Risk analysis procedure for autonomous ships

Japan Ship Technology Research Association
National Maritime Research Institute

Table of Contents

1. Outline

Autonomous ships have been developed in recent years and guidelines for autonomous ship have been published by multiple classification societies and flag states. 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 autonomous ships. It contributes to better safety and promotion of development in regard to autonomous ships.

2. Key Principles

2.1 Target ships of this manual

Though there is no international consensus on the definition of autonomous ship and level of automation, this manual focuses on phase II autonomous ships of "Roadmap to Realize Autonomous Ships" by Maritime Bureau, Ministry of Land, Infrastructure, Transport and Tourism (ships on which sailors, the ultimate decision makers, are supported by the operation from land and/or the proposal by artificial intelligence (AI)).

2.2 Target risk analysis of this manual

As autonomous ships, 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.

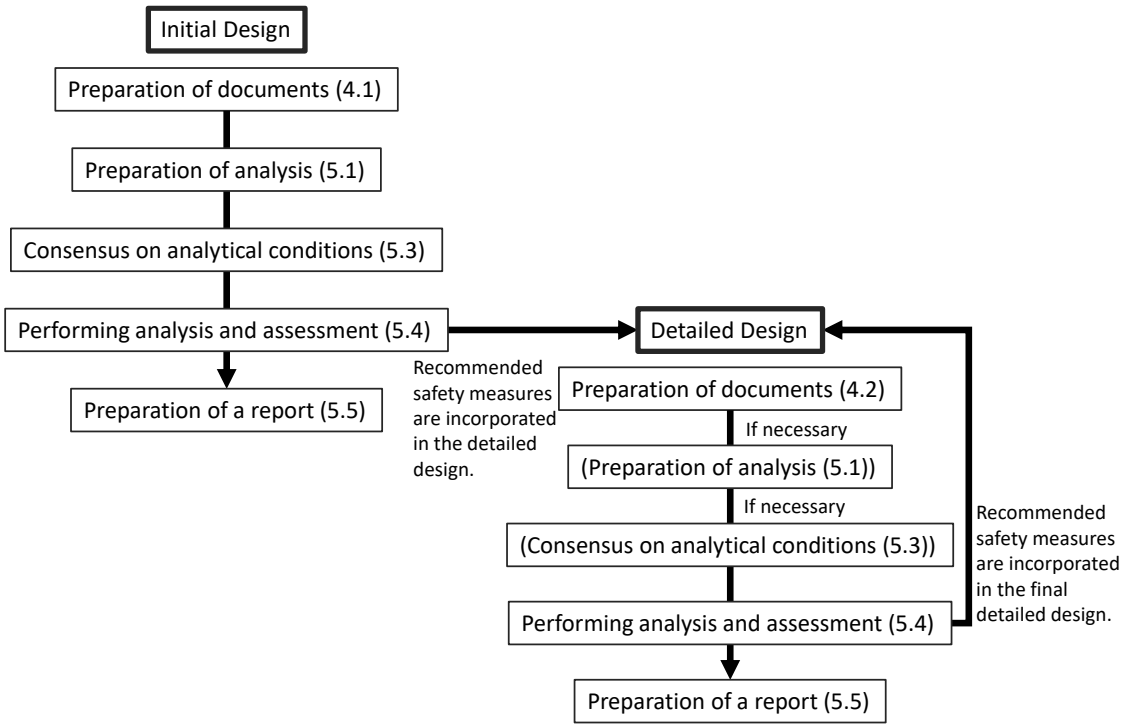

Figure 3.1. Flow chart of procedures used for risk analysis.

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.

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. Figure A1.1 in the Appendix 1 shows an example 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 Appendix 1.

- 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.

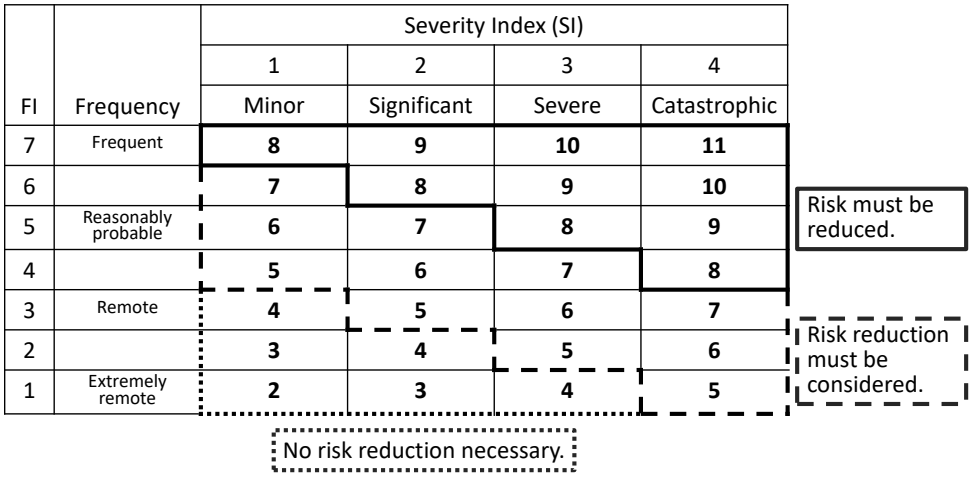

Figure 5.1. Example of judgment criteria.

