	Same as ID40	• Alarms in case of actuator failure or malfunction • Alarm when control variables not obtained • Alarm activated when a certain amount of time is exceeded	1	4	5	Same as ID1	1	4	5	Same as ID1	• Consideration of measures to improve reliability (redundancy, etc.) (including cost–benefit study) • Introduction of a function to deal with cases where the rudder/engine is not under control (e.g., restarting the system in question) • If there is no response, the inquiry source shall be made to ask again with new input information. • Introduce a function to deal with no response even after re querying (implemented by human or machine, depending on the level of automation)

42	Too late/too early to implement controlling the rudder or engine	C42.1 Wrong timing of obtaining input information (control variables) C42.2 Malfunction or failure of the actuator C42.3 Wrong timing of inquiry (trigger for activation of this function)	Same as ID40	Same as ID41	1	5	6	Same as ID1	1	5	6	Same as ID1	• Consideration of measures to improve reliability (redundancy, etc.) (including cost–benefit study) • Introduction of a function to deal with rudder/engine control delays exceeding a certain level (e.g., restarting the system in question). • If the response is too late, the inquiry source shall be made to ask again with new input information. • Introduce a function to deal with cases where a response is not received in time (implemented by human or machine, depending on the level of automation)

43	Error in diagnosis of rudder/engine conditions	C43.1 Failure or malfunction of the rudder/engine condition diagnostic function C43.2 Wrong algorithm for the rudder/engine condition diagnostic function C43.3 Incorrect input information (information required for rudder/engine condition diagnosis) C43.4 Malware intrusion or hacking	Same as ID7	Same as ID7	1	5	6	Same as ID1	1	5	6	Same as ID1	• Improved algorithms for rudder/engine condition diagnostic functions
44	No implementation of diagnosis of rudder/engine conditions	C44.1 Failure or malfunction of the rudder/engine condition diagnostic function C44.2 Input information (information required for rudder/engine condition diagnosis) not obtained C44.3 Malware intrusion or hacking	Same as ID8	Same as ID8	1	5	6	Same as ID1	1	5	6	Same as ID1	Same as ID43

45	Too late/too early to implement diagnosis of rudder/engine conditions	C45.1 Failure or malfunction of the rudder/engine condition diagnostic function C45.2 Malfunction of the rudder/engine condition diagnostic algorithm (self-diagnostic operation takes too much time) C45.3 Wrong timing of obtaining input information (information required for rudder/engine condition diagnosis) C45.4 Malware intrusion or hacking	Same as ID9	Same as ID9	1	5	6	Same as ID1	1	5	6	Same as ID1	Same as ID43
46	Error in diagnosing own status	C46.1 Failure or malfunction of the self-diagnostic function C46.2 Wrong algorithm for the self-diagnostic function C46.3 Incorrect input information (information required for self-diagnosis) C46.4 Malware intrusion or hacking	Same as ID7	Same as ID7	1	5	6	Same as ID1	1	5	6	Same as ID1	Same as ID13

47	No implementation of diagnosing own status	C47.1 Failure, malfunction, or stoppage of the self-diagnostic function C47.2 Input information (information necessary for self-diagnosis) not obtained C47.3 Malware intrusion or hacking	Same as ID8	Same as ID8	1	5	6	Same as ID1	1	5	6	Same as ID1	Same as ID13
48	Too late/too early implementation of diagnosing own status	C48.1 Failure or malfunction of the self-diagnostic function C48.2 Malfunction of the self-diagnostic algorithm (self-diagnostic operation takes too much time) C48.3 Incorrect timing of obtaining input information (information required for self-diagnosis) C48.4 Malware intrusion or hacking	Same as ID9	Same as ID9	1	5	6	Same as ID1	1	5	6	Same as ID1	Same as ID13
Autonomous Operation Management System														

49	Error in instructions for switching the ship steering mode	C49.1 Failure or malfunction of the autonomous operation management system C49.2 Error in the algorithm to switch the operation mode C49.3 Error in input information (information required for making the operation mode switching decision) C49.4 Malware intrusion or hacking	E49.1 Autonomous steering outside ODD E49.2 Deviation from course E49.3 Abnormal approach to other ships/objects or areas with grounding risk E49.4 Collision, grounding, capsizing, or sinking	• Alarm for each system failure • Double-checking at the time of ODD input • Alarm at the time of route deviation • Prior verification of the instruction function to switch the ship steering mode through simulations • Connect only to removable media with no viruses detected by virus detection software as well as no connection to external networks	1	5	6	Same as ID1	1	5	6	Same as ID1	• Improvement of the ship steering mode switching algorithm • Consideration of measures to improve system reliability (redundancy, etc.) (including cost–benefit study)

50	No implementation of the ship steering mode switching instructions	C50.1 Failure or malfunction of the autonomous operation management system C50.2 Error in the algorithm to switch the operation mode C50.3 Error in input information (information required for making the operation mode switching decision) C50.4 Malware intrusion or hacking C50.5 Failure to receive inquiry (trigger for activating this function)	Same as ID49	• Alarm for each system failure • Alarm activated when a certain amount of time is exceeded • Double-checking at the time of ODD input • Alarm at the time of route deviation • Prior verification of the instruction function to switch the ship steering mode through simulations • Connect only to removable media with no viruses detected by virus detection software as well as no connection to external networks	1	5	6	Same as ID1	1	5	6	Same as ID1	Same as ID2

51	Too late/too early to give the ship steering mode switching instructions	C51.1 Failure or malfunction of the autonomous operation management system C51.2 Malfunction of the algorithm to switch the operation mode (calculating the decision to switch the operation mode takes too much time) C51.3 Wrong timing of obtaining input information (information necessary to decide whether to switch the operation mode) C51.4 Malware infiltration or hacking C51.5 Wrong timing of inquiry (trigger for activation of this function)	Same as ID49	Same as ID50	1	5	6	Same as ID1	1	5	6	Same as ID1	Same as ID3

52	Error in diagnosing own status	C52.1 Failure or malfunction of the self-diagnostic function C52.2 Wrong algorithm for the self-diagnostic function C52.3 Incorrect input information (information required for self-diagnosis) C52.4 Malware intrusion or hacking	Same as ID7	Same as ID7	1	5	6	Same as ID1	1	5	6	Same as ID1	Same as ID13
53	No implementation of diagnosing own status	C53.1 Failure, malfunction, or stoppage of the self-diagnostic function C53.2 Input information (information necessary for self-diagnosis) not obtained C53.3 Malware intrusion or hacking	Same as ID8	Same as ID8	1	5	6	Same as ID1	1	5	6	Same as ID1	Same as ID13

54	Too late/too early implementation of diagnosing own status	C54.1 Failure or malfunction of the self-diagnostic function C54.2 Malfunction of the self-diagnostic algorithm (self-diagnostic operation takes too much time) C54.3 Incorrect timing of obtaining input information (information required for self-diagnosis) C54.4 Malware intrusion or hacking	Same as ID9	Same as ID9	1	5	6	Same as ID1	1	5	6	Same as ID1	Same as ID13
Onboard crew														
55	Failure to go to the bridge based on instructions from the autonomous operation management system	C55.1 Failure to go to the bridge C55.2 Failure to go to the bridge due to lack of understanding of the need for going to the bridge or instructions from the system C55.3 Inability to grasp instructions due to inappropriate HMI, etc. C55.4 Restraint by other tasks	Same as ID49	• Transition to MRM/MRC if the crew does not respond after a certain period of time • Appropriate HMI design and verification	1	6	7	Same as ID1	1	5	6	Same as ID1	• Consider introducing a crew monitoring system and a system for preventing the crew from falling asleep • Verification of MRM/MRC coverage for various situations • Workload management for onboard crew members (limiting the work they can perform)

56	Too late to go to the bridge based on the instructions from the autonomous operation management system	C56.1 Going to the bridge is delayed and standby location is far away C56.2 Going to the bridge is delayed due to the too much required time to understand instructions due to inappropriate HMI, etc. C56.3 Instructions from the autonomous operation management system are too late C56.4 Takes time to release from other tasks	Same as ID49	• Appropriate HMI design and verification • Transition to MRM/MRC if the crew does not respond after a certain period of time • Verification of the algorithms for autonomous flight management systems to provide instructions at the appropriate time.	1	6	7	Same as ID1	1	6	7	Same as ID1	• Consider introducing a crew monitoring system and a system for preventing the crew from falling asleep • Verification of MRM/MRC coverage for various situations • Workload management for standby crew members (limiting the work they can perform) • Restrictions on the whereabouts of standby crews

57	Mistake in understanding the current situation	C57.1 HMI giving a wrong understanding of the current situation C57.2 The crew does not understand how to operate the system C57.3 Wrong information displayed due to system malfunction or failure C57.4 Misinterpretation of the displayed information C57.5 Distraction due to concurrent tasks and time pressure	E57.1 Manual steering based on incorrect understanding E57.2 Abnormal approach to other ships/objects or areas with grounding risk E57.3 Collision, stranding, capsizing, or sinking	• Appropriate HMI design and verification • training for the crew • Transition to MRM/MRC if the crew does not respond after a certain period of time	1	6	7	Same as ID1	1	5	6	Same as ID1	• Consideration of measures to improve system reliability (redundancy, etc.) (including cost–benefit study) • Verification of MRM/MRC coverage for various situations • Workload management in situations that call for the crew to go to the bridge (ensuring that the enough number of crew for the amount of tasks that may arise and replenishing resources by implementing automation that can be used when the crew is called)

58	No implementation of understanding the current situation	C58.1 HMI with difficulty in understanding the current situation C58.2 The crew does not understand how to operate the system or cannot understand the current situation C58.3 System malfunction or failure prevents understanding the current situation C58.4 Forgetting due to concurrent tasks	E58.1_1 Autonomous steering outside the ODD E58.1_2 Manual steering based on incorrect understanding E58.2 Deviation from course E58.3 Abnormal approach to other ships/objects or areas with grounding risk E58.4 Collision, stranding, capsizing, or sinking	Same as ID57	1	5	6	Same as ID1	1	5	6	Same as ID1	Same as ID57

59	Too late to understand the current situation	C59.1 HMI that is difficult to operate or HMI that makes it difficult to understand the current situation and thus takes time to understand the current situation C59.2 The crew does not understand how to operate the system, or it takes time to understand the current situation C59.3 Understanding the current situation takes time due to system malfunctions or failures C59.4 Insufficient resources due to concurrent tasks	E59.1 Autonomous steering outside the ODD E59.2 Deviation from course E59.3 Abnormal approach to other ships/objects or areas with grounding risk E59.4 Collision, stranding, capsizing, or sinking	Same as ID57	1	6	7	Same as ID1	1	5	6	Same as ID1	Same as ID57
60	Error in switching the steering mode based on instructions from the system	C60.1 Failure or malfunction of the ship steering mode switching function C60.2 The crew is not familiar with the procedure C60.3 Distraction or time pressure due to concurrent tasks	Same as ID49	• Alarm for each system failure • Advance training for the crew • Preparation of manuals on how to switch the steering mode	1	6	7	Same as ID1	1	5	6	Same as ID1	Same as ID57

61	Failure to switch the steering mode based on instructions from the system	C61.1 Failure to go to the bridge C61.2 Insufficient understanding of the need for the ship steering mode switching operation C61.3 HMI finding it difficult to understand the ship steering mode C61.4 Failure or malfunction of the ship steering mode switching function C61.5 Ship operation mode switching instruction not activated C61.6 Forgetting due to concurrent tasks	Same as ID49	• Alarm for each system failure • Alarm activated when a certain amount of time is exceeded • Preparation of manuals to improve crews' understanding of the system • Appropriate HMI design and verification	1	5	6	Same as ID1	1	5	6	Same as ID1	Same as ID57

62	Too late/too early to implement switching of the steering mode based on instruction from the system	C62.1 Insufficient understanding of the operation method C62.2 HMI finding it difficult to understand the necessity of switching the ship steering mode, thus taking time to switch C62.3 Failure or malfunction of the ship steering mode switching function C62.4 Too late issuance of the ship steering mode switching instruction C62.5 Lack of resources due to concurrent tasks	Same as ID49	Same as ID61	1	6	7	Same as ID1	1	5	6	Same as ID1	Same as ID57

63	Mistakes in manual steering	C63.1 Failure or malfunction of the manual ship steering system C63.2 The crew does not understand how to operate the manual ship steering system C63.3 Misjudgment of other ships' movements C63.4 The crew is not proficient in manual ship steering C63.5 The crew has relied on automatic ship steering for a long time and their manual ship steering skills are deteriorating C63.6 Distraction or time pressure due to concurrent tasks	E63.1 Manual steering different from crew's intention E63.2 Abnormal approach to other ships/objects or areas with grounding risk E63.3 Collision, stranding, capsizing, or sinking	• Redundancy of the manual steering system • Training for the crew	1	6	7	Same as ID1	1	6	7	Same as ID1	• Inspection of the manual steering system • Appropriate HMI design for the manual steering system • Workload management in situations that call for the crew to the bridge (ensuring that the enough number of crew for the amount of tasks that may arise and replenishing resources by implementing automation that can be used when the crew is called)

64	No implementation of manual steering	C64.1 Failure or malfunction of the manual ship steering system C64.2 The crew does not understand how to operate the manual ship steering system C64.3 Switching to manual steering not performed C64.4 Forgetting due to concurrent tasks	E64.1 Operation not based on manual or autonomous steering E64.2 Abnormal approach to other ships/objects or areas with grounding risk E64.3 Collision, stranding, capsizing, or sinking	Same as ID63	1	6	7	Same as ID1	1	5	6	Same as ID1	Same as ID63
65	Too late/too early execution of manual steering	C65.1 Failure or malfunction of the manual ship steering system C65.2 The crew does not understand how to operate the manual ship steering system C65.3 Misjudgment of other ships' movements C65.4 Delay in switching to manual ship steering C65.5 Lack of resources due to concurrent tasks	E65.1 Incorrect steering E65.2 Abnormal approach to other ships/objects or areas with grounding risk E65.3 Collision, stranding, capsizing, or sinking	Same as ID63	1	6	7	Same as ID1	1	6	7	Same as ID1	Same as ID63
Shadow crew														

66	Errors in constant monitoring of each system and surrounding situations	C66.1 HMI gives a false understanding of the current situation C66.2 Shadow crew does not understand how to operate the system C66.3 Wrong information displayed due to system malfunction or failure C66.4 Distraction due to other tasks and time pressure	Same as ID1	NA	1	6	7	• Preparation of the manual on how to operate each system • training of the shadow crew • Appropriate HMI design and verification •Alarm for each system failure • Manufacturer's engineers onboard the ship during demonstration • Workload management of the shadow crew (ensuring the enough number of the shadow crews for the amount of tasks and replenishing resources by introducing available automation)	1	5	6	Same as ID1	NA

