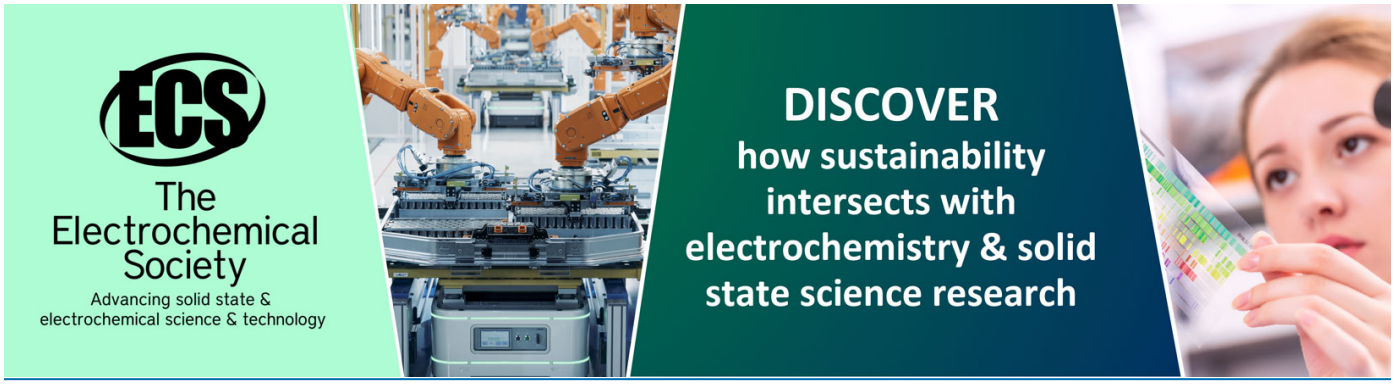
Evaluation of effectiveness of the STAMP / STPA in risk analysis of autonomous ship systems



Evaluation of effectiveness of the STAMP / STPA in risk analysis of autonomous ship systems

Tomoaki YAMADA[1*], Makoto SATO[1], Rikiya KURANOBU[1], Ryo WATANABE[1], Hiroko ITOH[2], Megumi SHIOKARI[2], Tomohiro YUZUI[2].

1 Nippon Kaiji Kyokai, Japan

2 National Maritime Research Institute, National Institute of Maritime, Port and Aviation Technology, Japan

Corresponding author: Tomoaki YAMADA; e-mail: t-yamada@classnk.or.jp;
Tel.: 81 3 52262737 Fax: 81 3 52262736

Abstract. To ensure safety of Maritime Autonomous Surface Ships (MASS), the importance of risk assessment is emphasized in classification societies, but the assessment method is not specified, and standardization of the method is expected. In the risk analysis of conventional ship, we focus on equipment failure mainly on hardware, but in MASS, it is necessary to analyze not only hardware but also large-scale and complicated systems including software and human beings. STAMP / STPA is an analysis method for large-scale and complicated systems, and it may be applicable to MASS risk analysis. In this paper, we will verify the effectiveness of STAMP / STPA in the initial stage of MASS design and consider it from a certification point of view.

1. Introduction

Maritime Autonomous Surface Ship (hereinafter MASS) is a large-scale and complicated system consisting of many functional groups. When determining a concept of a MASS, it is important to organize a wide variety of onboard tasks from the perspective of "to what extent" and "which tasks" are autonomous (automated or remotely controlled) in the MASS [1]. For example, system configuration for maneuvering tasks of MASS is constituted conceptually of a group of sensors for collecting information, a group of cognitive functions for analyzing and recognizing information on other ships and obstacles from the input information, and a group of control functions that control the direction and propulsion of the ship based on the voyage plan approved before departure and the action plan for avoiding obstacles on the route. In addition, a communication system between the MASS and the Remote Operation Center (hereinafter ROC) is required for remote monitoring and emergency response.

The necessity of new goal-based MASS instrument is being discussed at International Maritime Organization (IMO). From certification point of view, in the case of MASS, a highly complicated system will be installed, and it is difficult to set uniform requirements for such a large-scale system. Even for systems with the same function, the requirements and performance standards specified for certification might differ depending on the conditions under which it is operated. To ensure goal-based safety, risk management from the early design stages is important.

The interim guidelines issued by IMO [2] and guidelines issued by some flag states [3]-[5] specify the implementation of risk assessment. Guidelines for MASS have already been issued by multiple classification societies [6]-[9], and risk assessment is also emphasized in all of them. For example, in ClassNK guidelines [6] it is necessary to carry out risk assessment depending on the development phase of the autonomous ship system.

On the other hand, there are no clear rules or guidelines regarding the method used for risk assessment, and the choice is up to the system supplier. Therefore, there are some cases where risk assessment is not always performed in the form intended by third-party certifiers such as classification societies, and standardization of risk assessment methods according to the development phase is expected in the industry.

In particular, in large-scale and complicated systems, not only failure of individual components / subsystems, but also hazards hidden in the interaction between components / subsystems may lead to accidents such as collisions, grounding, and sinking. In the conventional risk analysis for ships, hazards have been identified by focusing on equipment failures using a system configuration diagram mainly consists of hardware, but in risk analysis for MASS, it is important to comprehensively extract hazards based on the above characteristics. For that purpose, by aggregating hardware, software and human beings, etc. that compose MASS are regarded as one big system, and it is necessary to clearly define the task that each component of the entire system is in charge of, the processes for the exchange of information between the components / subsystems, and the processes that require human approval from the initial stage of design [10]-[12].