- 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)

Appendix 1. An example of confirming the analytical target scope

Below is an example of information that must be summarized to determine the analytical target scope in the preparation stage of an analysis. Here, we present an example of each item for a system in which a ship equipped with an autonomous ship control mechanism, with an onshore remote control center, performing an autonomous navigation.

- Definition of the feature

This feature targets a given voyage plan, detects obstacles that the ship encounters, disturbances caused by marine weather, and wireless communications and acoustic signals from other ships and the vessel traffic services, formulates an action plan according to the predetermined action policy, calculates and assesses the 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.

A voyage plan is formulated by the remote control center and consists of a list of waypoints prepared with conditions such as the departure point, departure date and time, arrival point, arrival date and time, and waypoints. The on board autonomous ship control mechanism formulates an action plan for the ship based on the voyage plan received from the remote control center. Through the autonomous navigation system and the autonomous engine monitoring and control system, the bridge automation system and engine automation system regulate operation and engine output according to the action plan.

<Voyage plan>

- Departure point: XX
- Departure date and time: X month X day X hour X minute
- Arrival point: YY
- Arrival date and time: Y month Y day Y hour Y minute
- Waypoint: ZZ
- Waypoint arrival date and time: Z month Z day Z hour Z minute

<Action plan>

- Secure an appropriate time to begin avoidance and an appropriate distance to avoid interfering navigation of other ships or causing fear on sailors 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 accept an approval by remote operators of the remote control center and plan/execute a response plan against external obstacles and disturbances that can become inhibiting factors based on the approval voyage plan.

- Extent of automation and relation of automation with operators (crew on board/remote operator)

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 assessed action plan is presented to crew on board through the autonomous ship control mechanism where it waits for an approval.
  - The approved 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 of automation with operators (crew on board/remote operator)

Extent of remote control of the present feature is equivalent to the Category I shown in the ClassNK Guidelines [4].

After being started by the crew on board, this feature is managed by the crew on board and operators of the remote control center. Within the assumed conditions of use discussed below, operation by the crew on board is unnecessary.

- Assumed conditions of use
  - Ship: Ship name, tonnage, length overall, etc.
  - Sea route: Within the sea route from XX to YY, from ZZ to WW.
  - Marine weather conditions:

- ODD (external conditions, internal conditions, and communication conditions under which the present new feature operates)
  - External conditions: Open sea where the sea route is within the assumed route range. Marine weather conditions are within the assumed conditions of use. There is no obstacle in the predetermined range.
  - Internal conditions: There is no problem with sensors, advanced sensor module, or each system.

- Communication conditions: Communication between the ship and onshore control center is healthy.

- Autonomous navigation methods

Autonomous navigation of a ship equipped with this feature is performed by taking over the tasks from the crew on board on the sea route within the assumed conditions of use and turning on the feature upon having the crew on board confirming the operation. Completing the autonomous navigation along the sea route within the assumed conditions of use and hanging over the tasks to the crew on board 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 crew on board.

- Means of monitoring the 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 and remote operators by the dedicated monitoring device on the ship and at the remote control center.

- Response procedure when autonomous navigation deviates from the ODD

Deviation from the ODD is detected by this feature and the onboard crew are notified by the on board alarm. Operation is immediately handed over to the onboard crew (fallback). This feature will not operate until it has been confirmed that the ship has returned to the ODD.

The information necessary to execute fallback is provided by the regular nautical equipment and dedicated auxiliary equipment.

- The feature(s) for each element constituting the new facility, such as hardware and software, interactions between elements (including relations with humans and existing facilities).
  - Remote control device: Formulation of a voyage plan, management of communications related to distress, monitoring of the overall ship operation, and transmission of a voyage plan to the autonomous ship control mechanism.
  - Autonomous ship control mechanism: Assessment of various data received, formulation of an action plan, transmission of information on the detected surrounding ships to the onshore control center, transmission of engine monitoring and control information to the onshore control center, and transmission of information and action plans received from the onshore control center to the autonomous navigation system and the autonomous engine monitoring/control system.
  - Autonomous navigation system: Weather routing, ship motion determination, buoyancy and

stability control, collision avoidance, and warnings and emergency response.

- Autonomous engine monitoring/control system: Monitoring/control of engine room system, transmission of the engine monitoring/control information to the autonomous ship control mechanism.
- Advanced sensor module: Integration of information from each sensor and transmission of the integrated sensor information to the autonomous navigation system.
- Bridge automation system: Reception of nautical alarms from NAVTEX, log maintenance, maintenance of course via autopilot, and transmission of alarm information and navigation logs to the autonomous navigation system.
- Engine automation system: Collection of engine information and transmission to the autonomous engine monitoring and control system.
- Sensor A: Detection of obstacles.