67	No implementation of constant monitoring of each system and surrounding situations	C67.1 HMI finding it difficult to understand the current situation C67.2 The shadow crew does not understand how to operate the system or cannot understand the current situation C67.3 System malfunction or failure prevents understanding the current situation C67.4 Shadow crew's sudden illness, napping, or engaging in other tasks, among other factors	Same as ID1	NA	1	5	6	Same as ID66	1	4	5	Same as ID1	NA

68	Too late/too early implementation of constant monitoring of each system and surrounding situations	C68.1 HMI finding it difficult to operate or HMI finds it difficult to understand the current situation and thus takes time to understand the current situation C68.2 The shadow crew does not understand how to operate the system, and it takes time to understand the current situation C68.3 Understanding the current situation takes time due to system malfunctions and failures C68.4 Shadow crew's sudden illness, napping, or engaging in other tasks, among other factors	Same as ID1	NA	1	6	7	Same as ID66	1	5	6	Same as ID1	NA

69	Error in emergency response (forced switchover to manual steering)	C69.1 Failure of the ship steering mode switching function C69.2 The shadow crew is not familiar with the ship steering mode switching method C69.3 Distraction due to other tasks and time pressure	Same as ID1	NA	1	7	8	• Preparation of the manual on how to switch the steering mode • Advance training of the shadow crew • Workload management of the shadow crew (ensuring the enough number of the shadow crews for the amount of tasks and replenishing resources by introducing available automation)	1	6	7	Same as ID1	NA

70	Failure to implement the emergency response (forced switchover to manual steering)	C70.1 Overconfidence in the autonomous ship steering system C70.2 The shadow crew does not understand that the current situation is an emergency (misperception of their own ship's performance or current information on their ship/surrounding/environment, etc.). C70.3 The shadow crew does not respond thinking that the onboard crew will respond C70.4 The shadow crew is not familiar with how to switch the ship steering mode C70.5 The shadow crew's sudden illness, napping, or engaging in other tasks, among other factors	Same as ID1	NA	1	6	7	Same as ID69	1	5	6	Same as ID1 * Ensure that the shadow crew respond if they sense even the slightest danger without expecting the onboard crew to respond	NA

71	Too late/too early to implement emergency response (forced switchover to manual steering)	C71.1 Malfunction of the ship steering mode switching function C71.2 The shadow crew is not familiar with the ship steering mode switching method C71.3 The shadow crew is late in responding because they think the regular crew will respond C71.4 Shadow crew's sudden illness, napping, or engaging in other tasks, among other factors	Same as ID1	NA	1	7	8	Same as ID69	1	6	7	Same as ID1 * Ensure that the shadow crew respond if they sense even the slightest danger without expecting the onboard crew to respond	NA

Table 2.8 HAZID WS (Phase: Berthing/unberthing)

Sheet ID: 2
Phase: Berthing/unberthing

ID	Hazard	Causes	Consequences	Existing Safeguards	Index(only existing safeguards)			Safeguards at Trial	Index(Include safeguards at trial)			Emergency Plan	Comments (safety measures for commercial operation, etc.)
					SI	FI	RI		SI	FI	RI		
自律操船システム													
1	Error in establishing the action plan for berthing/ unberthing	C1.1 Input information not obtained or incorrect (information on own ship, other ships and drifting objects, marine weather, target positions of berthing/ unberthing, etc.) C1.2 Voyage plan (given) not obtained or incorrect C1.3 Faulty algorithm for establishing the ship action plan for berthing/ unberthing in the autonomous ship steering system C1.4 Failure or malfunction of the autonomous ship steering system C1.5 Malware infiltration or hacking	E1.1 Abnormal approach to the berth, other ships/objects, or areas with grounding risk E1.2 Collision, contact, grounding, capsizing, and sinking	• Alarm for each system failure • Alarm when various information and voyage plans are not entered • Double-checking when entering voyage plans • Alarm when jumping position of own ship or other ships/drifts • Prior verification by simulations of berthing/ unberthing action planning algorithms • Connect only to removable media with no viruses detected by virus detection software as well as no connection to external networks	2	5	7	• Constant monitoring by the shadow crews • Takeover by the shadow crews • training of the shadow crews regarding switching to the ship steering mode, etc. • Terminate experiments in case of malfunctions or abnormalities.	2	5	7	(1) Activate alarm in case of failure or abnormality. Moreover, abnormality or failure is detected through constant monitoring by the shadow crews. (2) Switch to manual steering at the discretion of the shadow crews. *If necessary, prepare details of the emergency plan separately	• Improvement of the berthing/ unberthing action planning algorithm • Consideration of measures to improve system reliability (redundancy, etc.) (including cost–benefit study) • Verification of outputs and introduction of functions to deal with the verification results (implemented by human or machine, depending on the level of automation)

2	No implementation of the berthing/ unberthing action plan	C2.1 Input information not obtained (information on own ship, other ships and drifting objects, marine weather, target position of berthing/ unberthing, etc.) C2.2 Voyage plan (given) not obtained C2.3 Failure or malfunction of the autonomous ship steering system C2.4 Malware intrusion or hacking C2.5 Failure to receive inquiry (trigger for activating this function)	Same as ID1	• Alarm for each system failure • Alarm when various information and voyage plans are not entered • Alarm when a certain amount of time has elapsed • Pre verification through simulations • Connect only to removable media with no viruses detected by virus detection software as well as no connection to external networks	2	4	6	Same as ID1	2	4	6	Same as ID1	• Consideration of measures to improve system reliability (redundancy, etc.) (including cost-benefit study) • If there is no response, the inquiry source shall be made to ask again with new input information. • Introduce a function to deal with no response even after re querying (implemented by human or machine, depending on the level of automation)

3	Too late/too early implementation of the berthing/ unberthing action plan	C3.1 Input information not obtained or obtained at the wrong time (information on own ship, other ships and drifting objects, marine weather, target positions of berthing/ unberthing, etc.) C3.2 Failure of the autonomous ship steering system's berthing/ unberthing action planning algorithm (too much time is spent on calculations for berthing/ unberthing action planning) C3.3 Failure or malfunction of the autonomous ship steering system C3.4 Malware infiltration or hacking C3.5 Wrong timing of inquiry (trigger for activation of this	Same as ID1	Same as ID2	2	5	7	Same as ID1	2	5	7	Same as ID1	• Consideration of measures to improve system reliability (redundancy, etc.) (including cost–benefit study) • If the response is too late, the inquiry source shall be made to ask again with new input information. • Introduce a function to deal with cases where a response is not received in time (implemented by human or machine, depending on the level of automation)

4	Error in the switching operation phase (unberthing phase to normal navigation phase)	C4.1 Incorrect input of the (given) position to switch the operation phase C4.2 Incorrect input information (own ship's position information) C4.3 Failure or malfunction of the autonomous ship steering system C4.4 Malware intrusion or hacking	E4.1 Deviation from course E4.2 Abnormal approach to other ships/objects, berth, or areas with grounding risk E4.3 Collision with other ships or berth, grounding, and capsizing or sinking	• Alarm for each system failure • Double check when inputting the operation phase switching position • Alarm at the time of position jump of own ship • Alarm at the time of route deviation • Pre verification through simulations • Connect only to removable media with no viruses detected by virus detection software as well as no connection to external networks	2	5	7	Same as ID1	2	5	7	Same as ID1	• Consideration of measures to improve system reliability (redundancy, etc.) (including cost-benefit study)

5	No changeover of the operation phase (unberthing phase to normal navigation phase)	C5.1 Incorrect input of the (given) position to switch the operation phase C5.2 Incorrect input or no input of input information (own ship's position information) C5.3 Failure or malfunction of the autonomous ship steering system C5.4 Malware intrusion or hacking C5.5 Failure to receive inquiry (trigger for activating this function)	Same as ID4	• Alarm for each system failure • Double check when inputting the operation phase switching position • Alarm at the time of position jump of own ship • Alarm at the time of route deviation • Pre verification through simulations • Activate alarm when a certain distance from the operation phase switching position is exceeded • Connect only to removable media with no viruses detected by virus detection software as well as no connection to	2	4	6	Same as ID1	2	4	6	Same as ID1	Same as ID2

6	Too late/too early to implement switching the operation phases (unberthing phase to normal navigation phase)	C6.1 Wrong timing of obtaining input information (own ship's position) C6.2 Malfunction of the operation phase switching algorithm (switching operation takes too long) C6.3 Failure or malfunction of the autonomous ship steering system C6.4 Malware intrusion or hacking C6.5 Wrong timing of inquiry (trigger for activating this function)	Same as ID4	• System failure alarm • Alarm at the time of route deviation • Pre verification through simulations • Activate alarm when a certain distance from the operation phase switching position is exceeded • Connect only to removable media with no viruses detected by virus detection software as well as no connection to external networks	2	5	7	Same as ID1	2	5	7	Same as ID1	Same as ID3
7	Error in diagnosis of own status	C7.1 Wrong algorithm for the self-diagnostic function of the autonomous ship steering system C7.2 Incorrect input information (information required for self-diagnosis) C7.3 Malware intrusion or hacking	• Misdiagnose as normal when abnormal → Same as ID4 • Misdiagnose as abnormal when normal → Switch to manual steering based on alarm	• Pre verification of the self-diagnostic function • Connect only to removable media with no viruses detected by virus detection software as well as no connection to external networks	2	5	7	Same as ID1	2	5	7	Same as ID1	Same as ID4

8	No implementation of the diagnosis of own ship's status	C8.1 Failure, malfunction, or stoppage of the self-diagnostic function of the autonomous ship steering system C8.2 Input information (information necessary for self-diagnosis) not obtained C8.3 Malware intrusion or hacking	• Diagnosis not performed when normal → No problem (alarm will be activated when a certain period of time is exceeded) • Diagnosis not performed when abnormal → Same as ID4	• Pre verification of the self-diagnostic function • Alarm activated when a certain amount of time is exceeded • Connect only to removable media with no viruses detected by virus detection software as well as no connection to external networks	2	4	6	Same as ID1	2	4	6	Same as ID1	Same as ID4

9	Too late/too early to implement the diagnosis of own status	C9.1 Failure or malfunction of the self-diagnostic function of the autonomous ship steering system C9.2 Malfunction of the self-diagnostic algorithm of the autonomous ship steering system (self-diagnostic operation takes too much time) C9.3 Incorrect timing for obtaining input information (information necessary for self-diagnosis) C9.4 Malware intrusion or hacking	• Too late to diagnose when normal → No problem (alarm will be activated when a certain period of time is exceeded) • Too late to diagnose as abnormal when abnormal → E9.1 Delay in switching to the manual operation E9.2 Autonomous operation outside ODD E9.3 Abnormal approach to berth, other ships/objects, or areas with grounding risk E9.4 Collision, contact, grounding, capsizing, or	Same as ID8	2	5	7	Same as ID1	2	5	7	Same as ID1	Same as ID4
Information integration system for own ship														

10	Error in integration of own ship information	C10.1 Inconsistency in input information (e.g., different data between sensors of own ship, integration with old information, etc.) C10.2 Failure or malfunction of the information integration function and, error in the integration algorithm C10.3 Malware intrusion or hacking	E10.1 Establishment of the incorrect action plan for berthing/ unberthing E10.2 Incorrect calculation of the control variables E10.3 Incorrect/no switching of the operation phase E10.4 Deviation from course E10.5 Abnormal approach to other ships/objects, berth, or areas with grounding risk E10.6 Collision, grounding, capsizing, or	• Advance verification of the information integration function • Integrating a method for dealing with discrepancies in data (which data should be prioritized) • Alarm for each system failure • Warnings when the same type of data differs • Connect only to removable media with no viruses detected by virus detection software as well as no connection to external networks	2	4	6	Same as ID1	2	4	6	Same as ID1	• Consideration of measures to improve system reliability (redundancy, etc.) (including cost-benefit study) • Improvement of the information integration algorithm • Management of the reliability of integrated information (reliability evaluation and formulation of countermeasures in case of low reliability)

11	No implementation of integrating information of own ship	C11.1 Inconsistency in input information (different data between sensors of own ship) C11.2 Failure or malfunction of the information integration function and error in the integration algorithm C11.3 Malware intrusion or hacking C11.4 Failure to receive inquiry (trigger for activating this function)	Same as ID10	• Advance verification of the information integration function • Incorporating a method for dealing with discrepancies in data (which data should be prioritized) • Alarm for each system failure • Warnings when the same type of data differs • Alarm activated when a certain amount of time is exceeded • Connect only to removable media with no viruses detected by virus detection software as well as no connection to	2	4	6	Same as ID1	2	4	6	Same as ID1	• Consideration of measures to improve system reliability (redundancy, etc.) (including cost-benefit study) • Improvement of the information integration algorithm • Introduce a function to deal with the absence of outputs (e.g., restarting the system in question; prepared separately from diagnosis of own to deal with the case of a stoppage of functionality)

12	Too late/too early to implement integrating own ship information	C12.1 Malfunction of the information integration function/algorithm (information integration takes too much time) C12.2 Wrong timing of information acquisition from different sensors C12.3 Malware intrusion or hacking C12.4 Wrong timing of inquiry (trigger for activating this function)	E12.1 Establishment of the incorrect action plan for beathing/ unberthing E12.2 Incorrect calculation of the control variables E12.3 Switch the operation phase at wrong position E12.4 Deviation from course E12.5 Abnormal approach to other ships/objects, berth, or areas with grounding risk E12.6 Collision, grounding, capsizing, or sinking	Same as ID11	2	4	6	Same as ID1	2	4	6	Same as ID1	• Consideration of measures to improve system reliability (redundancy, etc.) (including cost–benefit study) • Improvement of the information integration algorithm • Introduce a function to deal with large delays in output (e.g., restarting the system in question).
13	Error in the diagnosis of own status	C13.1 Failure or malfunction of the self-diagnostic function C13.2 Wrong algorithm for the self-diagnostic function C13.3 Incorrect input information (information required for self-diagnosis) C13.4 Malware intrusion or hacking	Same as ID7	Same as ID7	2	5	7	Same as ID1	2	5	7	Same as ID1	• Improvements in algorithm for self-diagnostic function

14	No implementation of the diagnosis of own status	C14.1 Failure, malfunction, or stoppage of the self-diagnostic function C14.2 Input information (information necessary for self-diagnosis) not obtained C14.3 Malware intrusion or hacking	Same as ID8	Same as ID8	2	4	6	Same as ID1	2	4	6	Same as ID1	Same as ID13
15	Too late/too early to implement the diagnosis of own status	C15.1 Failure or malfunction of the self-diagnostic function C15.2 Malfunction of the self-diagnostic algorithm (self-diagnostic operation takes too much time) C15.3 Incorrect timing for obtaining input information (information required for self-diagnosis) C15.4 Malware intrusion or hacking	Same as ID9	Same as ID9	2	5	7	Same as ID1	2	5	7	Same as ID1	Same as ID13