As a safety analysis method for large-scale and complicated systems, system-theoretical approaches such as STAMP / STPA (Systems-Theoretic Accident Model and Processes / System Theoretic Process Analysis) [13] are attracting attention. STAMP / STPA is an analysis method that considers hazard factors in units of interacting functions [13], and is considered to be useful for risk analysis in the early stages of designing large-scale and complicated systems. It is also considered useful to select an appropriate analysis method according to the design stage [14],[15]. The application of STAMP / STPA to the autonomous ship system has already been studied in multiple papers [15]-[21].

In this paper, we evaluate the effectiveness of STAMP / STPA to a risk assessment in the initial stage of MASS design, and also considered how STAMP / STPA works in goal-based safety evaluation process from a certification point of view.

2. Analysis

2.1. Subject for analysis

In this study, the unmanned bridge ship that operate automatically under remote monitoring at ROC is analyzed. STAMP / STPA was performed on “the hypothetical autonomous ship” defined by Shiokari et al. (2021). Figure 1 shows the conceptual structure of “the hypothetical autonomous ship” set in this paper, and Table 1 shows the outline. In this paper, we consider only the mechanism from a technical point of view, and do not deal with legal issues (such as seafarers’ allocation and qualification requirements).

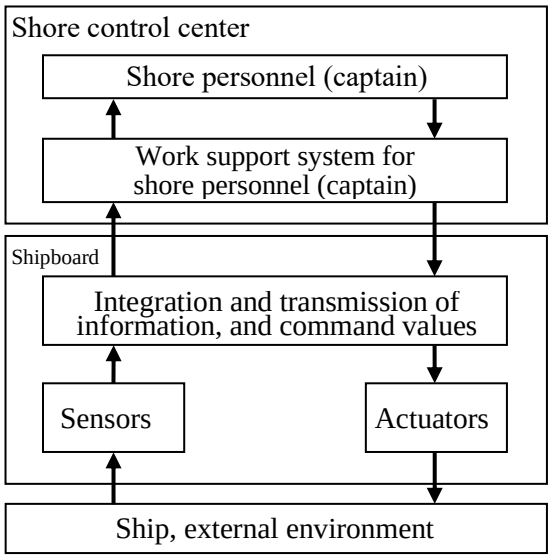


Figure 1. Conceptual structure of the hypothetical autonomous ship [11]

Table 1. Outline of the hypothetical autonomous ship

Degree of autonomy	Unmanned bridge - Autonomous "planning of operation and decision for ship maneuvering" and "condition check for equipment and automation system" - The decision maker is a remote operator (captain) on ROC. - Installed "emergency response system" for emergency response onboard
Target of autonomy	Navigation task on bridge (automation and remote monitoring)
Size of MASS	less than 500 GT class
Assumed route	Short-distance regular route
Others	- No ballast adjustments will be made during the voyage. - Mooring relies on port equipment.

2.2. Method (STAMP / STPA)

Figure 2 shows the basic STAMP / STPA method. In this study, risk analysis for the hypothetical autonomous ship was performed using this procedure. Information-technology promotion agency's STAMP Workbench [22] is used for analysis. This analysis was carried out by multiple people with different specialties, those who are familiar with risk assessment methods including STAMP / STPA, those who have experience in designing automated systems, and those who have experience for certification work in classification societies.

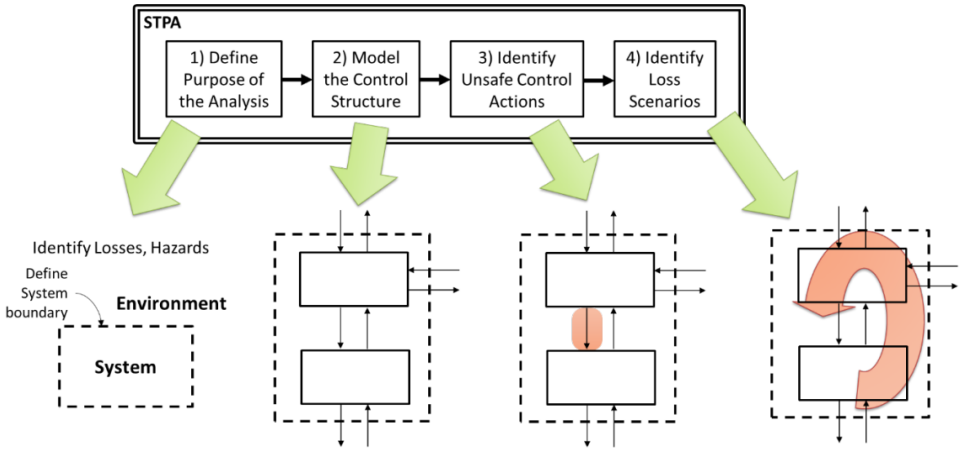


Figure 2. Overview of the basic STAMP / STPA Method [13]

3. Result

3.1. (Step 1) Define Purpose of the Analysis

As the first step of STAMP / STPA, hazards and safety constraints (hereinafter SC) were extracted after identifying losses for the autonomy of ship maneuvering tasks. The results are shown in Table 2. In this analysis, in order to consider the safety constraints that should be achieved as the entire MASS, we started with the highest concept of "ship".

