Journal of Physics: Conference Series

PAPER • **OPEN ACCESS**

Model-Based Design and Safety Assessment for Crewless Autonomous Vessel

To cite this article: Takuya Nakashima *et al* 2022 *J. Phys.: Conf. Ser.* **2311** 012024

View the article online for updates and enhancements.

You may also like

- On the use of maritime training simulators with humans in the loop for understanding and evaluating algorithms for autonomous vessels
  Anete Vagale, Ottar L Osen, Andreas Brandsæter et al.
- Utilizing optical spectroscopy and 2,7-difluorofluorescein to characterize the early stages of cement hydration
  J Pauli, A Ramírez, C Crasselt et al.
- Spacecraft autonomous navigation using unscented particle filter-based celestial/Doppler information fusion
  Xiaolin Ning and Jiancheng Fang

The Electrochemical Society
Advancing solid state & electrochemical science & technology

242nd ECS Meeting

Oct 9 – 13, 2022 • Atlanta, GA, US

Early hotel & registration pricing ends September 12

Presenting more than 2,400 technical abstracts in 50 symposia

The meeting for industry & researchers in

BATTERIES
ENERGY TECHNOLOGY
SENSORS AND MORE!

Register now!

ECS Plenary Lecture featuring M. Stanley Whittingham,
Binghamton University
Nobel Laureate –
2019 Nobel Prize in Chemistry

This content was downloaded from IP address 133.11.93.3 on 10/08/2022 at 09:08

doi:10.1088/1742-6596/2311/1/012024

Model-Based Design and Safety Assessment for Crewless Autonomous Vessel

Takuya Nakashima*[1], Koji Kutsuna[2], Rui Kureta[2], Hisaki Nishiyama[2], Tomoya Yanagihara[2], Jun Nakamura[2], Hideyuki Ando[2], Hideaki Murayama[1] and Satoru Kuwahara[3]

[1] Graduate School of Frontier Science, The University of Tokyo, Kashiwa, Japan
[2] MTI Co., Ltd., Tokyo, Japan
[3] Japan Marine Science Inc., Kawasaki, Japan

E-mail: nakashima@s.otpe.k.u-tokyo.ac.jp

Abstract. The Designing the Future of Full Autonomous Ship (DFFAS) Project conducted the crewless maritime autonomous surface ship long-distance demonstration in congested waters in March 2022. This study shows a model-based systematic design methodology and a safety evaluation method for autonomous ships conducted through this project. A reference model of ConOps (Concept of Operations) for autonomous navigation systems is proposed using the DFFAS system as an example. System Theoretic Process Analysis (STPA) is also applied at the subsystem and component levels according to the actual system development phase to extract appropriate granularity of safety requirements.

1. Introduction

In Japan, the ageing of the seafarers for coastal shipping and the difficulty of securing personnel have been big issues, significantly impacting the local economy and related industries. The introduction of autonomous and crewless vessels is expected to solve this problem.

The Nippon Foundation launched ”demonstration tests of The Nippon Foundation MEGURI2040 Fully Autonomous Ship Program” in 2020 to support the development of autonomous technologies. It promotes the transformation of the logistics, economy, and social infrastructure by fostering momentum for further technological development through the world's first successful demonstration of crewless domestic vessels. With the support of this project, the Designing the Future of Full Autonomous Ship (DFFAS) Project was launched, consisting of 30 domestic and foreign companies and institutions.

Based on the concept of "creating the future of crewless maritime autonomous surface ships - a grand design devised by various experts," the DFFAS project aims to develop a crewless vessel with open collaboration. It also aims to develop autonomous navigation and support functions such as monitoring and diagnosis from shore (including a communication system) and remote operation in emergencies.

The DFFAS project successfully carried out the demonstration experiment using a domestic container ship between Tokyo Bay and Ise Bay from February 26 to March 1, 2022. It demonstrated for the first time the use of a comprehensive fully autonomous navigation system (including remote control and land support) for a container ship operating in congested waters.