16	Error in diagnosing sensor status	C16.1 Failure or malfunction of the status diagnostic function for the sensor C16.2 Wrong algorithm for the status diagnostic function for the sensors of own ship C16.3 Incorrect input information (information required for sensor status diagnosis) C16.4 Malware intrusion or hacking	• Misdiagnose as normal when abnormal → Same as ID10 • Misdiagnose as abnormal when normal → Switch to manual steering based on alarm	• Pre verification of the status diagnostic function and algorithm for the sensor • Connect only to removable media with no viruses detected by virus detection software as well as no connection to external networks	2	5	7	Same as ID1	2	5	7	Same as ID1	• Improvements in algorithm for the diagnostic function of the sensor status
17	No implementation of the diagnosis of sensor status	C17.1 Failure or malfunction of the status diagnostic function for the sensors of own ship C17.2 Input information (information necessary for sensor status diagnosis) not obtained C17.3 Malware intrusion or hacking	• Diagnosis not performed when abnormal → Same as ID10 • Diagnosis not performed when normal → No problem (alarm will be activated when a certain period of time is exceeded)	• Pre verification of the status diagnostic function for the sensors • Alarm activated when a certain amount of time is exceeded • Connect only to removable media with no viruses detected by virus detection software as well as no connection to external networks	2	4	6	Same as ID1	2	4	6	Same as ID1	Same as ID16

18	Too late/too early to implement the diagnosis of sensor status	C18.1 Failure or malfunction of the status diagnostic function for the sensors of own ship C18.2 Malfunction of the sensor status diagnosis algorithm (status diagnosis operation takes too much time) C18.3 Wrong timing of obtaining input information (information required for sensor status diagnosis) C18.4 Malware intrusion or hacking	• Too late to diagnose as normal when normal → No problem (alarm will be activated when a certain period of time is exceeded) • Too late to diagnose as abnormal when abnormal → Same as ID12	• Pre verification of the status diagnostic function and algorithm for the sensors • Alarm activated when a certain amount of time is exceeded • Connect only to removable media with no viruses detected by virus detection software as well as no connection to external networks	2	5	7	Same as ID1	2	5	7	Same as ID1	Same as ID16
Measuring system for the distance from the berth													
19	Error in measuring the distance to the berth from own ship	C19.1 Failure or malfunction of the sensors for measuring the distance to the berth C19.2 Failure or malfunction of the system for measuring the distance to the berth C19.3 Communication failure or malfunction between the distance sensor and the measurement system C19.4 Malware intrusion or hacking	E19.1 Abnormal approach to the berth E19.2 Collision with the berth	• Alarm for each system failure • Connect only to removable media with no viruses detected by virus detection software as well as no connection to external networks	2	4	6	Same as ID1	2	4	6	Same as ID1	• Consideration of measures to improve the reliability sensor and system (redundancy, etc.) (including cost–benefit study)

20	No implementation of measuring the distance to the berth	Same as ID19	Same as ID19	Same as ID19	2	4	6	Same as ID1	2	4	6	Same as ID1	Same as ID19
21	Too late/too early to implement the measurement of the distance to the berth	Same as ID19	Same as ID19	Same as ID19	2	4	6	Same as ID1	2	4	6	Same as ID1	Same as ID19
22	Error in activating the close-proximity alarm	C22.1 Failure or malfunction of the system for measuring the distance to the berth C22.2 Error in the alarm activating algorithm of the system for measuring the distance to the berth C22.3 Wrong input information (information necessary for alarm activating decisions) C22.4 Malware intrusion or hacking	E22.1 Alarm activated but not actually close (see ID 23 and 24 when alarm not activated but the berth is actually close)	Same as ID19	2	4	6	Same as ID1	2	4	6	Same as ID1	• Consideration of measures to improve system reliability (redundancy, etc.) (including cost–benefit study) • Improvement of the alarm activating algorithm

23	No implementation of activating close-proximity alarm	Same as ID22	(Alarm not activated but the berth is actually close) E23.1 Delay or failure in switching the ship steering mode E23.2 Abnormal approach to the berth E23.3 Collision with the berth	Same as ID19	2	4	6	Same as ID1	2	4	6	Same as ID1	Same as ID22
24	Too late/too early to activate close-proximity alarm	C24.1 Failure or malfunction of the system for measuring the distance to the berth C24.2 Malfunction of the alarm activating algorithm for measuring the distance to the berth (calculating the decision to activate the alarm takes too much time) C24.3 Wrong timing of obtaining input information (information required to make alarm activating decision) C24.4 Malware intrusion or hacking	(Alarm delayed when the berth is actually close) E24.1 Delay or failure in switching the ship steering mode E24.2 Abnormal approach to the berth E24.3 Collision with the berth	• Verification of appropriate timing for activating the alarm • Alarm for each system failure • Connect only to removable media with no viruses detected by virus detection software as well as no connection to external networks	2	4	6	Same as ID1	2	4	6	Same as ID1	Same as ID22

25	Error in diagnosis of own status	C25.1 Failure or malfunction of the self-diagnostic function C25.2 Wrong algorithm for the self-diagnostic function C25.3 Incorrect input information (information required for self-diagnosis) C25.4 Malware intrusion or hacking	Same as ID7	Same as ID7	2	5	7	Same as ID1	2	5	7	Same as ID1	Same as ID13
26	No implementation of diagnosis of own status	C26.1 Failure or malfunction of the self-diagnostic function C26.2 Input information (information necessary for self-diagnosis) not obtained C26.3 Malware intrusion or hacking	Same as ID8	Same as ID8	2	4	6	Same as ID1	2	4	6	Same as ID1	Same as ID13
27	Too late/too early to implement diagnosis of own status	C27.1 Failure or malfunction of the self-diagnostic C27.2 Malfunction of the self-diagnostic algorithm of the system (self-diagnostic operation takes too much time) C27.3 Incorrect timing of obtaining input information (information required for self-diagnosis) C27.4 Malware intrusion or hacking	Same as ID9	Same as ID9	2	5	7	Same as ID1	2	5	7	Same as ID1	Same as ID13

28	Error in diagnosing sensor status	C28.1 Failure or malfunction of the status diagnostic function for the sensors C28.2 Wrong algorithm for the status diagnostic function for the sensors C28.3 Incorrect input information (information required for sensor status diagnosis) C28.4 Malware intrusion or hacking	• Misdiagnose as normal when abnormal →Same as ID19 • Misdiagnose as abnormal when normal →Switch to manual steering based on alarm	Same as ID16	2	5	7	Same as ID1	2	5	7	Same as ID1	Same as ID16
29	No implementation of diagnosis of sensor status	C29.1 Failure of the status diagnostic function for the sensors C29.2 Input information (information required for sensor status diagnosis) not obtained C29.3 Malware intrusion or hacking	• Diagnosis not performed when abnormal → Same as ID19 • Diagnosis not performed when normal → No problem (alarm will be activated when a certain period of time is exceeded)	Same as ID17	2	4	6	Same as ID1	2	4	6	Same as ID1	Same as ID16

30	Too late/too early to implement diagnosis of sensor status	C30.1 Failure or malfunction of the status diagnostic function for the sensors C30.2 Malfunction of the sensor status diagnosis algorithm of the system (status diagnosis operation takes too much time) C30.3 Wrong timing of obtaining input information (information required for sensor status diagnosis) C30.4 Malware intrusion or hacking	• Too late diagnosis as normal when normal → No problem (alarm will be activated when a certain period of time is exceeded) • Too late diagnosis as abnormal when abnormal → Same as ID19	Same as ID18	2	5	7	Same as ID1	2	5	7	Same as ID1	Same as ID16
Information integration system for other ships and drifting objects													
31	Error in integration information of other ships and drifting objects	C31.1 Inconsistency in input information (e.g., different data between sensors, integration with old information) C31.2 Failure or malfunction of the information integration function as well as errors in the integration algorithm C31.3 Malware intrusion or hacking	E31.1 Establishment of the incorrect action plan berthing/ unberthing. E31.2 Abnormal approach to other ships/objects or areas with grounding risk E31.3 Collision, grounding, capsizing, or sinking	Same as ID10	2	4	6	Same as ID1	2	4	6	Same as ID1	Same as ID10

32	No implementation of integration information of other ships and drifting objects	C32.1 Inconsistency in input information (e.g., different data between sensors) C32.2 Failure or malfunction of the information integration function as well as errors in the integration algorithm C32.3 Malware intrusion or hacking C32.4 Failure to receive inquiry (trigger for activating this function)	Same as ID31	Same as ID11	2	4	6	Same as ID1	2	4	6	Same as ID1	Same as ID11
33	Too late/too early implementation of integration information of other ships and drifting objects	C33.1 Failure of information integration function/algorithm (information integration takes too much time) C33.2 Wrong timing of information acquisition from different sensors C33.3 Malware intrusion or hacking C33.4 Wrong timing of inquiry (trigger for activation of this function)	Same as ID31	Same as ID11	2	4	6	Same as ID1	2	4	6	Same as ID1	Same as ID12

34	Error in diagnosing own status	C34.1 Failure or malfunction of the self-diagnostic function C34.2 Wrong algorithm for the self-diagnostic function C34.3 Incorrect input information (information necessary for self-diagnosis) C34.4 Malware intrusion or hacking	Same as ID7	Same as ID7	2	5	7	Same as ID1	2	5	7	Same as ID1	Same as ID13
35	No implementation of diagnosing own status	C35.1 Failure or malfunction of the self-diagnostic function C35.2 Input information (information necessary for self-diagnosis) not obtained C35.3 Malware intrusion or hacking	Same as ID8	Same as ID8	2	4	6	Same as ID1	2	4	6	Same as ID1	Same as ID13
36	Too late/too early implementation of diagnosing own status	C36.1 Failure or malfunction of the self-diagnostic function C36.2 Malfunction of the self-diagnostic algorithm (self-diagnostic operation takes too much time) C36.3 Wrong timing of obtaining input information (information required for self-diagnosis) C36.4 Malware intrusion or hacking	Same as ID9	Same as ID9	2	5	7	Same as ID1	2	5	7	Same as ID1	Same as ID13

37	Error in diagnosing sensor status	C37.1 Failure or malfunction of the status diagnostic function for the sensors C37.2 Wrong algorithm for the status diagnostic function for the sensors C37.3 Incorrect input information (information necessary for sensor status diagnosis) C37.4 Malware intrusion or hacking	• Misdiagnose as normal when abnormal → Same as ID31 • Misdiagnose as abnormal when normal → Switch to manual steering based on alarm	Same as ID16	2	5	7	Same as ID1	2	5	7	Same as ID1	Same as ID16
38	No implementation of diagnosing sensor status	C38.1 Failure or malfunction of the status diagnostic function for the sensors C38.2 Input information (information necessary for sensor status diagnosis) not obtained C38.3 Malware intrusion or hacking	• Diagnosis not performed when abnormal → Same as ID31 • Diagnosis not performed when normal → No problem (alarm will be activated when a certain period of time is exceeded)	Same as ID17	2	4	6	Same as ID1	2	4	6	Same as ID1	Same as ID16

39	Too late/too early implementation of diagnosing sensor status	C39.1 Failure or malfunction of the status diagnostic function for the sensors C39.2 Malfunction of the algorithm for the sensor status diagnosis (status diagnosis operation takes too much time) C39.3 Wrong timing of obtaining input information (information required for sensor status diagnosis) C39.4 Malware intrusion or hacking	• Too late diagnosis as normal when normal → No problem (alarm will be activated when a certain period of time is exceeded) • Too late diagnosis as abnormal when abnormal → Same as ID31	Same as ID18	2	5	7	Same as ID1	2	5	7	Same as ID1	Same as ID16
Information integration system for marine weather														
40	Error in integration of marine weather information	C40.1 Inconsistency in input information (e.g., different data between sensors, integration with old information) C40.2 Failure or malfunction of the information integration function as well as error in integration algorithm C40.3 Malware intrusion or hacking	Same as ID31	Same as ID10	2	4	6	Same as ID1	2	4	6	Same as ID1	Same as ID10

41	No implementation of integrating marine weather information	C41.1 Inconsistency in input information (e.g., different data between sensors) C41.2 Failure or malfunction of the information integration function as well as error in integration algorithm C41.3 Malware intrusion or hacking C41.4 Failure to receive inquiry (trigger for activating this function)	Same as ID31	Same as ID11	2	4	6	Same as ID1	2	4	6	Same as ID1	Same as ID11
42	Too late/too early implementation of integrating marine weather information	C42.1 Failure or malfunction of the information integration function/algorithm (information integration takes too much time) C42.2 Wrong timing of information acquisition from different sensors C42.3 Malware intrusion or hacking C42.4 Wrong timing of inquiry (trigger for activation of this function)	Same as ID31	Same as ID11	2	4	6	Same as ID1	2	4	6	Same as ID1	Same as ID12

43	Error in diagnosing own status	C43.1 Failure or malfunction of the self-diagnostic function C43.2 Wrong algorithm for the self-diagnostic function C43.3 Incorrect input information (information necessary for self-diagnosis) C43.4 Malware intrusion or hacking	Same as ID7	Same as ID7	2	5	7	Same as ID1	2	5	7	Same as ID1	Same as ID13
44	No implementation of diagnosing own status	C44.1 Failure or malfunction of the self-diagnostic function C44.2 Input information (information necessary for self-diagnosis) not obtained C44.3 Malware intrusion or hacking	Same as ID8	Same as ID8	2	4	6	Same as ID1	2	4	6	Same as ID1	Same as ID13
45	Too late/too early implementation of diagnosing own status	C45.1 Failure or malfunction of the self-diagnostic function C45.2 Malfunction of the self-diagnostic algorithm (self-diagnostic operation takes too much time) C45.3 Wrong timing of obtaining input information (information required for self-diagnosis) C45.4 Malware intrusion or hacking	Same as ID9	Same as ID9	2	5	7	Same as ID1	2	5	7	Same as ID1	Same as ID13

46	Error in diagnosing sensor status	C46.1 Failure or malfunction of the status diagnostic function for the sensors C46.2 Wrong algorithm for the status diagnostic function for the sensors C46.3 Incorrect input information (information necessary for sensor status diagnosis) C46.4 Malware intrusion or hacking	• Misdiagnose as normal when abnormal → Same as ID31 • Misdiagnose as abnormal when normal → Switch to manual steering based on alarm	Same as ID16	2	5	7	Same as ID1	2	5	7	Same as ID1	Same as ID16
47	No implementation of diagnosing sensor status	C47.1 Failure or malfunction of the status diagnostic function for the sensors C47.2 Input information (information necessary for sensor status diagnosis) not obtained C47.3 Malware intrusion or hacking	• Diagnosis not performed when abnormal → Same as ID31 • Diagnosis not performed when normal → No problem (alarm will be activated when a certain period of time is exceeded)	Same as ID17	2	4	6	Same as ID1	2	4	6	Same as ID1	Same as ID16