Table 2. Hazard identification and safety constraints

ID	Hazard	ID	Safety constraints
H1	The MASS is too close to other ships and drifting objects.	SC1	The MASS should not approach too close to other ships nor drifting objects.
H2	The MASS is too close to the quay.	SC2	The MASS should not approach too close to the quay.
H3	The MASS is too close to shallow water.	SC3	The MASS should not approach too close to shallow water.
H4	The MASS loses stability.	SC4	The MASS should not lose stability.
H5	The MASS tilts abnormally.	SC5	The MASS should not tilt abnormally.
H6	There is something wrong with the fire prevention / extinguishing equipment of the MASS.	SC6	There should be no abnormality in the fire prevention / extinguishing equipment of the MASS.
H7	The acceleration of the MASS is too large.	SC7	The acceleration of the MASS should not be too large.
H8	The MASS blacks out.	SC8	The MASS should not black out.
H9	An engine abnormality occurs on the MASS.	SC9	There should be no abnormality in the MASS's engine.
H10	An abnormality occurs in the maneuvering and propulsion equipment of the MASS.	SC10	There should be no abnormalities in the maneuvering and propulsion equipment of the MASS
H11	An abnormality occurs in the fuel oil system of the MASS.	SC11	There should be no abnormality in the fuel oil system of the MASS.

3.2. (Step 2) Model the Control Structure

Figure 3 shows the modeled control structure diagram (hereinafter CS diagram). Regarding communication between the MASS and ROC, each onboard system independently transmits information to ROC.

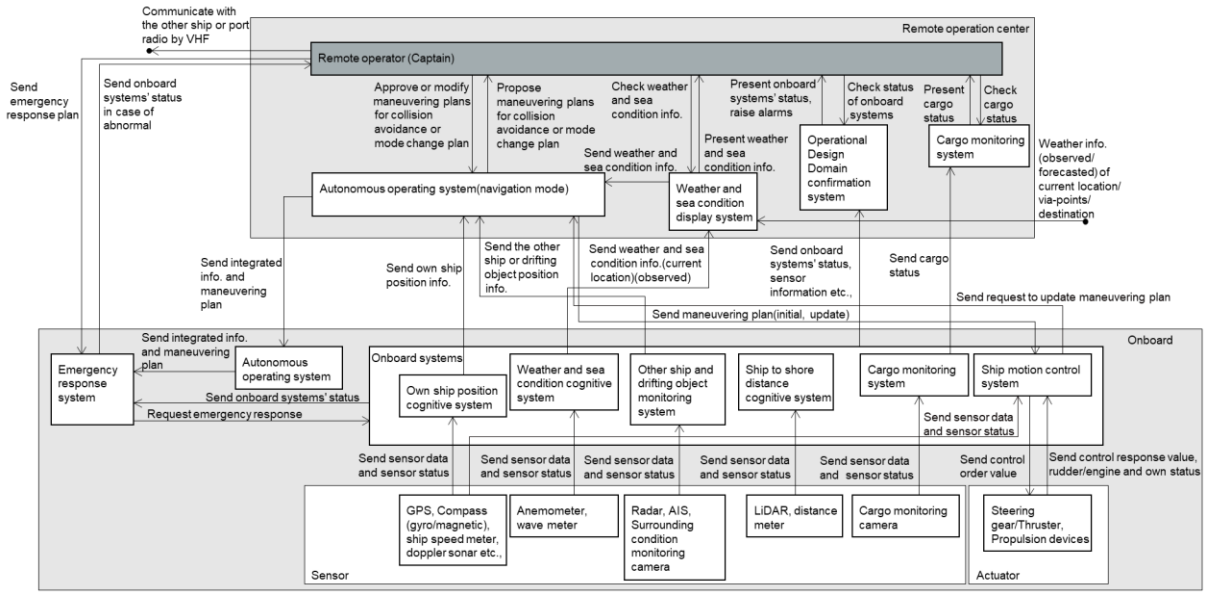


Figure 3. Control structure diagram of the hypothetical autonomous ship

3.3. (Step 3) Identify Unsafe Control Actions (UCA)

Table 3 shows typical UCAs identified in this study. Since the purpose is not to focus on equipment failure but to comprehensively identify hazards for the entire MASS system, we selected UCAs that include information exchange between each component / subsystem such as hardware, software, and humans, and processes that require human approval. “Stop too soon / Applying too long” was not extracted in Table 3.