Content from this work may be used under the terms of the Creative Commons Attribution 3.0 licence. Any further distribution of this work must maintain attribution to the author(s) and the title of the work, journal citation and DOI.
Published under licence by IOP Publishing Ltd

2. Background and Objectives

2.1. Application of MBSE to Autonomous Navigation System Development

When considering the design of an autonomous navigation system, it can be difficult to achieve an optimal system design by reassembling existing components based on conventional functions, as the function of the autonomous system will be changed by a role distribution between humans and machines. The concept of systems thinking is essential to consider overall requirements and functions based on the purpose and goal of the system. Particularly in development with multiple stakeholders, the concept of Model-Based Systems Engineering (MBSE) is effective describing the envisioned system as a model rather than as a natural language to provide a common understanding of the envisioned system.

In the DFFAS project, the conceptual design of an autonomous navigation and operation system has been conducted using the MBSE approach. There are several examples of conceptual design methods for autonomous navigation systems. As described in [1], the design should be materialised by the submitter and approved step by step for obtaining and maintaining approval of an alternative and/or equivalency. Tools and methodologies for autonomous ship design are being discussed [2], but most of the research focus are mainly on the conceptual phase. There are few examples of applying and breaking down this methodology to the autonomous ship to be built.

INCOSE defines MBSE as "the formalized application of modeling to support system requirements, design, analysis, verification and validation activities beginning in the conceptual design phase and continuing throughout product development and retirement. [3]" In this paper, we focused on the "modeling to support system requirements, design, analysis" from the perspective of system safety.

2.2. Establishment of Safety Evaluation Method for Autonomous Navigation Systems

It is important to deal with emergent hazardous events in designing complex systems using new technologies. The objective of a ship operation system is to ensure the safe, timely, and efficient operation of a ship in any environment, and particularly, safety seems to be the main perspective for defining requirements.

Several risk analysis methods for the system of systems have been developed to deal with emergent hazardous events caused by interactions of system components. This paper applies STPA (System Theoretic Process Analysis) based on the concept of STAMP (Systems-Theoretic Accident Model and Processes) proposed by [4]. Safety of the Intended Functionality (SOTIF), which has been discussed in the automotive industry as a complement to functional safety [5], is an approach to ensure safety, including emergent hazards and human factors due to the interaction of systems. In [6], STPA is also introduced as one of the analysis methods for emergent hazards.

There are several hazard analysis results regarding autonomous ship [7]. Some references apply STAMP/STPA to autonomous navigation systems. A framework for analysing and discussing uncertainty in mitigation measures obtained through STPA analysis was provided and the initial-stage concept was analyzed in [8]. A framework to model a hierarchical control structure for the STPA analysis of an autonomous ship was presented in [9]. A preliminary concept of safety validation method using STPA was proposed in [10]. A systematic and systemic hazard analysis and management process for a conceptual design phase were provided in [11]. They applied it to two pre-construction ferries, but the extracted safety actions are still general and broad.

This paper attempts to evaluate the safety of the entire autonomous navigation system, to organise the system requirements based on the evaluation, and to reflect them in the design using STPA.

3. Methodology

3.1. Establishment of ConOps reference model for crewless autonomous navigation system

The development of a system begins with its conceptual design. Concept of Operation (ConOps) is a document that defines the requirements of a system by envisioning its users and their usage scenarios. ConOps is also considered essential in the context of Requirements Engineering. ConOps is also used to study new systems in various fields, such as aerospace [12]. There have been many guidelines for autonomous ships in recent years [13][15][14][16], and some refer to the necessity of ConOps.

It seems to be common that ConOps is a document to confirm the purpose, assumptions, and scope of the system, to support requirements elicitation based on use cases etc., and to involve relevant stakeholders to convince them of the necessity of the system to be built. However, the granularity of this document is not clearly defined, especially for the autonomous navigation system. It is necessary that, by using ConOps, the system's requirements are extracted at an appropriate level of granularity and are utilised without reducing the degree of design freedom. Based on the literature survey on ConOps, a reference model of ConOps is presented using the DFFAS system as an example.