48	Too late/too early implementation of diagnosing sensor status	C48.1 Failure or malfunction of the status diagnostic function for the sensors C48.2 Malfunction of the algorithm for the sensor status diagnosis (status diagnosis operation takes too much time) C48.3 Wrong timing of obtaining input information (information required for sensor status diagnosis) C48.4 Malware intrusion or hacking	• Too late diagnosis as normal when normal → No problem (alarm will be activated when a certain period of time is exceeded) • Too late diagnosis as abnormal when abnormal → Same as ID31	Same as ID18	2	5	7	Same as ID1	2	5	7	Same as ID1	Same as ID16
Ship control system														
49	Error in calculation of the control variables based on the action plan for berthing/ unberthing	C49.1 Error in the action plan for berthing/ unberthing C49.2 Incorrect input information (information required for control variables calculation) C49.3 Error in the control variables calculation algorithm C49.3-2 Poor accuracy of the steering motion model of own ship C49.4 Failure or malfunction of the ship control system C49.5 Malware intrusion or hacking	E49.1 Deviation from course E49.2 Abnormal approach to other ships/objects or areas with grounding risk E49.3 Collision, grounding, capsizing, or sinking	• System failure alarm • Pre verification of the control variables calculation algorithm through simulations • Ensuring accuracy of the steering motion model of own ship • Connect only to removable media with no viruses detected by virus detection software as well as no connection to external networks	2	5	7	Same as ID1	2	5	7	Same as ID1	• Improvement of the control variables calculation algorithm • Consideration of measures to improve system reliability (redundancy, etc.) (including cost-benefit study)

50	No implementation of calculating the control variables based on the action plan for berthing/ unberthing	C50.1 Action plan for berthing/ unberthing not obtained C50.2 Input information (information required for control variables calculation) not obtained C50.3 Failure or malfunction of the ship control system C50.4 Malware intrusion or hacking C50.5 Failure to receive inquiry (trigger for activating this function)	Same as ID49	• System failure alarm • Alarm at the time when various information is not obtained • Pre verification through simulations • Alarm activated when a certain amount of time is exceeded • Connect only to removable media with no viruses detected by virus detection software as well as no connection to external networks	2	4	6	Same as ID1	2	4	6	Same as ID1	• Consideration of measures to improve system reliability (redundancy, etc.) (including cost–benefit study) • Introduction of mechanisms to verify ship behavior (e.g., watch for berthing speed) • If there is no response, the inquiry source shall be made to ask again with new input information. • Introduce a function to deal with no response even after re querying (implemented by human or machine, depending on

51	Too late/too early to implement control variables calculations based on the action plan for berthing/ unberthing	C51.1 Wrong timing of obtaining the action plan for berthing/ unberthing C51.2 Wrong timing of acquiring input information (information required for control variables calculation) C51.3 Malfunction in the control variables calculation algorithm (excessive time required for control variables calculation) C51.4 Failure or malfunction in the ship control system C51.5 Malware intrusion C51.6 Wrong timing of inquiry (trigger for activation of this	Same as ID49	• System failure alarm • Pre verification through simulations • Warning activated when a certain period of time has elapsed • Alarm activated when a certain amount of time is exceeded • Connect only to removable media with no viruses detected by virus detection software as well as no connection to external networks	2	5	7	Same as ID1	2	5	7	Same as ID1	• Consideration of measures to improve system reliability (redundancy, etc.) (including cost–benefit study) • Introduction of mechanisms to verify behavior (e.g., watch for berthing speed) • If the response is too late, the inquiry source shall be made to ask again with new input information. • Introduce a function to deal with cases where a response is not received in time (implemented by human or machine, depending on the level of automation)

52	Error in control of the rudder or engine	C52.1 Error in control variables calculation C52.2 Actuator malfunction or failure	E52.1 Unable to navigate E52.2 Deviation from course E52.3 Abnormal approach to other ships/objects, or areas with grounding risk E52.4 Collision, grounding, capsizing, or sinking	• Pre verification of the system • Alarms in case of actuator failure or malfunction	2	4	6	Same as ID1	2	4	6	Same as ID1	• Consideration of measures to improve reliability (redundancy, etc.) (including cost-benefit study) • Introduction of a function to deal with incorrect rudder/engine status (e.g., restarting the system in question)
53	No implementation of control of the rudder or engine	C53.1 Input information (control variables) not obtained C53.2 Malfunction or failure of the actuator C53.3 Failure to receive inquiry (trigger for activating this function)	Same as ID52	• Alarms in case of actuator failure or malfunction • Alarm when control variables not obtained • Alarm activated when a certain amount of time is exceeded	2	4	6	Same as ID1	2	4	6	Same as ID1	• Consideration of measures to improve reliability (redundancy, etc.) (including cost-benefit study) • Introduction of a function to deal with cases where the rudder/engine is not under control (e.g., restarting the system in question) • If there is no response, the inquiry source shall be made to ask again with new input information. • Introduce a function to deal with no response even after re querying (implemented by human or machine, depending on

54	Too late/too early to implement controlling the rudder or engine	C54.1 Wrong timing of obtaining input information (control variables) C54.2 Malfunction or failure of the actuator C54.3 Wrong timing of inquiry (trigger for activation of this function)	Same as ID52	Same as ID53	2	4	6	Same as ID1	2	4	6	Same as ID1	• Consideration of measures to improve reliability (redundancy, etc.) (including cost–benefit study) • Introduction of a function to deal with rudder/engine control delays exceeding a certain level (e.g., restarting the system in question). • If the response is too late, the inquiry source shall be made to ask again with new input information. • Introduce a function to deal with cases where a response is not received in time (implemented by human or machine, depending on the level of automation)

55	Error in diagnosis of rudder/engine conditions	C55.1 Failure or malfunction of the rudder/engine condition diagnostic function C55.2 Wrong algorithm for the rudder/engine condition diagnostic function C55.3 Incorrect input information (information required for rudder/engine condition diagnosis) C55.4 Malware	Same as ID7	Same as ID7	2	5	7	Same as ID1	2	5	7	Same as ID1	• Improved algorithms for rudder/engine condition diagnostic functions
56	No implementation of diagnosis of rudder/engine conditions	C56.1 Failure or malfunction of the rudder/engine condition diagnostic function C56.2 Input information (information required for rudder/engine condition diagnosis) not obtained C56.3 Malware	Same as ID8	Same as ID8	2	4	6	Same as ID1	2	4	6	Same as ID1	Same as ID55

57	Too late/too early to implement diagnosis of rudder/engine conditions	C57.1 Failure or malfunction of the rudder/engine condition diagnostic function C57.2 Malfunction of the rudder/engine condition diagnostic algorithm (self-diagnostic operation takes too much time) C57.3 Wrong timing of obtaining input information (information required for rudder/engine condition diagnosis)	Same as ID9	Same as ID9	2	5	7	Same as ID1	2	5	7	Same as ID1	Same as ID55
58	Error in diagnosing own status	C58.1 Failure or malfunction of the self-diagnostic function C58.2 Wrong algorithm for the self-diagnostic function C58.3 Incorrect input information (information required for self-diagnosis) C58.4 Malware intrusion or hacking	Same as ID7	Same as ID7	2	5	7	Same as ID1	2	5	7	Same as ID1	Same as ID13

59	No implementation of diagnosing own status	C59.1 Failure, malfunction, or stoppage of the self-diagnostic function C59.2 Input information (information necessary for self-diagnosis) not obtained C59.3 Malware intrusion or hacking	Same as ID8	Same as ID8	2	4	6	Same as ID1	2	4	6	Same as ID1	Same as ID13
60	Too late/too early implementation of diagnosing own status	C60.1 Failure or malfunction of the self-diagnostic function C60.2 Malfunction of the self-diagnostic algorithm (self-diagnostic operation takes too much time) C60.3 Incorrect timing of obtaining input information (information required for self-diagnosis) C60.4 Malware intrusion or hacking	Same as ID9	Same as ID9	2	5	7	Same as ID1	2	5	7	Same as ID1	Same as ID13
Autonomous Operation Management System													

61	Error in instructions for switching the ship steering mode	C61.1 Failure or malfunction of the autonomous operation management system C61.2 Error in the algorithm to switch the operation mode C61.3 Error in input information (information required for making the operation mode switching decision) C61.4 Malware intrusion or hacking	E61.1 Autonomous steering for berthing/ unberthing outside ODD E61.2 Deviation from course E61.3 Abnormal approach to other ships/objects or areas with grounding risk E61.4 Collision, stranding, capsizing or sinking	• Alarm for each system failure • Double-checking at the time of ODD input • Alarm at the time of route deviation • Prior verification of the instruction function to switch the ship steering mode through simulations • Connect only to removable media with no viruses detected by virus detection software as well as no connection to external networks	2	5	7	Same as ID1	2	5	7	Same as ID1	• Improvement of the ship steering mode switching algorithm • Consideration of measures to improve system reliability (redundancy, etc.) (including cost-benefit study)

62	No implementation of the ship steering mode switching instructions	C62.1 Failure or malfunction of the autonomous operation management system C62.2 Error in the algorithm to switch the operation mode C62.3 Error in input information (information required for making the operation mode switching decision) C62.4 Malware intrusion or hacking C62.5 Failure to receive inquiry (trigger for activating this function)	Same as ID61	• Alarm for each system failure • Alarm activated when a certain amount of time is exceeded • Double-checking at the time of ODD input • Alarm at the time of route deviation • Prior verification of the instruction function to switch the ship steering mode through simulations • Connect only to removable media with no viruses detected by virus detection software as well as no connection to	2	4	6	Same as ID1	2	4	6	Same as ID1	Same as ID2

63	Too late/too early to give the ship steering mode switching instructions	C63.1 Failure or malfunction of the autonomous operation management system C63.2 Malfunction of the algorithm to switch the operation mode (calculating the decision to switch the operation mode takes too much time) C63.3 Wrong timing of obtaining input information (information necessary to decide whether to switch the operation mode) C63.4 Malware infiltration or hacking C63.5 Wrong timing of inquiry (trigger for activation of this	Same as ID61	Same as ID62	2	5	7	Same as ID1	2	5	7	Same as ID1	Same as ID3
64	Error in diagnosing own status	C64.1 Failure or malfunction of the self-diagnostic function C64.2 Wrong algorithm for the self-diagnostic function C64.3 Incorrect input information (information required for self-diagnosis) C64.4 Malware intrusion or hacking	Same as ID7	Same as ID7	2	5	7	Same as ID1	2	5	7	Same as ID1	Same as ID13

65	No implementation of diagnosing own status	C65.1 Failure, malfunction, or stoppage of the self-diagnostic function C65.2 Input information (information necessary for self-diagnosis) not obtained C65.3 Malware intrusion or hacking	Same as ID8	Same as ID8	2	4	6	Same as ID1	2	4	6	Same as ID1	Same as ID13
66	Too late/too early implementation of diagnosing own status	C66.1 Failure or malfunction of the self-diagnostic function C66.2 Malfunction of the self-diagnostic algorithm (self-diagnostic operation takes too much time) C66.3 Incorrect timing of obtaining input information (information required for self-diagnosis) C66.4 Malware intrusion or hacking	Same as ID9	Same as ID9	2	5	7	Same as ID1	2	5	7	Same as ID1	Same as ID13
Onboard crew													

67	Failure to go to the bridge based on instructions from the autonomous operation management system	C67.1 Failure to go to the bridge C67.2 Failure to go to the bridge due to lack of understanding of the need for going to the bridge or instructions from the system C67.3 Inability to grasp instructions due to inappropriate HMI, etc. C67.4 Restraint by other tasks	Same as ID61	• Transition to MRM/MRC if the crew does not respond after a certain period of time • Appropriate HMI design and verification	2	5	7	Same as ID1	2	5	7	Same as ID1	• Consider introducing a crew monitoring system and a system for preventing the crew from falling asleep • Verification of MRM/MRC coverage for various situations • Workload management for onboard crew members (limiting the work they can perform)
68	Too late/too early to go to the bridge based on the instructions from the autonomous operation management system	C68.1 Going to the bridge is delayed and standby location is far away C68.2 Going to the bridge is delayed due to the too much required time to understand instructions due to inappropriate HMI, etc. C68.3 Instructions from the autonomous operation management system are too late C68.4 Takes time to release from other tasks	Same as ID61	• Appropriate HMI design and verification • Transition to MRM/MRC if the crew does not respond after a certain period of time • Verification of the algorithms for autonomous flight management systems to provide instructions at the appropriate time.	2	6	8	Same as ID1	2	5	7	Same as ID1	• Consider introducing a crew monitoring system and a system for preventing the crew from falling asleep • Verification of MRM/MRC coverage for various situations • Workload management for standby crew members (limiting the work they can perform) • Restrictions on the whereabouts of standby crews

69	Mistake in understanding the current situation	C69.1 HMI giving a wrong understanding of the current situation C69.2 The crew does not understand how to operate the system C69.3 Wrong information displayed due to system malfunction or failure C69.4 Misinterpretation of the displayed information C69.5 Distraction due to concurrent tasks and time pressure	E69.1 Manual steering based on incorrect understanding E69.2 Abnormal approach to other ships/objects or areas with grounding risk E69.3 Collision, stranding, capsizing, or sinking	• Appropriate HMI design and verification • training for the crew • Transition to MRM/MRC if the crew does not respond after a certain period of time	2	5	7	Same as ID1	2	5	7	Same as ID1	• Consideration of measures to improve system reliability (redundancy, etc.) (including cost–benefit study) • Verification of MRM/MRC coverage for various situations • Workload management in situations that call for the crew to go to the bridge (ensuring that the enough number of crew for the amount of tasks that may arise and replenishing resources by implementing automation that can be used when the crew is called)

70	No implementation of understanding the current situation	C70.1 HMI with difficulty in understanding the current situation C70.2 The crew does not understand how to operate the system or cannot understand the current situation C70.3 System malfunction or failure prevents understanding the current situation C70.4 Forgetting due to concurrent tasks	E70.1_1 Autonomous steering outside the ODD E70.1_2 Manual steering based on incorrect understanding E70.2 Deviation from course E70.3 Abnormal approach to other ships/objects or areas with grounding risk E70.4 Collision, stranding, capsizing, or	Same as ID69	2	5	7	Same as ID1	2	4	6	Same as ID1	Same as ID69