Table 3. UCA identified

(UCA No) CA	(UCA No.) Not Providing [related safety constrains]	(UCA No.) Providing causes Hazard [related safety constrains]	(UCA No.) Too early / Too late [related safety constrains]	Stop too soon / Applying too long
(UCA3) Check status of onboard systems (from Remote operator (captain) to Operational Design Domain confirmation system)	(UCA3-N-1) The remote operator (captain) does not check the status of onboard systems. [SC1][SC3][SC6][SC7][SC8][SC9][SC10][SC11]	(UCA3-P-1) The remote operator (captain) misidentifies the status of onboard systems. [SC1][SC3][SC6][SC7][SC8][SC9]SC10][SC11]	(UCA3-T-1) Too late： Confirmation of onboard systems by remote operator (captain) is delayed. [SC1][SC3][SC6][SC7][SC8][SC9][SC10][SC11]	Nil
(UCA7) Send integrated info. and maneuvering plan (from Autonomous operating system (ROC) to Autonomous operating system (onboard))	(UCA7-N-1) Do not send integrated information even when the transmission time comes. [SC1][SC3][SC4][SC5][SC6][SC7][SC8][SC9][SC10][SC11]	(UCA7-P-1) Send with errors in the integrated information. [SC1][SC3][SC4][SC5][SC6][SC7][SC8][SC9][SC10][SC11]	(UCA7-T-1) Too late：Delayed transmission of integrated information. [SC1][SC3][SC4][SC5][SC6][SC7][SC8][SC9][SC10][SC11]	Nil
(UCA16) Send onboard systems' status, sensor information, etc. (from Onboard systems to Operational Design Domain confirmation system)	(UCA16-N-1) Onboard systems does not send own status, sensor information, etc. [SC1][SC3][SC4][SC5][SC6][SC7][SC8][SC9][SC10][SC11]	(UCA16-P-1) The onboard systems send inappropriate own status, sensor information, etc. [SC1][SC3][SC4][SC5][SC6][SC7][SC8][SC9][SC10][SC11]	(UCA16-T-1) Too late： Transmission of own status, sensor information, etc. from onboard systems is delayed. [SC1][SC3][SC4][SC5][SC6][SC7][SC8][SC9][SC10][SC11]	Nil

3.4. (Step 4) Identify Loss Scenarios

For the UCA identified in Section 3.3, control loop diagrams between components / subsystems were developed by paying attention to the connection and operation between the component / subsystem. The hint word set for HCF (Hazard Causal Factor) [22] were also utilized to identify the HCF. As an example of a control loop diagram, Figure 4 shows a diagram of onboard systems and operational design domain (hereinafter ODD) confirmation system. Table 4 shows a summary of the loss scenarios for UCAs extracted in this way and their countermeasures.

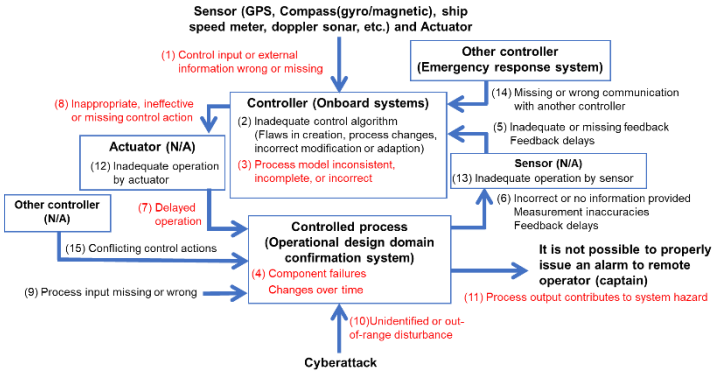


Figure 4. Control loop diagram between onboard systems and Operational Design Domain confirmation system

Table 4(a). Loss scenarios for UCAs extracted and countermeasures (UCA3-N-1)

HCF (HCF No.)	Loss scenarios	Countermeasures
The remote operator (captain) forgets/neglects to check the status of onboard systems periodically. (HCF3-N-1-6)	An error occurs in onboard systems and deviates from ODD. - The ODD confirmation system displays deviation from ODD without alarm. - The remote operator (captain) does not confirm the ODD confirmation system due to other operations, - The remote operator (captain) does not notice any abnormalities and does not give any instruction to the emergency response system. - Improper autonomous maneuvering will continue, and the MASS may approach or collide with other ships or drifting objects.	<Measures to prevent the occurrence of HCF> - Thoroughly pre-instruction to the remote operator (captain) that regular confirmation is required even if the alarm does not sound. - Addition of alarm function to periodically prompt confirmation to the remote operator (captain). - Optimization of the workload of remote operator (captain)
The remote operator (captain) does not notice the alarm. (HCF3-N-1-12)	An error occurs in the onboard systems and deviates from ODD. - An alarm is issued from the ODD confirmation system to the remote operator (captain), but the remote operator (captain) does not notice alarm because the alarm volume setting is low / the alarm is turned off by mistake / physical condition of the remote operator (captain) is bad. - The remote operator (captain) does not notice any abnormalities and does not give any instruction to the emergency response system. - Improper autonomous maneuvering will continue, and the MASS may approach or collide with other ships or drifting objects.	<Measures to prevent the occurrence of HCF> - Optimization of alarm volume. - Visually noticeable alarm <Measures to prevent accidents even if HCF occurs> - Thoroughly pre-instruction to the remote operator (captain) that regular confirmation is required even if the alarm does not sound. - Addition of detection function of remote operator (captain) condition
The ODD confirmation system has not received the information. (HCF3-N-1-15)	An error occurs in the onboard systems and deviates from ODD. - Onboard systems' error cannot be sent due to sensor failure, communication device failure or cyberattack, etc. - Since the ODD confirmation system has not received the error information, the error is not displayed on monitor and alarm is not issued. - The remote operator (captain) does not confirm the ODD confirmation system. - The remote operator (captain) does not notice any abnormalities and does not give any instruction to the emergency response system. - Improper autonomous maneuvering will continue, and the MASS may approach or collide with other ships or drifting objects.	<Measures to prevent the occurrence of HCF> - Ensuring the reliability of communication between the MASS and ROC - Implementation of reliable cyber security measures - Ensuring the redundancy of sensors - Ensuring the reliability of each onboard system <Measures to prevent accidents even if HCF occurs> - Alarm function to communication abnormality independent of the ODD confirmation system