3.2. Establishment of safety requirement elicitation scheme by STPA for detailed design

While extracting appropriate safety requirements and reflecting them in the design is an important process, there seems to be no completely established methodology. For example, safety analysis cannot be performed until the system structure has been realised to some extent, but there are no examples to show how much the system should be realised and at what stage safety analysis should be performed. The implementation of STPA during the requirements definition process of the V-model was systematised [17]. However, the proposed process did not address the case where the requirements are repeatedly detailed and hierarchically divided into subsystems and modules.

Therefore, a step-by-step safety analysis for the system to be developed should be needed. This paper discusses how the safety analysis can function in parallel with the development process and the appropriate granularity of the safety analysis with experts' opinions. By doing this, the flow from the concept to the detailed design of the system using ConOps is concretised.

Figure 1 shows the focus of this paper in the system development process. The italic number in the figure corresponds to the section number of this paper.

4. Result

This chapter introduces the results of the study conducted in the DFFAS project.

4.1. Construction of Concept of Operation

Based on the literature review, the elements necessary for ConOps for autonomous navigation systems has been visualised in Figure 2. In addition to the system's requirements, functions, and components, it is necessary to consider the system's background, purpose, use cases, the external environment, and other external constraints. It is also necessary to consider the risk and impact of the system.

ConOps and Operational Concept are described separately in [18]. In this case, the former is a document from the business strategy viewpoint in promoting the system, and the latter is closer to the ConOps to be discussed here. Also, in some documents, it is mentioned that the system's future development should be considered [19]. Therefore, a chapter on the system's future development to clarify the current position of the envisioned system is included.

Based on the contents in Table 1, the Concept of Operation for the DFFAS system is outlined.

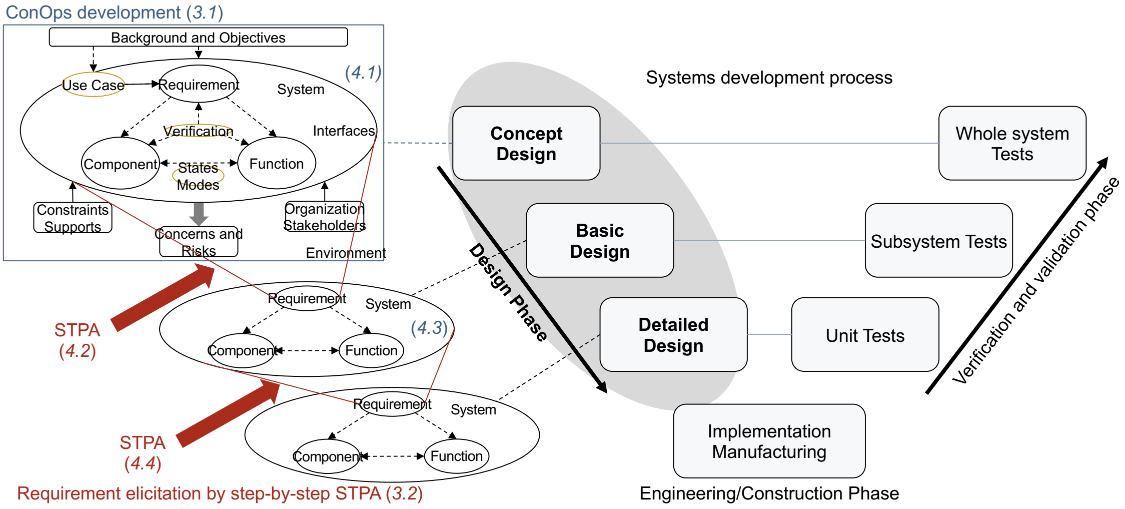


Figure 1. Focus of this paper.

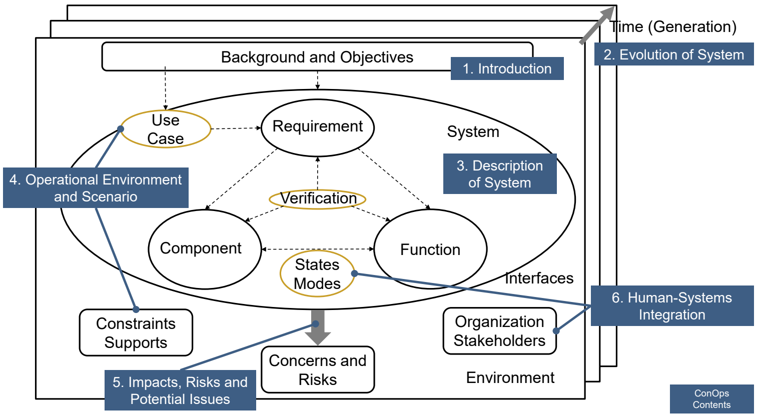


Figure 2. Required elements for system description.