71	Too late/too early to understand the current situation	C71.1 HMI that is difficult to operate or HMI that makes it difficult to understand the current situation and thus takes time to understand the current situation C71.2 The crew does not understand how to operate the system, or it takes time to understand the current situation C71.3 Understanding the current situation takes time due to system malfunctions or failures C71.4 Insufficient resources due to concurrent tasks	E71.1 Autonomous steering outside the ODD E71.2 Deviation from course E71.3 Abnormal approach to other ships/objects or areas with grounding risk E71.4 Collision, stranding, capsizing, or sinking	Same as ID69	2	5	7	Same as ID1	2	5	7	Same as ID1	Same as ID69
72	Error in switching the steering mode based on instructions from the system	C72.1 Failure or malfunction of the ship steering mode switching function C72.2 The crew is not familiar with the procedure C72.3 Distraction or time pressure due to concurrent tasks	Same as ID61	• Alarm for each system failure • Advance training for the crew • Preparation of manuals on how to switch the steering mode	2	5	7	Same as ID1	2	5	7	Same as ID1	Same as ID69

73	Failure to switch the steering mode based on instructions from the system	C73.1 Failure to go to the bridge C73.2 Insufficient understanding of the need for the ship steering mode switching operation C73.3 HMI finding it difficult to understand the ship steering mode C73.4 Failure or malfunction of the ship steering mode switching function C73.5 Ship operation mode switching instruction not activated C73.6 Forgetting due to concurrent tasks	Same as ID61	• Alarm for each system failure • Alarm activated when a certain amount of time is exceeded • Preparation of manuals to improve crews' understanding of the system • Appropriate HMI design and verification	2	5	7	Same as ID1	2	4	6	Same as ID1	Same as ID69

74	Too late/too early to implement switching of the steering mode based on instruction from the system	C74.1 Insufficient understanding of the operation method C74.2 HMI finding it difficult to understand the necessity of switching the ship steering mode, thus taking time to switch C74.3 Failure or malfunction of the ship steering mode switching function C74.4 Too late issuance of the ship steering mode switching instruction C74.5 Lack of resources due to concurrent tasks	Same as ID61	Same as ID73	2	5	7	Same as ID1	2	5	7	Same as ID1	Same as ID69

75	Mistakes in manual steering	C75.1 Failure or malfunction of the manual ship steering system C75.2 The crew does not understand how to operate the manual ship steering system C75.3 Misjudgment of other ships' movements C75.4 The crew is not proficient in manual ship steering C75.5 The crew has relied on automatic ship steering for a long time and their manual ship steering skills are deteriorating C75.6 Distraction or time pressure due to	E75.1 Manual steering different from crew's intention E75.2 Abnormal approach to other ships/objects or areas with grounding risk E75.3 Collision, stranding, capsizing, or sinking	• Redundancy of the manual steering system • Training for the crew	2	6	8	Same as ID1	2	5	7	Same as ID1	• Inspection of the manual steering system • Appropriate HMI design for the manual steering system • Workload management in situations that call for the crew to the bridge (ensuring that the enough number of crew for the amount of tasks that may arise and replenishing resources by implementing automation that can be used when the crew is called)
76	No implementation of manual steering	C76.1 Failure or malfunction of the manual ship steering system C76.2 The crew does not understand how to operate the manual ship steering system C76.3 Switching to manual steering not performed C76.4 Forgetting due to concurrent tasks	E76.1 Operation not based on manual or autonomous steering E76.2 Abnormal approach to other ships/objects or areas with grounding risk E76.3 Collision, stranding, capsizing, or sinking	Same as ID75	2	5	7	Same as ID1	2	5	7	Same as ID1	Same as ID75

77	Too late/too early execution of manual steering	C77.1 Failure or malfunction of the manual ship steering system C77.2 The crew does not understand how to operate the manual ship steering system C77.3 Misjudgment of other ships' movements C77.4 Delay in switching to manual ship steering C77.5 Lack of resources due to concurrent tasks	E77.1 Incorrect steering E77.2 Abnormal approach to other ships/objects or areas with grounding risk E77.3 Collision, stranding, capsizing, or sinking	Same as ID75	2	6	8	Same as ID1	2	5	7	Same as ID1	Same as ID75
Shadow crew														

78	Errors in constant monitoring of each system and surroundin g situations	C78.1 HMI gives a false understanding of the current situation C78.2 Shadow crew does not understand how to operate the system C78.3 Wrong information displayed due to system malfunction or failure C78.4 Distraction due to other tasks and time pressure	Same as ID1	NA	2	5	7	• Preparation of the manual on how to operate each system • training of the shadow crew • Appropriate HMI design and verification •Alarm for each system failure • Manufacturer's engineers onboard the ship during demonstration • Workload management of the shadow crew (ensuring the enough number of the shadow crews for the amount of tasks and replenishing resources by introducing available automation)	2	4	6	Same as ID1	NA

79	No implementation of constant monitoring of each system and surrounding situations	C79.1 HMI finding it difficult to understand the current situation C79.2 The shadow crew does not understand how to operate the system or cannot understand the current situation C79.3 System malfunction or failure prevents understanding the current situation C79.4 Shadow crew's sudden illness, napping, or engaging in other tasks, among other factors	Same as ID1	NA	2	5	7	Same as ID78	2	4	6	Same as ID1	NA

80	Too late/too early implementation of constant monitoring of each system and surrounding situations	C80.1 HMI finding it difficult to operate or HMI finds it difficult to understand the current situation and thus takes time to understand the current situation C80.2 The shadow crew does not understand how to operate the system, and it takes time to understand the current situation C80.3 Understanding the current situation takes time due to system malfunctions and failures C80.4 Shadow crew's sudden illness, napping, or engaging in other tasks, among other factors	Same as ID1	NA	2	5	7	Same as ID78	2	5	7	Same as ID1	NA

81	Error in emergency response (forced switchover to manual steering)	C81.1 Failure of the ship steering mode switching function C81.2 The shadow crew is not familiar with the ship steering mode switching method C81.3 Distraction due to other tasks and time pressure	Same as ID1	NA	2	6	8	• Preparation of the manual on how to switch the steering mode • Advance training of the shadow crew • Workload management of the shadow crew (ensuring the enough number of the shadow crews for the amount of tasks and replenishing resources by introducing available automation)	2	5	7	Same as ID1	NA

82	Failure to implement the emergency response (forced switchover to manual steering)	C82.1 Overconfidence in the autonomous ship steering system C82.2 The shadow crew does not understand that the current situation is an emergency (misperception of their own ship's performance or current information on their ship/surrounding/environment, etc.). C82.3 The shadow crew does not respond thinking that the onboard crew will respond C82.4 The shadow crew is not familiar with how to switch the ship steering mode C82.5 The shadow crew's sudden illness, napping, or engaging in other tasks, among other factors	Same as ID1	NA	2	6	8	Same as ID81	2	5	7	Same as ID1 * Ensure that the shadow crew respond if they sense even the slightest danger without expecting the onboard crew to respond	NA

83	Too late/too early to implement emergency response (forced switchover to manual steering)	C83.1 Malfunction of the ship steering mode switching function C83.2 The shadow crew is not familiar with the ship steering mode switching method C83.3 The shadow crew is late in responding because they think the regular crew will respond C83.4 Shadow crew's sudden illness, napping, or engaging in other tasks, among other factors	Same as ID1	NA	2	6	8	Same as ID81	2	5	7	Same as ID1 * Ensure that the shadow crew respond if they sense even the slightest danger without expecting the onboard crew to respond	NA

Appendix 3. A practical example of risk analysis on a phase III autonomous ship

A practical example of risk analysis on a phase III autonomous ship are shown in this Appendix. We assume one phase, that is, navigation in ocean (Navigation in port and Berthing/unberthing phases are out of this risk analysis because we assume that manual operation is conducted in these phases). It should be noted that risk analysis is desirable considering more phases to increase the comprehensiveness of hazards.

i. Preparation of documents

Examples of the documents mentioned in section 4.1 of this procedure are shown as follows:

(0) ConOps

Table 3.1 ConOps

● Definition of the feature This feature targets a given voyage plan, detects other ships and wreckage that the ship encounters, disturbances caused by marine weather, formulates a ship action plan according to a predetermined action policy, calculates engine output and steering commands to achieve the action plan, and outputs the speed and the course for the ship to achieve the voyage plan. The voyage plan consists of the departure point, departure date and time, arrival point, arrival date and time, and way point. The autonomous ship steering system onboard the ship will formulate a ship action plan based on the voyage plan and control the steering and engine output in accordance with the ship action plan using the ship control system. <Navigation Plan> Departure point: XXX Port Departure date and time: Month/date, XX:XX Arrival point: YYY Port Arrival date and time: Month/date, YY:YY Waypoint: ZZZ Port Waypoint arrival date and time: Month/date, ZZ:ZZ <Action Policy> Secure an appropriate time to begin avoidance and an appropriate distance to avoid interfering navigation of other ships or causing fear on sailor of other ships. Considering the voyage plan, in order to prevent a large delay, the time spent on avoidance navigation should be minimized while securing the above mentioned appropriate avoidance start time and distance.
● Objective of the feature The objective of this feature is to develop the ship steering plan that includes responses to external

obstacles and disturbances that may act as impediments in the realization of the voyage plan and to control the ship according to that action plan.
● Extend of automation and relation of automation with operators (onboard crew/remote operators) Extent of automation of the present feature is equivalent to the Category II shown in the ClassNK Guidelines [4]. Collection of information on obstacles, integration of the collected information, and preparation of the action plan are performed with this feature. The action plan is output to the steering and engine equipment by the present feature. Within the assumed conditions of use for this feature discussed below, autonomous navigation is performed with this feature. Outside these conditions, the crew on board steers in the conventional method.
● Extent of remote control and relation with operators (onboard crew/remote operators) This feature does not have remote control capability.
●Assumed range of use ship: Ship name: ○○○ Type of ship: Ferry Gross tonnage: 199 tons Loa: 45 m Width: 9 m Navigation area: Coasting area Route: Port XXX to Port YYY Phase of autonomous navigation: navigation in ocean (manual operation is conducted in navigation in port and berthing/un-berthing phases).
● Autonomous navigation methods Autonomous navigation of a ship equipped with this feature is performed by taking over the tasks from the onboard crew on the sea route within the assumed conditions of use and turning on the feature upon having the onboard crew confirming the operation. t Completing the autonomous navigation along the sea route within the assumed conditions of use and hanging over the tasks to the onboard crew completes the extent of autonomous navigation. If the ship leaves the ODD during its route, even within the assumed conditions of use, autonomous navigation is stopped by handing over to the onboard crew.
● Means of monitoring relevant feature The sensor information collected and integrated into the present feature, the prepared action plan, and the position of the ship within the ODD are constantly provided to the onboard crew by the

dedicated monitoring device on the ship.
● Response procedures in case of deviation from the ODD during the automatic operation Deviation from the ODD is detected by this feature and the onboard crew are notified by the onboard alarm. After the crew switch from autonomous mode to manual mode in a defined procedure, the crew take over the control of the ship.

(1) Functional requirements for the automation system (target tasks and subtasks of the automation)

Table 3.2 Functional requirements for the automation system (Phase: Navigation in ocean)

ID	Element name	Task	Subtask
1	Autonomous ship steering system	· Establish action plan · Diagnose own status	· Obtain integrated information on own ship · Obtain integrated information on other ships and drifting objects · Obtain integrated information on marine weather conditions · Calculate navigational safety and economic efficiency · Present ship action plans · Obtain information necessary to diagnose own status
2	Information integration system for own ship	· Integrate information on own ship · Diagnose own status · Diagnose sensor status	· Obtain information on own ship · Obtain information necessary to diagnose own status · Obtain information necessary to diagnose sensor status · Transmit integrated information, own status, and sensor status
3	Information integration system for other ships/ drifting objects	· Integrate information on other ships and drifting objects · Diagnose own status · Diagnose sensor status	· Obtain information on other ships and drifting objects · Obtain information necessary to diagnose own status · Obtain information necessary to diagnose sensor status

			· Transmit integrated information, own status, and sensor status
4	Information integration system for marine weather	· Integrate of the information on marine weather conditions · Diagnose own status · Diagnose sensor status	· Obtain information on marine weather conditions (current location) · Obtain marine weather condition forecast information · Obtain information necessary to diagnose own status · Obtain information necessary to diagnose sensor status · Transmit integrated information, own status, and sensor status
5	Ship control system	· Calculate control variables based on ship action plans · Rudder/engine control · Diagnose rudder/engine status · Diagnose own status	· Obtain ship action plans · Obtain actual ship's position · Calculate of the deviation between the ship action plans and the ship's position · Compare current situation with control threshold values · Transmit rudder/engine status and own status
6	Autonomous operation management system	· Control mode switching instructions · Diagnose own status	· Obtain information on own ship, other ships, drifting objects, marine weather conditions · Obtain information on the status of each system · Determine whether inside or outside ODD · Obtain information necessary to diagnose own status
7	Onboard crew	(Immediately before going to the bridge) · Go to the bridge based on instructions from the autonomous operation management system	· Confirm the operation mode switching instructions of the autonomous operation management system · Confirm information on own ship, other ships/drifting objects, weather/sea conditions

		(After arriving at the bridge) ・ Identify current situation ・ Switch the ship steering mode based on instructions from the system ・ Manual operation	