Table 4(b). Loss scenarios for UCAs extracted and countermeasures (UCA7-N-1and UCA7-P-1)

HCF (HCF No.)	Loss scenarios	Countermeasures
The Autonomous operating system (ROC) cannot send integrated information due to poor communication status. (HCF7-N-1-1)	The Autonomous operating system (ROC) cannot send integrated information to the Autonomous operating system (onboard) due to poor communication. - The latest integration information is not sent from the autonomous operating system (onboard) to the emergency response system. - Even if the emergency response system finds the mismatch between information from autonomous operating system and information from onboard systems, its findings cannot be sent to the remote operator (Captain) due to poor communication status. - Because the remote operator (captain) does not pay special attention to the autonomous operating system due to dozing or sudden illness, etc., the remote operator (captain) cannot notice the poor communication status. - Autonomous maneuvering continues with poor communication status, and the MASS may approach or collide with other ships or drifting objects.	<Measures to prevent the occurrence of HCF> - Ensuring the reliability of communication between the MASS and ROC - Implementation of cyber security measures <Measures to prevent accidents even if HCF occurs> - Addition of function to check the current communication status of the autonomous operating system - Installation of a function that can detect and report doze and sudden illness of remote operator (Captain)
Each information of the integrated information is missing or incorrect (HCF7-P-1-1)	Each information of the integrated information (position of own ship / other ships / drifting objects, weather and sea condition, etc.) is missing or incorrect. - The MASS may be maneuvered based on an incorrect decision, and the MASS may approach or collide with other ships or drifting objects.	<Measures to prevent the occurrence of HCF> - Addition of function to verify reliability of each information of integrated information - Development of reliable calculation algorithm <Measures to prevent accidents even if HCF occurs> - Examination of countermeasures when reliability is low

Table 4(c). Loss scenarios for UCAs extracted and countermeasures (UCA16-P-1)

HCF (HCF No.)	Loss scenarios	Countermeasures
Incorrect information is sent to the ODD confirmation system due to improper processing by some of onboard systems. (HCF16-P-1-1)	Incorrect information is sent to the ODD confirmation system due to improper processing by some of onboard systems. - Since the ODD confirmation system processes based on incorrect information, it is not possible to issue an alarm properly. - Even if the MASS status is out of ODD, the remote operator (captain) does not give an instruction to the emergency response system because the alarm is not issued properly. - Improper autonomous maneuvering will continue, and the MASS may approach or collide with other ships or drifting objects.	<Measures to prevent the occurrence of HCF> - Ensuring data quality - Ensuring the redundancy of sensors <Measures to prevent accidents even if HCF occurs> -Addition of function to onboard systems to verify the reliability of each sensor information. And do not send sensor information to the ODD confirmation system if reliability is suspected. -Addition of function to the ODD confirmation system to notify the remote operator (captain) of an error when the information from onboard systems is missing.

From Table 4, we got the awareness from two viewpoints, one that leads to the improvement of the CS diagram and another that leads to the detailed design (concrete functional requirements) of each component / subsystem.

For example, the following items were extracted as common to multiple HCFs that would lead to the improvement of the CS diagram.

Improvement points of the CS diagram for the ROC are shown as follows.

- Review of the number of people performing tasks at ROC (it is necessary to change the composition that one remote operator (captain) must check the status of the onboard systems.)
- Clarification of countermeasure when the remote operator (captain) is in poor physical condition (Establishment of fallback system in ROC)"
- Installation of a component / subsystem that can detect and report doze or sudden illness of remote operator (captain).

Similarly, the following items were extracted as those that lead to the detailed design (materialization of functional requirements) of each component / subsystem.

- For the systems on ROC, "reliable cyber security measures", "audiovisually noticeable alarms", and "alarm function to communication abnormality between the MASS and ROC" are required.
- For onboard systems (own ship position cognitive system, weather and sea condition display system, other ship and drifting object monitoring system, etc.), "function to verify reliability of each information of integrated information" and "development of reliable calculation algorithm" are required.

4. Discussion

4.1. Consideration of system safety design through validity verification of conceptual design from a certification point of view

In the case of MASS, a highly complicated system will be installed, and it is difficult to set uniform requirements for such a large-scale system. This is because even if the system has the same function, the requirements and performance standards to be specified differ depending on the conditions under which it is operated [1],[6],[10].

The policy of the NK guidelines [6] is goal-based. In case of ClassNK, examinations based on the functional requirement specifications of autonomous operation systems will be conducted. For example, the NK guidelines describe the basic elements for ensuring safety that should be considered at the conceptual design stage. The purpose of this is to correctly understand the characteristics of the autonomous operation system by organizing the information based on these basic elements. Table 5 shows a summary of the basic elements for the hypothetical autonomous ship dealt with in this study.