(1) Introduction The background and objectives of the DFFAS project are as described above; to construct a system for unmanned navigation in Japan's coastal shipping lanes and to complete a demonstration experiment.

Table 2 shows the goals and major assumptions for constructing this system. These were determined through discussions within the DFFAS project, in consultation with The Nippon Foundation and other related stakeholders. In addition, the scope of the system to be built has been detailed in Table 3 based on the goals and assumptions.

(2) Evolution of systems There are various possible use cases for introducing unmanned systems, both in terms of time and area. Therefore, developing a general-purpose system that will contribute to the gradual introduction of unmanned navigation systems is necessary to

Table 1. ConOps Contents.

Content	Description
1. Introduction	Background, System Scope, Assumption and Constraints
2. Evolution of System	Justification for changes Future Roadmap and Status of the envisioned system
3. Description of System	Needs, Goals and Objectives of the system Overview Architecture incl. Interfaces (Major System elements and interconnections) Modes of Operation Basic Functions (Proposed Capabilities)
4. Operational Environment and Scenario	Use Cases (Nominal, Off nominal) Actors/Stakeholders Operational Scenario Data flow (input and output of the system)
5. Impacts and Potential Issues	Operational impacts, Environmental Impacts, Organizational Impacts, Scientific/Technical Impacts Regulatory Compliance, How to Implement the system
6. Human-Systems Integration	Human-in-the-loop involvement Human-machine interface etc.
Appendix	Glossary, Acronyms, Reference Documents

Table 2. Goals and assumptions of the DFFAS project.

Goal	- To implement a crewless autonomous vessel based on economic rationality. - To contribute to ensuring maritime safety by reducing the number of accidents caused by human error.
Assumption	- The system should be designed to take advantage of the actual business strengths of various stakeholders, such as shipyards and marine equipment manufacturers. - The system should be implemented at a low cost by utilising existing facilities as much as possible. - The system should be designed to withstand conditions like actual coastal ship operation. (The system should be used in narrow waterways and congested waters.) - Do not aim to make all operations unmanned but focus on the parts that contribute to safe operations and actual business. - The system should be able to be easily backed up by humans in case of emergency.

reduce the workload at sea and ensure maritime safety, regardless of the revision schedule of laws and regulations. This aim is also considered in defining the system's scope.

In addition, open development methodology based on Model-Based Systems Engineering will contribute to developing new concept ships, not just limited to autonomous ships in the future. So, constructing a general framework for many stakeholders to develop and verify novel systems can be a target as well.

Table 3. Scope of the system to be built with DFFAS.

Element	Details
Target ship (Automation functions)	- Retrofit a 749 GRT container ship. (Average size for a Japanese coastal ship). - The actuators are assumed to be standard equipment for general merchant ships.
Internal environment	- A highly autonomous Berth-to-Berth operation system will be established. - Emergency response is assumed to be carried out by the seafarer, and the operator ashore will be in charge of remote operations. - The shipowner and captain will be responsible for maintaining the ship's seaworthiness and formulating long-term voyage plans. - Mooring and cargo handling operations, which are greatly affected by infrastructure development, are outside the scope. - It should be possible to flexibly change the division of roles between machines and humans, and between onboard and ashore, depending on the situation.
External environment	- A situation is assumed where there is a mixture of ships of various autonomous operation levels and existing ships. - Port control is assumed to be existing. No onboard pilot is assumed. - Current navigation rules are to be observed (COLREG, SOLAS, Port regulations and the other domestic laws).