(2) System architecture that clarifies the entire image of the automation system

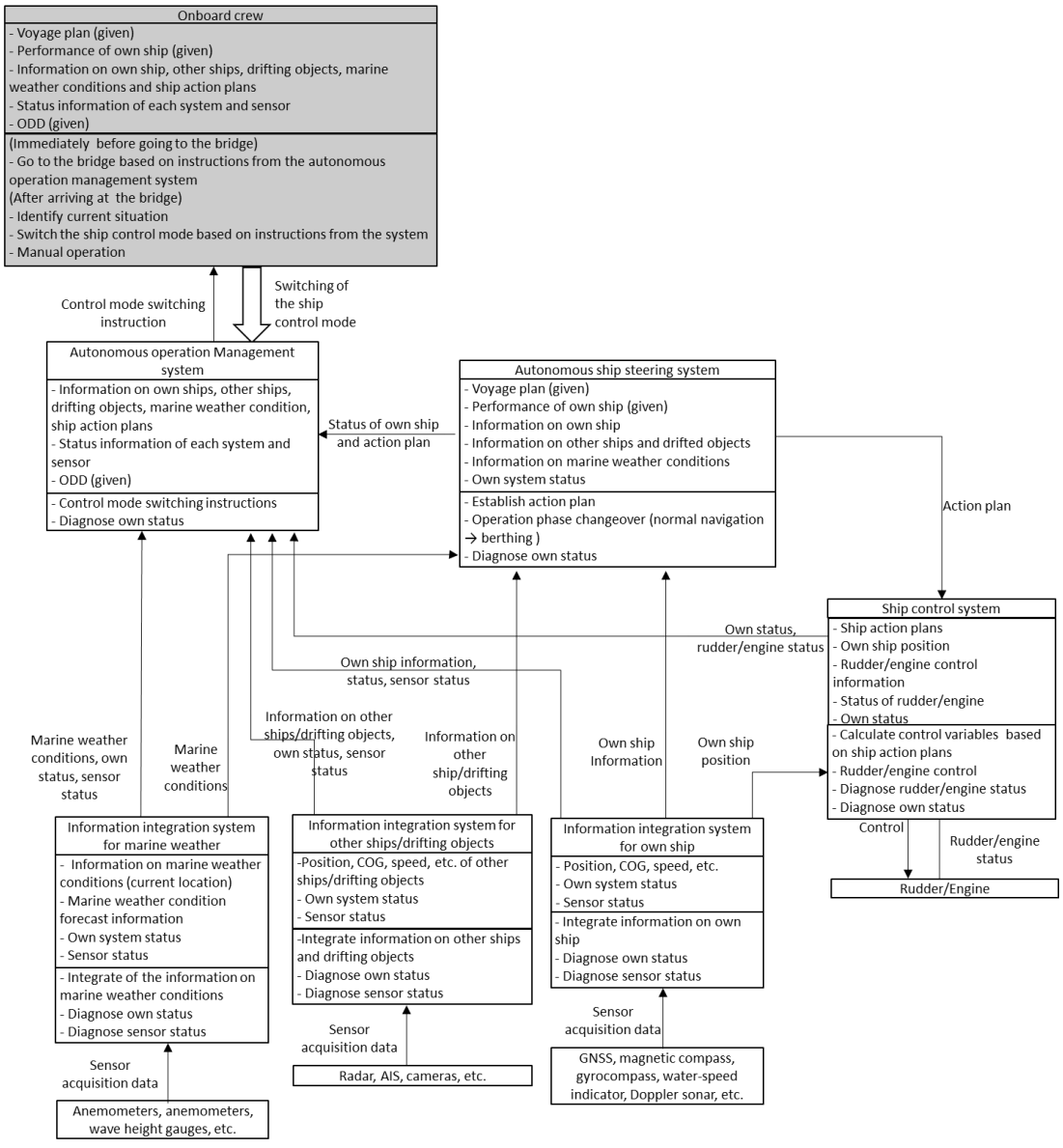

Figure 3.1 System architecture (Phase: Navigation in ocean)

(3) Outline of the internal operation of the automation system

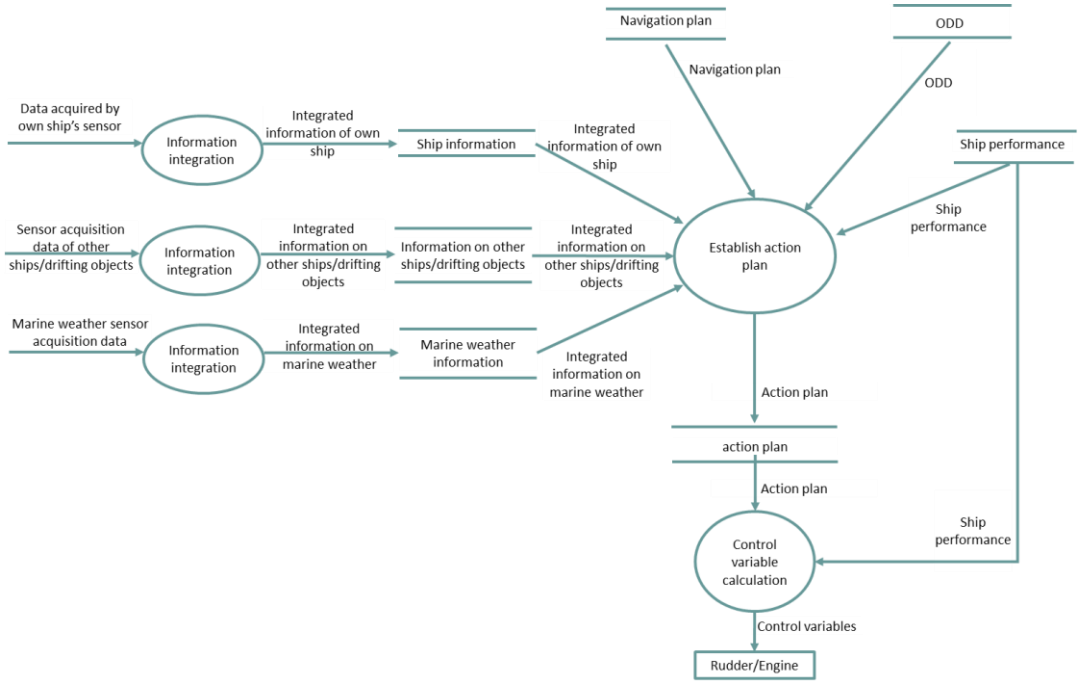

Figure 3.2 Outline of the internal operation regarding autonomous navigation (Phase: Navigation in ocean)

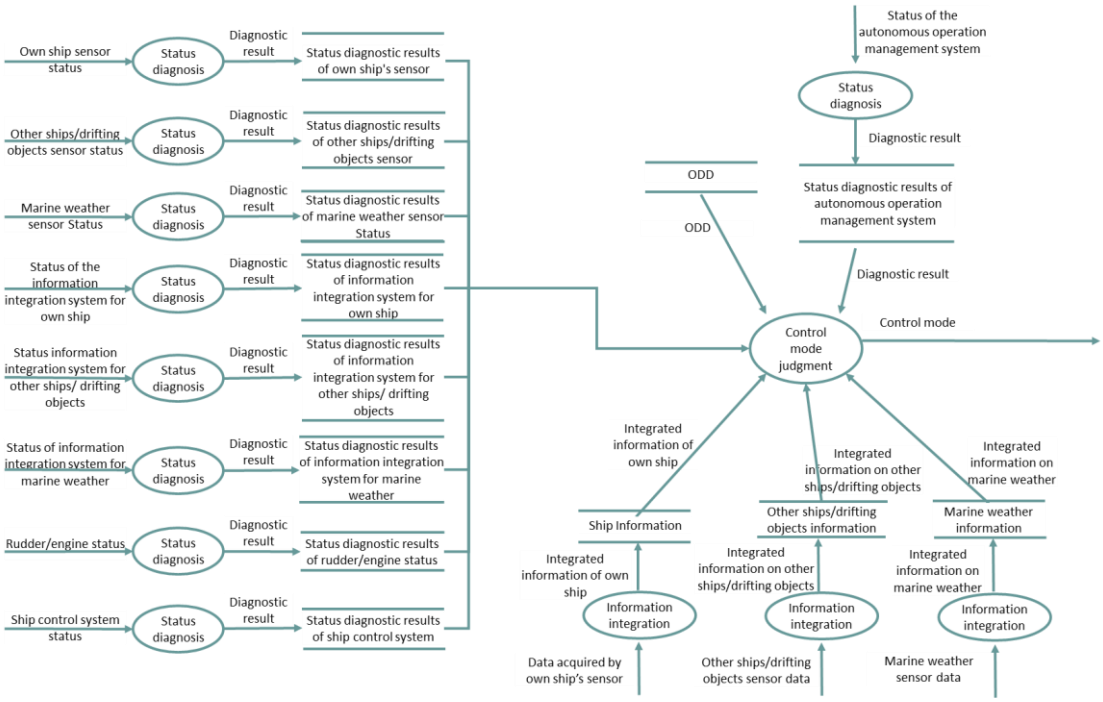

Figure 3.3 Outline of the internal operation regarding mode decision (Phase: Navigation in ocean)

(4) Outline of the division of roles for the automation system and humans

Table 3.3 Outline of the division of roles for the automation system and humans (Phase: Navigation in ocean)

Task	Autonomous ship steering system	Information integration system for own ship	Information integration system for other ships/drifting objects	Information integration system for marine weather	Ship control system	Autonomous operation management system	Onboard crew
Obtaining information on own ship		(1) Acquiring and integrating information					
Obtaining information on other ships/drifting objects, etc.			(1) Acquiring and integrating information				
Obtaining marine weather information				(1) Acquiring and integrating information			
Establishing	(1) Establishing						

(avoid-ance) action plan							
Execut-ing (avoid-ance) action plan					(1) Exe-cuting		
Diagno-sis of re-lated sensor status		(1) Diag-nosis of conditions	(1) Diag-nosis of conditions	(1) Diag-nosis of conditions			
Diagno-sis of own sta-tus	(1) Diag-nosis of conditions	(1) Diag-nosis of conditions	(1) Diag-nosis of conditions	(1) Diag-nosis of conditions	(1) Diag-nosis of conditions	(1) Diag-nosis of conditions	
Judging inside or outside the ODD and de-termin-ing steering mode						(1) Judg-ing and determin-ing	
Control mode switch-ing in-struc-tions and						(1) Con-trol mode switching instruc-tions	(2) Going to the bridge (3) Identi-fying cur-rent status

control mode switch-over							(4) Mode switching

(5) ODD of an automation system

Table 3.4 ODD of an automation system

Marine area conditions	
Navigation zone	Designated ship course
Degree of congestion	Low Congestion: Up to 5 ships within a 3 NM range
Ships not equipped with AIS and obstructions	No non-AIS equipped ships or obstacles that the system cannot detect: No dangerous obstacles of less than 1 m in size within 700 m
Environmental condition	
Marine weather	Calm condition: Wind: 7 m/s or less, wave height: 1.5 m or less, and visibility: 500 m or more
Time	All day
Internal state	
System state	Running normally: No error indication
Equipment required for operation	Running normally: No error indication
Ship motion	Within design constraints of the hull: No anomaly indicated
Other	No emergency events have occurred: No inboard fire, outboard fire, overboard, emergency signal interception, etc.

ii. Risk analysis

Examples of HAZID WS are shown in Table 3.5. These are risk analysis results on Phase III autonomous ship which explained in the above i (Preparation of documents). The definitions of FI (Frequency Index), SI (Severity Index) and RI (Risk Index) are the same as those of section5.3 of this procedure document.

Table 3.5 HAZID WS (Phase: Navigation in ocean)

Sheet ID: 1
Phase: Navigation in ocean

ID	Hazard	Causes	Consequences	Existing Safeguards	Index(only existing safeguards)			Recommendation	Index(Include safeguards recommendation)			Comments
					SI	FI	RI		SI	FI	RI	
Autonomous ship steering system												
1	Error in establishing the action plan	C1.1 Input information not obtained or incorrect (information on own ship, other ships and drifting objects, marine weather, etc.) C1.2 Voyage plan (given) not obtained or incorrect C1.3 Faulty algorithm for establishing the ship action plan in the autonomous ship steering system C1.4 Failure or malfunction of the autonomous ship steering system C1.5 Malware infiltration or hacking	E1.1 Abnormal approach to other ships/objects, or areas with grounding risk E1.2 Collision, grounding, capsizing, and sinking	• Alarm for each system failure • Alarm when various information and voyage plans are not entered • Double-checking when entering voyage plans • Alarm when jumping position of own ship or other ships/drifts • Prior verification by simulations of action planning algorithms • Connect only to removable media with no viruses detected by virus detection software as well as no connection to external networks	1	5	6	• Improvement of the action planning algorithm	1	5	6	

2	No implementation of the action plan	C2.1 Input information not obtained (information on own ship, other ships and drifting objects, marine weather, etc.) C2.2 Voyage plan (given) not obtained C2.3 Failure or malfunction of the autonomous ship steering system C2.4 Malware intrusion or hacking C2.5 Failure to receive inquiry (trigger for activating this function)	Same as ID1	• Alarm for each system failure • Alarm when various information and voyage plans are not entered • Alarm when a certain amount of time has elapsed • Pre verification through simulations • Connect only to removable media with no viruses detected by virus detection software as well as no connection to external networks	1	5	6	• Improvement of the action planning algorithm (If the response is too late, the inquiry source shall be made to ask again with new input information.)	1	5	6	

3	Too late/too early implementation of the action plan	C3.1 Input information not obtained or obtained at the wrong time (information on own ship, other ships and drifting objects, marine weather, etc.) C3.2 Failure of the autonomous ship steering system's berthing/ unberthing action planning algorithm (too much time is spent on calculations for action planning) C3.3 Failure or malfunction of the autonomous ship steering system C3.4 Malware infiltration or hacking C3.5 Wrong timing of inquiry (trigger for activation of this function)	Same as ID1	Same as ID2	1	5	6	• Improvement of the action planning algorithm (If the response is too late, the inquiry source shall be made to ask again with new input information.)	1	5	6	

4	Error in diagnosis of own status	C4.1 Wrong algorithm for the self-diagnostic function of the autonomous ship steering system C4.2 Incorrect input information (information required for self-diagnosis) C4.3 Malware intrusion or hacking	• Misdiagnose as normal when abnormal → E4.1 Deviation from course E4.2 Abnormal approach to other ships/objects, berth, or areas with grounding risk E4.3 Collision with other ships or berth, grounding, and capsizing or sinking • Misdiagnose as abnormal when normal → Switch to manual steering based on alarm	• Pre verification of the self-diagnostic function • Connect only to removable media with no viruses detected by virus detection software as well as no connection to external networks	1	5	6	• Improvement of the algorithm for the self diagnostic function of the autonomous ship steering system	1	5	6	
5	No implementation of the diagnosis of own ship's status	C5.1 Failure, malfunction, or stoppage of the self-diagnostic function of the autonomous ship steering system C5.2 Input information (information necessary for self-diagnosis) not obtained C5.3 Malware intrusion or hacking	• Diagnosis not performed when normal → No problem (alarm will be activated when a certain period of time is exceeded) • Diagnosis not performed when abnormal → Same as ID4	• Pre verification of the self-diagnostic function • Alarm activated when a certain amount of time is exceeded • Connect only to removable media with no viruses detected by virus detection software as well as no connection to external networks	1	5	6	Same as ID4	1	4	5	

6	Too late/too early to implement the diagnosis of own status	C6.1 Failure or malfunction of the self-diagnostic function of the autonomous ship steering system C6.2 Malfunction of the self-diagnostic algorithm of the autonomous ship steering system (self-diagnostic operation takes too much time) C6.3 Incorrect timing for obtaining input information (information necessary for self-diagnosis) C6.4 Malware intrusion or hacking	• Too late to diagnose when normal → No problem (alarm will be activated when a certain period of time is exceeded) • Too late to diagnose as abnormal when abnormal → E6.1 Delay in switching to the manual operation E6.2 Autonomous operation outside ODD E6.3 Deviation from course E6.4 Abnormal approach to other ships/objects, or areas with grounding risk E6.5 Collision, grounding, capsizing, or sinking	Same as ID5	1	5	6	Same as ID4	1	5	6	
Information integration system for own ship												