Table 5. Items to be considered at conceptual design phase and the settings in the hypothetical autonomous ship [6], [11]

Basic elements for ensuring safety	Model of the hypothetical autonomous ship
Target task of automated operation on a ship	Ship maneuvering tasks in each phase (planning, berthing and unberthing, and voyage)
Division of roles between humans and automated operation systems	Situation awareness：Onboard systems Decision：Remote operator (captain) Action：Onboard systems
Prerequisite specification for system installation	See the sensors and actuators in Figure 3. Surrounding condition monitoring cameras, LiDAR, distance meters, cargo monitoring camera, and communication antennas for onboard systems to send information to and ROC are notable differences from conventional ships.
Operational design domain (ODD)	Materialized at detailed design
Fallback executor	Emergency response system
Human machine interface (HMI)	Materialized at detailed design
Cyber security	Materialized at detailed design
Reliability of computer systems	Materialized at detailed design

In the actual examination by ClassNK, a document examination and a function verification test are performed to confirm the validity of the design and that the developed system meets the functional requirement specifications. The document examination also includes a review of risk assessment results. In addition to confirming that the validity of the overall system configuration has been properly verified, it is also an important point whether the three relationships between ODD, fallback, and MRC (Minimum Risk Condition) are properly designed. As for the function verification test, the test items are to be decided according to the characteristics of the autonomous operation system. So, it is important to properly organize the functional requirements of the autonomous operation system in advance. That is why, the NK guidelines also mention the design and development process, and the application of the Verification and Validation (V&V) processes is recommended as an example in order to execute this flow effectively. The general procedure of V&V process is as follows.

a) Validation of conceptual design
b) Extraction of functional requirements for each component / subsystem to be considered during detailed design
c) Verification for each component / subsystem
d) Verification for integrated subsystem
e) Validation of the entire system

Although it is possible to receive a review of classification societies with complete evidence after the V&V process has been completed, it is also expected that the time required for examination for certification will be shortened by adding classification societies to the flow of this V&V process and conducting a step-by-step review.

In this study, consideration from a certification point of view using the NK Guidelines [6] for the analysis results of "the hypothetical autonomous ship" by STAMP / STPA were performed. Assuming analysis for conceptual design and keeping Approval in Principle (AiP) in mind, STAMP / STPA was applied to the processes a) and b). At the conceptual design stage, the validity of the entire system is mainly confirmed rather than the details of the subsystem / component.

4.1.1. Validity of conceptual design. As described in Section 3.4, the following notices have been obtained through the analysis, which will lead to the improvement of the CS diagram.

- Review of the number of people performing tasks at ROC (it is necessary to change the composition that one remote operator (captain) must check the status of the onboard systems.
- Clarification of countermeasure when the remote operator (captain) is in poor physical condition (Establishment of fallback system in ROC)
- Installation of a component / subsystem that can detect and report doze or sudden illness of remote operator (captain).

Based on this awareness, the modified CS diagram in which remote operator monitoring system is newly installed is shown in Figure 5.

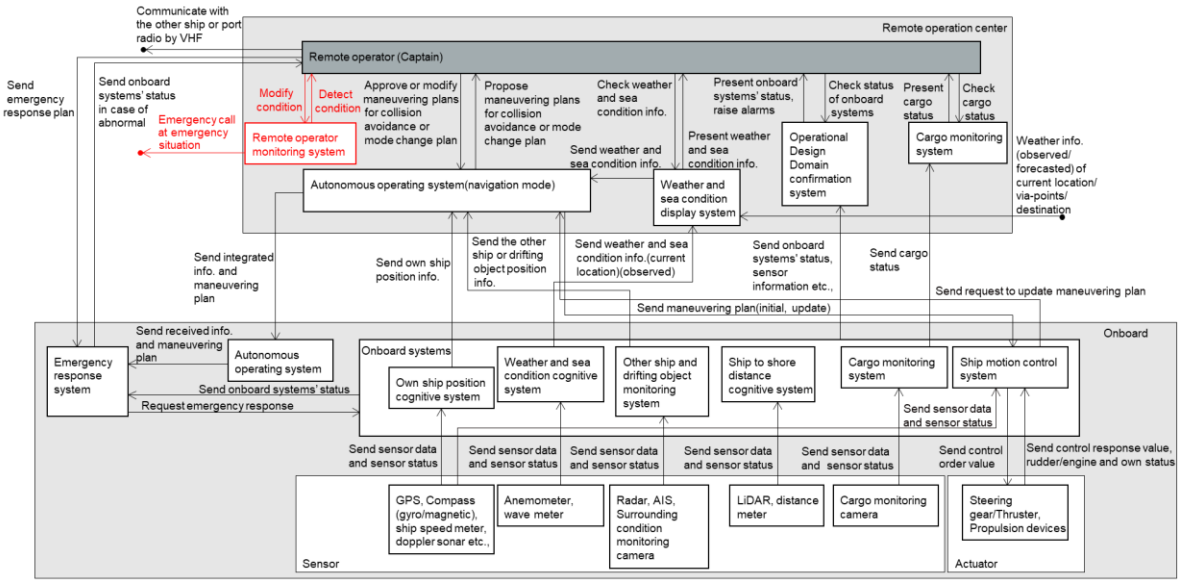


Figure 5. Modified CS diagram

Although not reflected in Figure 5, the analysis in this study clearly showed that there are a large number of functional requirements for each component / subsystem, especially those required of remote operator (captain). With this in mind, we can review the minimum number of people required in ROC at the conceptual design stage. Also, it is important to thoroughly consider the necessary HMI of ROC equipment required at the detailed design stage. These items could be functional requirements for the ROC operations and ROC equipment, respectively.

In this way, by describing loss scenarios and examining countermeasures, the CS diagram could be improved. It can be said that the validity of the conceptual design could be verified by STAMP / STPA. According to the NK guidelines, it is necessary to confirm the safety of the design of the autonomous system by using an appropriate risk analysis method. From the result of this study, it is considered that the verification required by the classification society can be effectively carried out by using STAMP / STPA at conceptual design phase.