(3) Description of the system Based on the above assumptions, the necessary elements of the system have been organised. First, ship operation and manoeuvring can be divided into seven stages: information acquisition, information integration, situation analysis, planning, plan verification, detailed control order, and execution of control. It is assumed that humans would carry out these tasks with the support of machines and equipment in existing ships. However, in the case of autonomous navigation, the information acquisition, integration, situation analysis and planning would, in effect, be processed continuously by the computer, making it difficult to distinguish between them. Therefore, the function group is divided as shown in Table 4 and Figure 3. The tasks from information acquisition to verification can be divided into strategic and tactical tasks, which may vary depending on the time axis of planning.

It is difficult to operate a vessel with a system in which the roles of man and machine are firmly fixed in a situation in which the ocean, communication environment, and internal system conditions change dynamically. Therefore, it is required to have a system status manager that can appropriately judge the system's status based on the information obtained.

The system structure to achieve these functions has been defined at the subsystem level in Figure 4. Based on the communication environment and the business feasibility, it is assumed that strategic decisions would continue to be made on land. In addition, an executor for the propulsion subsystem is assumed to be on board, as it seems unfeasible to execute maintenance of current machinery room by automation e.g., robots with manipulators.

The architecture has been created based on the scope mentioned in *(1)* and *(2)*. While assuming the use of existing systems as much as possible, the Fleet Operation and the Central Information Management (CIM) subsystems are two new systems for this novel system. The former is responsible for navigation support from shore. The shipowner is expected to be

Table 4. Basic Function.

Function	Description
Object and Environment Detection (LOED)	A function group corresponds to detecting objects and events via integrating information on a wide-range environment.
Short-term Object and Environment Detection (SOED)	A function group corresponds to detecting objects and events via integrating information on a surrounding environment.
Long-term Event Response and Path Planning (LERPP)	A function group corresponds to planning based on LOED and making a navigation plan.
Short-term Event Response and Path Planning (SERPP)	A function group corresponds to planning based on SOED and making an action plan.
Dynamic train control and Actuation	A function group corresponds to the control and actuation of the ship as planned.
System Status Management	A function group corresponds to managing information of system status.
Communication	A function group corresponds to communication between ship and shore (Fleet Operation Centre: FOC).
Propulsion and Power Management	A function group corresponds to managing electricity and controlling the power systems of the ship.

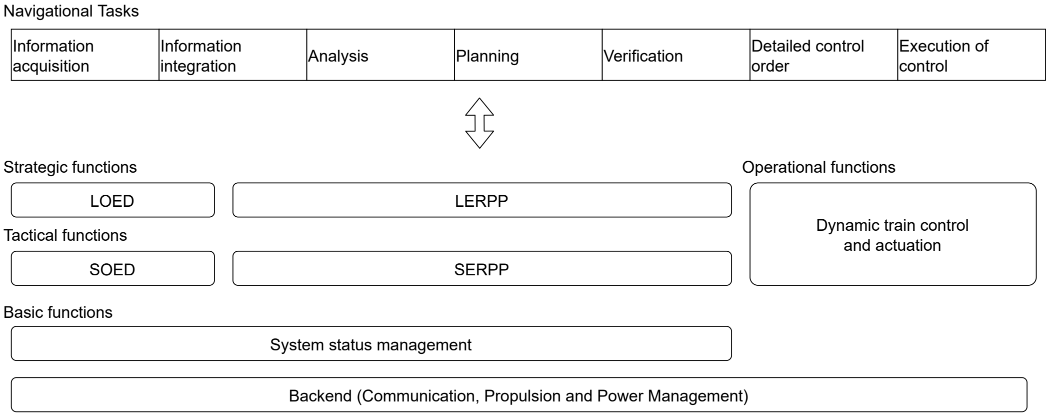


Figure 3. Functions, Tasks, Category of components and Role.

responsible for long-term voyage planning, and the master and crew are also expected to be responsible for monitoring and fallback operations. The latter is responsible for the functions of System Status Management and is designed to change the operational status according to the situation.

(4) Operational Environment and Scenario This section describes the environment surrounding the system, including the use cases, related stakeholders, and data exchanged inside and outside the system. As the assumed scenarios define parts of the functions, it is concretised in an iterative manner with *(3)*.