7	Error in integration of own ship information	C7.1 Inconsistency in input information (e.g., different data between sensors of own ship, integration with old information, etc.) C7.2 Failure or malfunction of the information integration function and, error in the integration algorithm C7.3 Malware intrusion or hacking	E7.1 Establishment of the incorrect avoidance action plan E7.2 Incorrect calculation of the control variables E7.3 Incorrect/no switching of the operation phase E7.4 Deviation from course E7.5 Abnormal approach to other ships/objects or areas with grounding risk E7.6 Collision, grounding, capsizing, or sinking	• Advance verification of the information integration function • Integrating a method for dealing with discrepancies in data (which data should be prioritized) • Alarm for each system failure • Warnings when the same type of data differs • Connect only to removable media with no viruses detected by virus detection software as well as no connection to external networks	1	5	6	• Improvement of the information integration algorithm	1	4	5	

8	No implementation of integrating information of own ship	C8.1 Inconsistency in input information (different data between sensors of own ship) C8.2 Failure or malfunction of the information integration function and error in the integration algorithm C8.3 Malware intrusion or hacking C8.4 Failure to receive inquiry (trigger for activating this function)	Same as ID7	• Advance verification of the information integration function • Incorporating a method for dealing with discrepancies in data (which data should be prioritized) • Alarm for each system failure • Warnings when the same type of data differs • Alarm activated when a certain amount of time is exceeded • Connect only to removable media with no viruses detected by virus detection software as well as no connection to external networks	1	4	5	Same as ID7	1	4	5	

9	Too late/too early to implement integrating own ship information	C9.1 Malfunction of the information integration function/algorithm (information integration takes too much time) C9.2 Wrong timing of information acquisition from different sensors C9.3 Malware intrusion or hacking C9.4 Wrong timing of inquiry (trigger for activating this function)	E9.1 Establishment of the incorrect avoidance action plan E9.2 Incorrect calculation of the control variables E9.3 Switch the operation phase at wrong position E9.4 Deviation from course E9.5 Abnormal approach to other ships/objects or areas with grounding risk E9.6 Collision, grounding, capsizing, or sinking	Same as ID8	1	5	6	Same as ID7	1	5	6	
10	Error in the diagnosis of own status	C10.1 Failure or malfunction of the self-diagnostic function C10.2 Wrong algorithm for the self-diagnostic function C10.3 Incorrect input information (information required for self-diagnosis) C10.4 Malware intrusion or hacking	Same as ID4	Same as ID4	1	5	6	Same as ID4	1	5	6	

11	No implementation of the diagnosis of own status	C11.1 Failure, malfunction, or stoppage of the self-diagnostic function C11.2 Input information (information necessary for self-diagnosis) not obtained C11.3 Malware intrusion or hacking	Same as ID5	Same as ID5	1	5	6	Same as ID4	1	4	5	
12	Too late/too early to implement the diagnosis of own status	C12.1 Failure or malfunction of the self-diagnostic function C12.2 Malfunction of the self-diagnostic algorithm (self-diagnostic operation takes too much time) C12.3 Incorrect timing for obtaining input information (information required for self-diagnosis) C12.4 Malware intrusion or hacking	Same as ID6	Same as ID6	1	5	6	Same as ID4	1	5	6	
13	Error in diagnosing sensor status	C13.1 Failure or malfunction of the status diagnostic function for the sensor C13.2 Wrong algorithm for the status diagnostic function for the sensors of own ship C13.3 Incorrect input information (information required for sensor status diagnosis) C13.4 Malware intrusion or hacking	• Misdiagnose as normal when abnormal → Same as ID7 • Misdiagnose as abnormal when normal → Switch to manual steering based on alarm	• Pre verification of the status diagnostic function and algorithm for the sensor • Connect only to removable media with no viruses detected by virus detection software as well as no connection to external networks	1	5	6	• Improvements in algorithm for the diagnostic function of the sensor status	1	5	6	

14	No implementation of the diagnosis of sensor status	C14.1 Failure or malfunction of the status diagnostic function for the sensors of own ship C14.2 Input information (information necessary for sensor status diagnosis) not obtained C14.3 Malware intrusion or hacking	• Diagnosis not performed when abnormal → Same as ID7 • Diagnosis not performed when normal → No problem (alarm will be activated when a certain period of time is exceeded)	• Pre verification of the status diagnostic function for the sensors • Alarm activated when a certain amount of time is exceeded • Connect only to removable media with no viruses detected by virus detection software as well as no connection to external networks	1	5	6	Same as ID13	1	4	5	
15	Too late/too early to implement the diagnosis of sensor status	C15.1 Failure or malfunction of the status diagnostic function for the sensors of own ship C15.2 Malfunction of the sensor status diagnosis algorithm (status diagnosis operation takes too much time) C15.3 Wrong timing of obtaining input information (information required for sensor status diagnosis) C15.4 Malware intrusion or hacking	• Too late to diagnose as normal when normal → No problem (alarm will be activated when a certain period of time is exceeded) • Too late to diagnose as abnormal when abnormal → Same as ID9	• Pre verification of the status diagnostic function and algorithm for the sensors • Alarm activated when a certain amount of time is exceeded • Connect only to removable media with no viruses detected by virus detection software as well as no connection to external networks	1	5	6	Same as ID13	1	5	6	
Information integration system for other ships and drifting objects												

16	Error in integration information of other ships and drifting objects	C16.1 Inconsistency in input information (e.g., different data between sensors, integration with old information) C16.2 Failure or malfunction of the information integration function as well as errors in the integration algorithm C16.3 Malware intrusion or hacking	E16.1 Establishment of the incorrect avoidance action plan E16.2 Abnormal approach to other ships/objects or areas with grounding risk E16.3 Collision, grounding, capsizing, or sinking	Same as ID7	1	5	6	Same as ID7	1	4	5	
17	No implementation of integration information of other ships and drifting objects	C17.1 Inconsistency in input information (e.g., different data between sensors) C17.2 Failure or malfunction of the information integration function as well as errors in the integration algorithm C17.3 Malware intrusion or hacking C17.4 Failure to receive inquiry (trigger for activating this function)	Same as ID16	Same as ID8	1	4	5	Same as ID7	1	4	5	

18	Too late/too early implementation of integration information of other ships and drifting objects	C18.1 Failure of information integration function/algorithm (information integration takes too much time) C18.2 Wrong timing of information acquisition from different sensors C18.3 Malware intrusion or hacking C18.4 Wrong timing of inquiry (trigger for activation of this function)	Same as ID16	Same as ID8	1	5	6	Same as ID7	1	5	6	
19	Error in diagnosing own status	C19.1 Failure or malfunction of the self-diagnostic function C19.2 Wrong algorithm for the self-diagnostic function C19.3 Incorrect input information (information necessary for self-diagnosis) C19.4 Malware intrusion or hacking	Same as ID4	Same as ID4	1	5	6	Same as ID4	1	5	6	
20	No implementation of diagnosing own status	C20.1 Failure or malfunction of the self-diagnostic function C20.2 Input information (information necessary for self-diagnosis) not obtained C20.3 Malware intrusion or hacking	Same as ID5	Same as ID5	1	5	6	Same as ID4	1	4	5	

21	Too late/too early implementation of diagnosing own status	C21.1 Failure or malfunction of the self-diagnostic function C21.2 Malfunction of the self-diagnostic algorithm (self-diagnostic operation takes too much time) C21.3 Wrong timing of obtaining input information (information required for self-diagnosis) C21.4 Malware intrusion or hacking	Same as ID6	Same as ID6	1	5	6	Same as ID4	1	5	6	
22	Error in diagnosing sensor status	C22.1 Failure or malfunction of the status diagnostic function for the sensors C22.2 Wrong algorithm for the status diagnostic function for the sensors C22.3 Incorrect input information (information necessary for sensor status diagnosis) C22.4 Malware intrusion or hacking	• Misdiagnose as normal when abnormal → Same as ID16 • Misdiagnose as abnormal when normal → Switch to manual steering based on alarm	Same as ID13	1	5	6	Same as ID13	1	5	6	

23	No implementation of diagnosing sensor status	C23.1 Failure or malfunction of the status diagnostic function for the sensors C23.2 Input information (information necessary for sensor status diagnosis) not obtained C23.3 Malware intrusion or hacking	• Diagnosis not performed when abnormal → Same as ID16 • Diagnosis not performed when normal → No problem (alarm will be activated when a certain period of time is exceeded)	Same as ID14	1	5	6	Same as ID13	1	4	5	
24	Too late/too early implementation of diagnosing sensor status	C24.1 Failure or malfunction of the status diagnostic function for the sensors C24.2 Malfunction of the algorithm for the sensor status diagnosis (status diagnosis operation takes too much time) C24.3 Wrong timing of obtaining input information (information required for sensor status diagnosis) C24.4 Malware intrusion or hacking	• Too late diagnosis as normal when normal → No problem (alarm will be activated when a certain period of time is exceeded) • Too late diagnosis as abnormal when abnormal → Same as ID16	Same as ID15	1	5	6	Same as ID13	1	5	6	
Information integration system for marine weather												

25	Error in integration of marine weather information	C25.1 Inconsistency in input information (e.g., different data between sensors, integration with old information) C25.2 Failure or malfunction of the information integration function as well as error in integration algorithm C25.3 Malware intrusion or hacking	Same as ID16	Same as ID7	1	5	6	Same as ID7	1	4	5	
26	No implementation of integrating marine weather information	C26.1 Inconsistency in input information (e.g., different data between sensors) C26.2 Failure or malfunction of the information integration function as well as error in integration algorithm C26.3 Malware intrusion or hacking C26.4 Failure to receive inquiry (trigger for activating this function)	Same as ID16	Same as ID8	1	4	5	Same as ID7	1	4	5	

27	Too late/too early implementation of integrating marine weather information	C27.1 Failure or malfunction of the information integration function/algorithm (information integration takes too much time) C27.2 Wrong timing of information acquisition from different sensors C27.3 Malware intrusion or hacking C27.4 Wrong timing of inquiry (trigger for activation of this function)	Same as ID16	Same as ID8	1	5	6	Same as ID7	1	5	6	
28	Error in diagnosing own status	C28.1 Failure or malfunction of the self-diagnostic function C28.2 Wrong algorithm for the self-diagnostic function C28.3 Incorrect input information (information necessary for self-diagnosis) C28.4 Malware intrusion or hacking	Same as ID4	Same as ID4	1	5	6	Same as ID4	1	5	6	
29	No implementation of diagnosing own status	C29.1 Failure or malfunction of the self-diagnostic function C29.2 Input information (information necessary for self-diagnosis) not obtained C29.3 Malware intrusion or hacking	Same as ID5	Same as ID5	1	5	6	Same as ID4	1	4	5	

30	Too late/too early implementation of diagnosing own status	C30.1 Failure or malfunction of the self-diagnostic function C30.2 Malfunction of the self-diagnostic algorithm (self-diagnostic operation takes too much time) C30.3 Wrong timing of obtaining input information (information required for self-diagnosis) C30.4 Malware intrusion or hacking	Same as ID6	Same as ID6	1	5	6	Same as ID4	1	5	6	
31	Error in diagnosing sensor status	C31.1 Failure or malfunction of the status diagnostic function for the sensors C31.2 Wrong algorithm for the status diagnostic function for the sensors C31.3 Incorrect input information (information necessary for sensor status diagnosis) C31.4 Malware intrusion or hacking	• Misdiagnose as normal when abnormal → Same as ID16 • Misdiagnose as abnormal when normal → Switch to manual steering based on alarm	Same as ID13	1	5	6	Same as ID13	1	5	6	

32	No implementation of diagnosing sensor status	C32.1 Failure or malfunction of the status diagnostic function for the sensors C32.2 Input information (information necessary for sensor status diagnosis) not obtained C32.3 Malware intrusion or hacking	• Diagnosis not performed when abnormal → Same as ID16 • Diagnosis not performed when normal → No problem (alarm will be activated when a certain period of time is exceeded)	Same as ID14	1	5	6	Same as ID13	1	4	5	
33	Too late/too early implementation of diagnosing sensor status	C33.1 Failure or malfunction of the status diagnostic function for the sensors C33.2 Malfunction of the algorithm for the sensor status diagnosis (status diagnosis operation takes too much time) C33.3 Wrong timing of obtaining input information (information required for sensor status diagnosis) C33.4 Malware intrusion or hacking	• Too late diagnosis as normal when normal → No problem (alarm will be activated when a certain period of time is exceeded) • Too late diagnosis as abnormal when abnormal → Same as ID16	Same as ID15	1	5	6	Same as ID13	1	5	6	
Ship control system												

34	Error in calculation of the control variables based on the action plan	C34.1 Error in the action plan C34.2 Incorrect input information (information required for control variables calculation) C34.3 Error in the control variables calculation algorithm C34.4 Failure or malfunction of the ship control system C34.5 Malware intrusion or hacking	E34.1 Deviation from course E34.2 Abnormal approach to other ships/objects or areas with grounding risk E34.3 Collision, grounding, capsizing, or sinking	• System failure alarm • Pre verification of the control variables calculation algorithm through simulations • Connect only to removable media with no viruses detected by virus detection software as well as no connection to external networks	1	5	6	• Improvement of the control variables calculation algorithm	1	5	6	
35	No implementation of calculating the control variables based on the action plan	C35.1 Action plan not obtained C35.2 Input information (information required for control variables calculation) not obtained C35.3 Failure or malfunction of the ship control system C35.4 Malware intrusion or hacking C35.5 Failure to receive inquiry (trigger for activating this function)	Same as ID34	• System failure alarm • Alarm at the time when various information is not obtained • Pre verification through simulations • Alarm activated when a certain amount of time is exceeded • Connect only to removable media with no viruses detected by virus detection software as well as no connection to external networks	1	5	6	Same as ID34	1	5	6	

36	Too late/too early to implement control variables calculations based on the action plan	C36.1 Wrong timing of obtaining the action plan C36.2 Wrong timing of acquiring input information (information required for control variables calculation) C36.3 Malfunction in the control variables calculation algorithm (excessive time required for control variables calculation) C36.4 Failure or malfunction in the ship control system C36.5 Malware intrusion C36.6 Wrong timing of inquiry (trigger for activation of this function)	Same as ID34	• System failure alarm • Pre verification through simulations • Warning activated when a certain period of time has elapsed • Alarm activated when a certain amount of time is exceeded • Connect only to removable media with no viruses detected by virus detection software as well as no connection to external networks	1	5	6	Same as ID34	1	5	6	
37	Error in control of the rudder or engine	C37.1 Error in control variables calculation C37.2 Actuator malfunction or failure	E37.1 Unable to navigate E37.2 Deviation from course E37.3 Abnormal approach to other ships/objects, or areas with grounding risk E37.4 Collision, grounding, capsizing, or sinking	• Pre verification of the system • Alarms in case of actuator failure or malfunction	1	5	6	Same as ID34	1	5	6	