(Below has been omitted)

- Data on failures and defects in each component included in the analytical target scope.
  - Sensor A failure rate: One (1) failure per unit, per year.

(Below has been omitted)

Figure A1.1 shows a model of a hypothetical autonomous ship that uses the modeling method [10], an application of UML class diagrams, as an example of modeling a new feature used for autonomous navigation among the information summarized to determine the analytical target scope.

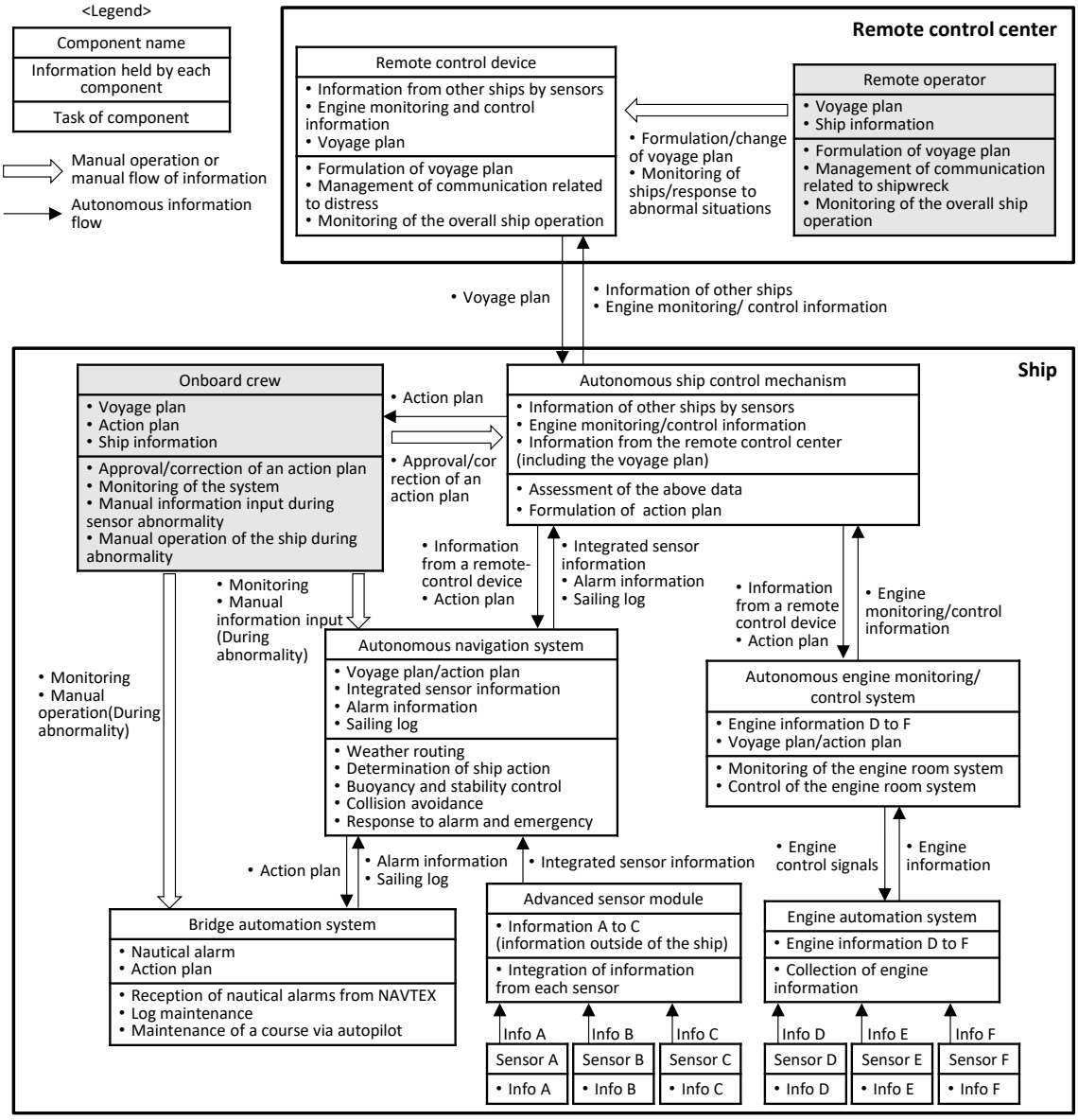

Figure A1.1. An example of modeling a hypothetical autonomous ship.

Appendix 2. An example of hazards to consider

Table A2.1 shows examples of hazards to consider by summarizing hazards from each class guide [4], [8], and [9] and existing studies [11]–[14].

Table A2.1. 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

Appendix 3. 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 A3.1. 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 A3.1 shows a summary of the characteristics of the above methods and SWIFT.

Table A3.1. 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	Concept study, concept design,	Concept study, concept design,

	detailed design			detailed 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 manhours 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.

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)