4.1.2. Extraction of functional requirements (for component / subsystem) to be considered during detailed design. As described in Section 3.4, applying STPA to the CS diagram (Figure 3) modeled by STAMP, we got the awareness which will lead to the detailed design (materialization of functional requirements) of each component / subsystem.

For the systems on ROC, awareness has been obtained that following items are required:

- reliable cyber security measures,
- audiovisually noticeable alarms, and
- alarm function to communication abnormality between the MASS and ROC

For onboard systems (own ship position cognitive system, weather and sea condition display system, other ship and drifting object monitoring system, etc.), following items are required:

- function to verify reliability of each information of integrated information and
- development of reliable calculation algorithm

By paying attention to the cooperation between components / subsystems, for example, it is possible to realize the necessity of having a function to check the reliability of the received information in the downstream subsystem (the subsystem that receives the information). In addition, it has been possible to extract specific requirements for HMI of components / subsystems that require cooperation with humans. In this way, STPA makes it possible to extract the functional requirements of subsystems / components in consideration of the characteristics of autonomous operating systems.

It will lead to a great reduction in development rework by sharing and agreeing on the functional requirements extracted in this way with the certification side such as classification societies. In addition, the content and method of the test to be carried out in step c) can be efficiently discussed with certification side.

4.1.3. Consideration for test method (Verification). In this study, it was confirmed that the upstream part of V & V process can be effectively carried out even for the hypothetical autonomous ship by analyzing the CS diagram modeled by STAMP / STPA. On the other hand, once the CS diagram can be modeled, it is possible to check or sophisticate it virtually by computer simulation such as 1D simulation, and such efforts are being promoted in the automobile industry, etc., which model-based development has already been adopted. In the shipping industry as well, the Comprehensive Simulation System for MASS is being developed by Minami et al. [24]. In this paper, verification using 1D simulation has not been carried out, but it is considered effective to combine STAMP / STPA and 1D simulation as a method to consider the validity of the MASS design efficiently and effectively.

4.2. Points to keep in mind when applying the STAMP/STPA method to MASS widely

(1) Safety Constraint

Assuming that designers who are unfamiliar with STAMP / STPA will analyze by themselves, there is a concern that considerably disjointed SCs will appear.

Therefore, it is effective to present the market view of SC by presenting analysis examples. Based on such analysis examples, it is important to share the awareness among stakeholders about the safety level required for the system from the initial design stage.

(2) UCA

While the UCA could be extracted efficiently by having the guide words, the work of describing the UCA in combination with the guide words is monotonous and mechanical work continues. If the CS diagram is drawn in too much detail from the beginning, the amount of work will be enormous. By keeping the appropriate size of the component / subsystem to be analyzed in such as information gathering / situation awareness / decision / action (control), it is possible to efficiently define UCA.

(3) HCF and Loss scenarios

The points that we noticed when describing the loss scenarios in this study are shown below.

- When extracting HCF, it is unclear whether to describe the scenarios that lead to all related SC violations or only the most probable scenario.
- The interaction between components / subsystems can be expressed as CA, but the interaction between CAs (dependency, order of CAs in time series, etc.) is difficult to express.
- When extracting the HCF, whether to consider not only the direct causes of UCA but also the indirect causes or not. Combinatorial explosions can be occurred if the cause investigation is traced back too much to.

Since there is no clear explanation for these points in the method, it can be said that it is necessary to set rules when performing analysis.

(4) Consideration throughout

The major feature of the maritime industry is that there are many stakeholders, but the structure becomes more complicated in MASS, where the concept of operation (CONOPS) and the degree of system autonomy must be considered in parallel. Therefore, risk analysis for MASS tends to be complicated as well, but at least at the conceptual design stage, it is possible to carry out risk analysis, which some classification societies can accept, by using STAMP / STPA.

In the case of MASS, it seems that STAMP / STPA is more effective when the system scale is large and the degree of design progress is upstream. On the other hands, as the design goes downstream, conventional methods may be easier to use for stakeholders in the shipping industry. Therefore, it is necessary to select a method according to both the size of target system and the degree of design progress, considering whether the analysis target is a ship or system as well as conceptual design or detailed design.

5. Conclusions

In this study, STAMP / STPA [13] was carried out for the hypothetical autonomous ship by Shiokari et al. (2021), and the effectiveness of STAMP / STPA at the conceptual design stage of MASS was evaluated, together with consideration how STAMP / STPA works in goal-based safety evaluation process from a certification point of view. The findings obtained in this study are summarized below.

a) By using STAMP / STPA for risk analysis at the conceptual design stage of MASS, it is possible to easily share the characteristics of the autonomous operation system with the certification side such as classification societies. In addition, the analysis result can be used as a material for the classification societies' review for AiP and so on. For example, the NK guideline requires "system architecture that gives an overview of the autonomous operation system" at the time of examination, and the CS diagram modelled by STAMP/STPA can be utilized as this material.
b) In this study, we showed that STAMP / STPA extracted the functional requirements for the hypothetical autonomous ship. By sharing and agreeing on the extracted functional requirements with the certification side such as classification societies, it is expected to reduce development rework and help analysts efficiently consider the content and method of the test to be conducted. On the other hand, we analyzed the typical use cases assumed from the system model and extracted the functional requirements this time, but since multiple different uses are possible depending on the system model, it is necessary to organize the use cases and consider the relationship with the functional requirements.
c) Considering that there are many possible forms of autonomous operating systems, it is also necessary to perform risk assessment in a form that is easy for certifiers to review. From that point of view, this paper has showed the possibilities that STAMP / STPA can work effectively as a method of both risk assessment and extraction of functional requirements. On the other hand, STAMP/STPA is still unfamiliar in the maritime industry, especially for ship designer. This means there is a risk that the analysis by ship designer may become analyst-dependent. In order to solve this, it is necessary to present an analysis example like this paper and proceed with standardization.