38	No implementation of control of the rudder or engine	C38.1 Input information (control variables) not obtained C38.2 Malfunction or failure of the actuator C38.3 Failure to receive inquiry (trigger for activating this function)	Same as ID37	• Alarms in case of actuator failure or malfunction • Alarm when control variables not obtained • Alarm activated when a certain amount of time is exceeded	1	4	5	Same as ID34	1	4	5	
39	Too late/too early to implement controlling the rudder or engine	C39.1 Wrong timing of obtaining input information (control variables) C39.2 Malfunction or failure of the actuator C39.3 Wrong timing of inquiry (trigger for activation of this function)	Same as ID37	Same as ID38	1	5	6	Same as ID34	1	5	6	
40	Error in diagnosis of rudder/engine conditions	C40.1 Failure or malfunction of the rudder/engine condition diagnostic function C40.2 Wrong algorithm for the rudder/engine condition diagnostic function C40.3 Incorrect input information (information required for rudder/engine condition diagnosis) C40.4 Malware intrusion or hacking	Same as ID4	Same as ID4	1	5	6	• Improved algorithms for rudder/engine condition diagnostic functions	1	5	6	

41	No implementation of diagnosis of rudder/engine conditions	C41.1 Failure or malfunction of the rudder/engine condition diagnostic function C41.2 Input information (information required for rudder/engine condition diagnosis) not obtained C41.3 Malware intrusion or hacking	Same as ID5	Same as ID5	1	5	6	Same as ID40	1	4	5	
42	Too late/too early to implement diagnosis of rudder/engine conditions	C42.1 Failure or malfunction of the rudder/engine condition diagnostic function C42.2 Malfunction of the rudder/engine condition diagnostic algorithm (self-diagnostic operation takes too much time) C42.3 Wrong timing of obtaining input information (information required for rudder/engine condition diagnosis) C42.4 Malware intrusion or hacking	Same as ID6	Same as ID6	1	5	6	Same as ID40	1	5	6	

43	Error in diagnosing own status	C43.1 Failure or malfunction of the self-diagnostic function C43.2 Wrong algorithm for the self-diagnostic function C43.3 Incorrect input information (information required for self-diagnosis) C43.4 Malware intrusion or hacking	Same as ID4	Same as ID4	1	5	6	Same as ID4	1	5	6	
44	No implementation of diagnosing own status	C44.1 Failure, malfunction, or stoppage of the self-diagnostic function C44.2 Input information (information necessary for self-diagnosis) not obtained C44.3 Malware intrusion or hacking	Same as ID5	Same as ID5	1	5	6	Same as ID4	1	4	5	
45	Too late/too early implementation of diagnosing own status	C45.1 Failure or malfunction of the self-diagnostic function C45.2 Malfunction of the self-diagnostic algorithm (self-diagnostic operation takes too much time) C45.3 Incorrect timing of obtaining input information (information required for self-diagnosis) C45.4 Malware intrusion or hacking	Same as ID6	Same as ID6	1	5	6	Same as ID4	1	5	6	
Autonomous Operation Management System												

46	Error in instructions for switching the ship steering mode	C46.1 Failure or malfunction of the autonomous operation management system C46.2 Error in the algorithm to switch the operation mode C46.3 Error in input information (information required for making the operation mode switching decision) C46.4 Malware intrusion or hacking	E46.1 Autonomous steering outside ODD E46.2 Deviation from course E46.3 Abnormal approach to other ships/objects or areas with grounding risk E46.4 Collision, grounding, capsizing, or sinking	• Alarm for each system failure • Double-checking at the time of ODD input • Alarm at the time of route deviation • Prior verification of the instruction function to switch the ship steering mode through simulations • Connect only to removable media with no viruses detected by virus detection software as well as no connection to external networks	1	5	6	• Improvement of the ship steering mode switching algorithm	1	5	6	
47	No implementation of the ship steering mode switching instructions	C47.1 Failure or malfunction of the autonomous operation management system C47.2 Error in the algorithm to switch the operation mode C47.3 Error in input information (information required for making the operation mode switching decision) C47.4 Malware intrusion or hacking C47.5 Failure to receive inquiry (trigger for activating this function)	Same as ID46	• Alarm for each system failure • Alarm activated when a certain amount of time is exceeded • Double-checking at the time of ODD input • Alarm at the time of route deviation • Prior verification of the instruction function to switch the ship steering mode through simulations • Connect only to removable media with no viruses detected by virus detection software as well as no connection to external networks	1	5	6	Same as ID46	1	4	5	

48	Too late/too early to give the ship steering mode switching instructions	C48.1 Failure or malfunction of the autonomous operation management system C48.2 Malfunction of the algorithm to switch the operation mode (calculating the decision to switch the operation mode takes too much time) C48.3 Wrong timing of obtaining input information (information necessary to decide whether to switch the operation mode) C48.4 Malware infiltration or hacking C48.5 Wrong timing of inquiry (trigger for activation of this function)	Same as ID46	Same as ID47	1	5	6	Same as ID46	1	5	6	
49	Error in diagnosing own status	C49.1 Failure or malfunction of the self-diagnostic function C49.2 Wrong algorithm for the self-diagnostic function C49.3 Incorrect input information (information required for self-diagnosis) C49.4 Malware intrusion or hacking	Same as ID4	Same as ID4	1	5	6	Same as ID4	1	5	6	

50	No implementation of diagnosing own status	C50.1 Failure, malfunction, or stoppage of the self-diagnostic function C50.2 Input information (information necessary for self-diagnosis) not obtained C50.3 Malware intrusion or hacking	Same as ID5	Same as ID5	1	5	6	Same as ID4	1	4	5	
51	Too late/too early implementation of diagnosing own status	C51.1 Failure or malfunction of the self-diagnostic function C51.2 Malfunction of the self-diagnostic algorithm (self-diagnostic operation takes too much time) C51.3 Incorrect timing of obtaining input information (information required for self-diagnosis) C51.4 Malware intrusion or hacking	Same as ID6	Same as ID6	1	5	6	Same as ID4	1	5	6	
Onboard crew												
52	Failure to go to the bridge based on instructions from the autonomous operation management system	C52.1 Failure to go to the bridge C52.2 Failure to go to the bridge due to lack of understanding of the need for going to the bridge or instructions from the system C52.3 Inability to grasp instructions due to inappropriate HMI, etc. C52.4 Restraint by other tasks	Same as ID46	• Transition to MRM/MRC if the crew does not respond after a certain period of time • Appropriate HMI design and verification	1	6	7	• Verification of MRM/MRC coverage for various situations	1	6	7	

53	Too late/too early to go to the bridge based on the instructions from the autonomous operation managemen t system	C53.1 Going to the bridge is delayed and standby location is far away C53.2 Going to the bridge is delayed due to the too much required time to understand instructions due to inappropriate HMI, etc. C53.3 Instructions from the autonomous operation management system are too late C53.4 Takes time to release from other tasks	Same as ID46	• Appropriate HMI design and verification • Transition to MRM/MRC if the crew does not respond after a certain period of time • Verification of the algorithms for autonomous flight management systems to provide instructions at the appropriate time.	1	6	7	Same as ID52	1	6	7	
54	Mistake in understandi ng the current situation	C54.1 HMI giving a wrong understanding of the current situation C54.2 The crew does not understand how to operate the system C54.3 Wrong information displayed due to system malfunction or failure C54.4 Misinterpretation of the displayed information C54.5 Distraction due to concurrent tasks and time pressure	E54.1 Manual steering based on incorrect understanding E54.2 Abnormal approach to other ships/objects or areas with grounding risk E54.3 Collision, stranding, capsizing, or sinking	• Appropriate HMI design and verification • training for the crew • Transition to MRM/MRC if the crew does not respond after a certain period of time	1	6	7	Same as ID52	1	6	7	

55	No implementation of understanding the current situation	C55.1 HMI with difficulty in understanding the current situation C55.2 The crew does not understand how to operate the system or cannot understand the current situation C55.3 System malfunction or failure prevents understanding the current situation C55.4 Forgetting due to concurrent tasks	E55.1_1 Autonomous steering outside the ODD E55.1_2 Manual steering based on incorrect understanding E55.2 Deviation from course E55.3 Abnormal approach to other ships/objects or areas with grounding risk E55.4 Collision, stranding, capsizing, or sinking	Same as ID54	1	5	6	Same as ID52	1	5	6	
56	Too late/too early to understand the current situation	C56.1 HMI that is difficult to operate or HMI that makes it difficult to understand the current situation and thus takes time to understand the current situation C56.2 The crew does not understand how to operate the system, or it takes time to understand the current situation C56.3 Understanding the current situation takes time due to system malfunctions or failures C56.4 Insufficient resources due to concurrent tasks	E56.1 Autonomous steering outside the ODD E56.2 Deviation from course E56.3 Abnormal approach to other ships/objects or areas with grounding risk E56.4 Collision, stranding, capsizing, or sinking	Same as ID54	1	6	7	Same as ID52	1	6	7	

57	Error in switching the steering mode based on instructions from the system	C57.1 Failure or malfunction of the ship steering mode switching function C57.2 The crew is not familiar with the procedure C57.3 Distraction or time pressure due to concurrent tasks	Same as ID46	• Alarm for each system failure • Advance training for the crew • Preparation of manuals on how to switch the steering mode	1	6	7	Same as ID52	1	6	7	
58	Failure to switch the steering mode based on instructions from the system	C58.1 Failure to go to the bridge C58.2 Insufficient understanding of the need for the ship steering mode switching operation C58.3 HMI finding it difficult to understand the ship steering mode C58.4 Failure or malfunction of the ship steering mode switching function C58.5 Ship operation mode switching instruction not activated C58.6 Forgetting due to concurrent tasks	Same as ID46	• Alarm for each system failure • Alarm activated when a certain amount of time is exceeded • Preparation of manuals to improve crews' understanding of the system • Appropriate HMI design and verification	1	5	6	Same as ID52	1	5	6	

59	Too late/too early to implement switching of the steering mode based on instruction from the system	C59.1 Insufficient understanding of the operation method C59.2 HMI finding it difficult to understand the necessity of switching the ship steering mode, thus taking time to switch C59.3 Failure or malfunction of the ship steering mode switching function C59.4 Too late issuance of the ship steering mode switching instruction C59.5 Lack of resources due to concurrent tasks	Same as ID46	Same as ID58	1	6	7	Same as ID52	1	6	7	

60	Mistakes in manual steering	C60.1 Failure or malfunction of the manual ship steering system C60.2 The crew does not understand how to operate the manual ship steering system C60.3 Misjudgment of other ships' movements C60.4 The crew is not proficient in manual ship steering C60.5 The crew has relied on automatic ship steering for a long time and their manual ship steering skills are deteriorating C60.6 Distraction or time pressure due to concurrent tasks	E60.1 Manual steering different from crew's intention E60.2 Abnormal approach to other ships/objects or areas with grounding risk E60.3 Collision, stranding, capsizing, or sinking	• Redundancy of the manual steering system • Training for the crew	1	6	7	• Appropriate HMI design for the manual steering system	1	6	7	
61	No implementation of manual steering	C61.1 Failure or malfunction of the manual ship steering system C61.2 The crew does not understand how to operate the manual ship steering system C61.3 Switching to manual steering not performed C61.4 Forgetting due to concurrent tasks	E61.1 Operation not based on manual or autonomous steering E61.2 Abnormal approach to other ships/objects or areas with grounding risk E61.3 Collision, stranding, capsizing, or sinking	Same as ID60	1	6	7	Same as ID60	1	5	6	

62	Too late/too early execution of manual steering	C62.1 Failure or malfunction of the manual ship steering system C62.2 The crew does not understand how to operate the manual ship steering system C62.3 Misjudgment of other ships' movements C62.4 Delay in switching to manual ship steering C62.5 Lack of resources due to concurrent tasks	E62.1 Incorrect steering E62.2 Abnormal approach to other ships/objects or areas with grounding risk E62.3 Collision, stranding, capsizing, or sinking	Same as ID60	1	6	7	Same as ID60	1	6	7	

References

[1] IMO: MSC.1/Circ.1455 Guidelines for the approval of alternatives and equivalents as provided for in various IMO instruments (2013)

[2] ClassNK: Risk Assessment Guidelines (2009)

[3] MLIT: Safety Guidelines for MASS (provisional translation) (2022) (in Japanese)

[4] ClassNK: Guidelines for Automated/Autonomous Operation on ships (Ver.1.0) (2020)

[5] IMO: MSC.1/Circ.1212 Guidelines on alternative design and arrangements for SOLAS chapters II-1 and III (2006)

[6] IMO: MSC/Circ.1002 Guidelines on alternative design and arrangements for fire safety (2001)

[7] IMO: MSC-MEPC.2/Circ.12 Revised guidelines for formal safety assessment (FSA) for use in the IMO rule-making process (2013)

[8] Bureau Veritas: Guidelines for Autonomous Shipping (2019)

[9] DNV-GL: Autonomous and remotely operated ships (2018)

[10] M. Shiokari et al.: Application of Risk Analysis Method with System Modeling to Conceptual Design of Autonomous Ships, Proc. Conf. on the Japan Society of Naval Architects and Ocean Engineers, Vol.32, pp.355–366 (2021) (in Japanese)

[11] MUNIN: D9.2, Qualitative assessment, FP7 GA-No 314286 (2015)

[12] EMSA: Study of the risks and regulatory issues of specific cases of MASS—Part 1, Report No. 2019-1296, Rev.0 (2020)

[13] EMSA: Study of the risks and regulatory issues of specific cases of MASS—Part 2, Report No. 2019-0805, Rev.0 (2020)

[14] USTRAT: AUTOSHIP D2.4a—Risk assessments, fail-safe procedures and acceptance criteria The Inland Waterway vessel analysis (2020)

[15] ISO/IEC 31010 (Risk management—Risk assessment techniques)

[16] ISO/IEC 27005 (information technology—Security techniques—Information security risk management)

[17] IEC 60812:2006 (Analysis technique for system reliability—Procedure for failure mode and effects analysis. (FMEA))

[18] IEC 61882:2016 (Hazard and operability studies (HAZOP studies) – Application guide)

[19] NK: Risk Assessment Guidelines (2nd edition) Annex 1 Guidelines for implementation of FMEA (related to the IGC Code) (provisional translation) (2017)

[20] N. G. Leveson and J. P. Thomas: STPA HANDBOOK (2018)

[21] IMO: MSC.97(73) Adoption of the international code of safety for high-speed craft, 2000 (2000 HSC code) (2000)

[22] IPA/SEC: Survey report on the STAMP method (provisional translation) (2015)
[23] Y. Fukuzawa: System Safety and Security Analysis by STAMP/STPA, Systems, control and information.Vol.62, No.4, pp.130–133 (2018) (in Japanese)