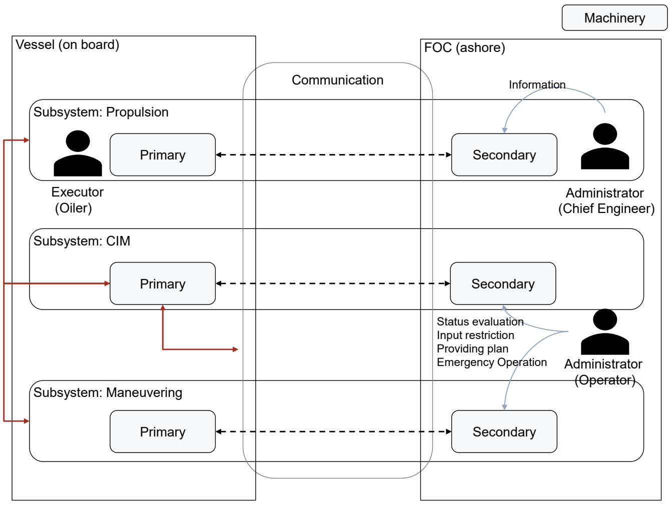


Figure 4. System structure at the subsystem level.

Actors and stakeholders include shipping companies and operators, port authorities, administrations and classification societies, shipyards, marine manufacturers, insurance companies, etc. We worked closely with these stakeholders to exchange opinions and obtain feedback on the design based on their needs.

As for use cases, berth to berth operation is assumed in the nominal case, while remote operation from the Fleet Operation Centre is assumed in the off-nominal case. In addition, the system automatically stops safely in an emergency to ensure Minimal Risk Condition.

As an Operational Scenario, since there are various navigational patterns for berth-to-berth operations, the modes of the operation have been defined. The actual voyage can be divided into seven modes: unberthing, leaving, harbour out, coastal, harbour in, approaching and berthing.

The degree to which humans should contribute varies depending on the internal and external environment. Here, the following four levels of system statuses are defined based on existing literature. The definition of each status is shown in Table 5. In the basic and detailed design stages, the criteria for each mode are refined.

Table 5. Definition of Status.

Status	Description
Normal (N)	Running without any involvement by the operator
Active Monitoring (AM)	Running under monitoring and verification by the operator
Remote Fallback (RFB)	Running under fallback operations by the operator at FOC
Independent Fallback (IFB)	Running under fallback operations by the machinery on the vessel to keep the system at Minimal Risk Condition

The mode change is implemented in the form of embedding it in the waypoint according to the operational status. As a result, the mode changes automatically according to the position information of the own ship. On the other hand, the status is determined by the CIM subsystem. The status decision criteria are divided into two categories: those defined by the system's internal state (internal health level) and those defined by the external influence

(External Operational Design Domain: EODD). The internal health level is defined by the state of the subsystem responsible for the operation task, divided into the Manoeuvring, Propulsion, and Communication subsystem. The state of each subsystem is defined as shown in Tables 6, 7 and 8. The whole system status is defined in Table 9, assuming the system is in EODD.

The EODD represents the range of external conditions that can be expected when a ship is in operation. The appropriate range of rudder angle and speed should be determined based on the magnitude and direction of the external forces, in accordance with the ship's manoeuvrability. Although the ship should be designed to operate automatically without deviating from these conditions, if the ship deviates from these conditions and gets out of EODD, it is designed to immediately switch to Independent Fallback (IFB) Operation.

The basic idea of the status setting is shown in [20]. As the status can define responsibilities between humans and machines, it can be considered as the foundation for the operational envelope proposed in [21].
There are two types for status transition: one is Approval, in which the status is switched with the operator's approval, and the other is Acknowledgement, in which the operator is only notified of the switch. Approval is required for those that require human involvement in the future and those that no longer require active involvement, while Acknowledgement is used for those that require a quick transition to IFB.

The concept of Dynamic Positioning System (DPS) was referred to for the concrete realisation of each subsystem level [22]. The DPS should be designed redundantly, and its functions are defined at different levels according to the situation.