Acknowledgements
This work was partly supported by JSPS KAKENHI Grant Number JP20K14969.

References

[1] Yamada T: Safety Evaluation for Technologies related to Autonomous Ships, ClassNK Technical Journal No.3, 2021(I)
[2] IMO MSC.1/Circ.1604 (2019), INTERIM GUIDELINES FOR MASS TRIALS
[3] Maritime Bureau, Ministry of Land, Infrastructure, Transport and Tourism: [Guidelines for Safety design of MASS] Jidouunkousen no anzen sekkei gaidorain (2020) (Japanese)
[4] VTMIS, EU OPERATIONAL GUIDELINES FOR SAFE, SECURE AND SUSTAINABLE TRIALS OF MARITIME AUTONOMOUS SURFACE SHIPS (MASS)
[5] Norwegian Maritime Authority, RSV 12-2020: Guidance in connection with the construction or installation of automated functionality aimed at performing unmanned or partially unmanned operations
[6] ClassNK: Guidelines for Automated/Autonomous Operation on ships (Ver. 1.0) (2020)
[7] DNVGL: Autonomous and remotely operated ships, DNVGL-CG-0264 (2018)
[8] Bureau Veritas: Guidelines for Autonomous Shipping, Guidance Note NI 641 DT R01 E (2019)
[9] ABS: ABS advisory on autonomous functionality (2020)
[10] Shiokari M, Itoh H and Yuzui T: Towards the Development of Risk Analysis Method for Autonomous Ships, Conference proceedings of the Japan Society of Naval Architects and Ocean Engineers, No. 30, 393–396, 2020. (In Japanese)
[11] Shiokari M, Itoh H, Yuzui T, Ishimura E, Miyake R, Kudo J and Kawashima S: Application of

Risk Analysis Method with System Modeling to Conceptual Design of Autonomous Ships, Conference proceedings of the Japan Society of Naval Architects and Ocean Engineers, No. 32, 355–366, 2021. (In Japanese)
[12] Itoh H, Yuzui T, Shiokari M, Ishimura E, Miyake R, Kudo J: Risk Assessment of Autonomous Ship Systems, ClassNK Technical Journal No.4, 2021.
[13] Leveson NG and Thomas JP, STPA handbook, 2018.
[14] Yamaguchi S, Shirasaka S: Evaluation of the Sequential Safety Analysis Method Based on the Related Severity of Hazards Using STAMP/STPA, JOURNAL OF JAPAN SOCIETY FOR SAFETY ENGINEERING, Vol. 58 No.2,pp.124-132,2019.
[15] Xiang-Yu Zhou, Zheng-Jiang Liu, Feng-Wu Wang, Zhao-Lin Wu, Ren-Da Cui: Towards applicability evaluation of hazard analysis methods for autonomous ships, Ocean Engineering, 214(October), 2020.
[16] Wróbel K, Montewka J, Kujala P: Towards the development of a system-theoretic model for safety assessment of autonomous merchant vessels, Reliability Engineering and System Safety 178, 209–224 (2018)
[17] Wróbel K, Montewka J, Kujala P: (2018). System-theoretic approach to safety of remotely-controlled merchant vessel. Ocean Engineering, 152(January), 334–345. https://doi.org/10.1016/j.oceaneng.2018.01.020
[18] Børge Rokseth, Odd Ivar Haugen and Ingrid Bouwer Utne: Safety Verification for Autonomous Ships, MATEC Web of Conferences 273, 02002 (2019), ICSC-ESWC 2018. https://doi.org/10.1051/matecconf/201927302002
[19] Hyungju KIM, Odd Ivar HAUGEN, Børge ROKSETH, Mary Ann LUNDTEIGEN: Comparison of Hazardous Scenarios for Different Ship Autonomy Types using Systems-Theoretic Process Analysis, Proceedings of the 29th European Safety and Reliability Conference (2019)
[20] Osiris A. Valdez Banda, Sirpa Kannos, HAZARD ANALYSIS PROCESS FOR AUTONOMOUS VESSELS, Novia Publikation och produktion, serie R: Rapporter 2/2019, ISBN: 978‐952‐7048‐47‐4 (online), ISSN: 1799‐4179 (2019)
[21] Meriam Chaal, Osiris A. Valdez Banda, Jon Arne Glomsrud, Sunil Basnet, Spyros Hirdaris, Pentti Kujala: A framework to model the STPA hierarchical control structure of an autonomous ship, Safety Science 132 (2020) 104939
[22] Information-technology Promotion Agency, Japan: STAMP Workbench, https://www.ipa.go.jp/english/sec/reports/20180330.html
[23] Information-technology Promotion Agency, Japan: The introductory guidebook of STAMP/STPA (in Japanese)
[24] Minami M, Kokubun K, Kobayashi M, Hikida K, Yoshimura K, Sato K, Saito E, Sawada R: Development of Comprehensive Simulation System for Autonomous Ships, ClassNK Technical Journal No.4, 2021(II)