Table 6. Manoeuvring subsystem health level.

Level	Definition
Level1	Possible to design an action plan with sufficient reliability all by oneself
Level2	Possible to design an action plan under monitoring by the operators; The operators complement reliability and integrity
Level3	Possible to design an action plan within a limited scope; the operators complement subsystem function
Level4	Possible to design an action plan within a limited scope; machines on the vessel complement subsystem function
Level5	Unable to design an action plan; Unable to take supplementary operation by either human or machines on the vessel

Table 7. Propulsion subsystem health level.

Level	Definition
Level1	Possible to deliver the power of propulsion and control
Level2	Possible to deliver the power of propulsion and control, but with alert (caution or warning) or on monitoring by the operators
Level3	Possible to deliver the power of propulsion and control within a limited scope, e.g., alert to trigger auto-slow-down is activated
Level4	Possible to deliver the power of propulsion and control within an extremely limited scope, e.g., the subsystem can continue only anchoring
Level5	Unable to deliver the power of propulsion and control

Table 8. Communication subsystem health level.

Level	Definition
Level1	Possible to monitor and control the system
Level2	Possible to monitor and change the status of the system within a limited scope; RFB operations unavailable
Level3	Disconnection or impossible to monitor

Table 9. Whole system status definition.

C: 1	P: 1	P: 2	P: 3	P: 4	P: 5
M: 1	N	N	RFB	IFB	NUC
M: 2	AM	AM	RFB	IFB	NUC
M: 3	RFB	RFB	RFB	IFB	NUC
M: 4	IFB	IFB	IFB	IFB	NUC
M: 5	NUC	NUC	NUC	NUC	NUC
C: 2	P: 1	P: 2	P: 3	P: 4	P: 5
M: 1	N*	IFB	IFB	IFB	NUC
M: 2	AM*	IFB	IFB	IFB	NUC
M: 3	IFB	IFB	IFB	IFB	NUC
M: 4	IFB	IFB	IFB	IFB	NUC
M: 5	NUC	NUC	NUC	NUC	NUC
C: 3	P: 1	P: 2	P: 3	P: 4	P: 5
M: 1	N*	IFB	IFB	IFB	NUC
M: 2	IFB	IFB	IFB	IFB	NUC
M: 3	IFB	IFB	IFB	IFB	NUC
M: 4	IFB	IFB	IFB	IFB	NUC
M: 5	NUC	NUC	NUC	NUC	NUC

M: Maneuvering subsystem health level, P: Propulsion subsystem health level, C: Communication subsystem health level, N: Normal Operation, AM: Active Monitoring Operation, RFB: Remote Fallback Operation, IFB: Independent Fallback Operation, NUC: Not Under Command, *: With a time limit

(5) Impacts and potential issues The impacts of this system on various fields are summarised in Table 10 in terms of operation, environment, organisation, technology, legal system, and social implementation. As a result, the important elements for future risk assessment and requirement elicitation are summarised.

(6) Human-Systems Integration The division of roles between humans and machines is practically included in *(3)* and *(4)*. It can be organised again at the subsystem level, as shown in Figure 5.

4.2. Initial safety analysis using STPA

Based on the ConOps, safety analysis using STAMP/STPA has been conducted. The STPA consists of four major steps: two preparation phases (Step 0-1, 0-2), Step 1 and Step 2.

Table 10. Impacts and potential issues.

Category	Description
Operation	The envisioned system reduces the load on the crew and ensures safe and efficient operation (with the effect of reducing accidents caused by human); maintenance requires flexible software updates from remote locations.
Environment	Efficient operation by the envisioned system can reduce impacts.
Organisation	The number of seafarers could be reduced. It is also necessary to have a shore support centre.
Technology	Design and construction require the system integration capabilities to bring together many technologies and achieve efficiency and safety and the ability to manage many stakeholders.
Legal	Although the introduction of the envisioned system does not violate current legal system, it is necessary to lobby the IMO and the national government to change rules such as the lookout to make efficient use of this system.
Implementation	At present, there are hurdles in implementing the envisioned system because of the initial cost.

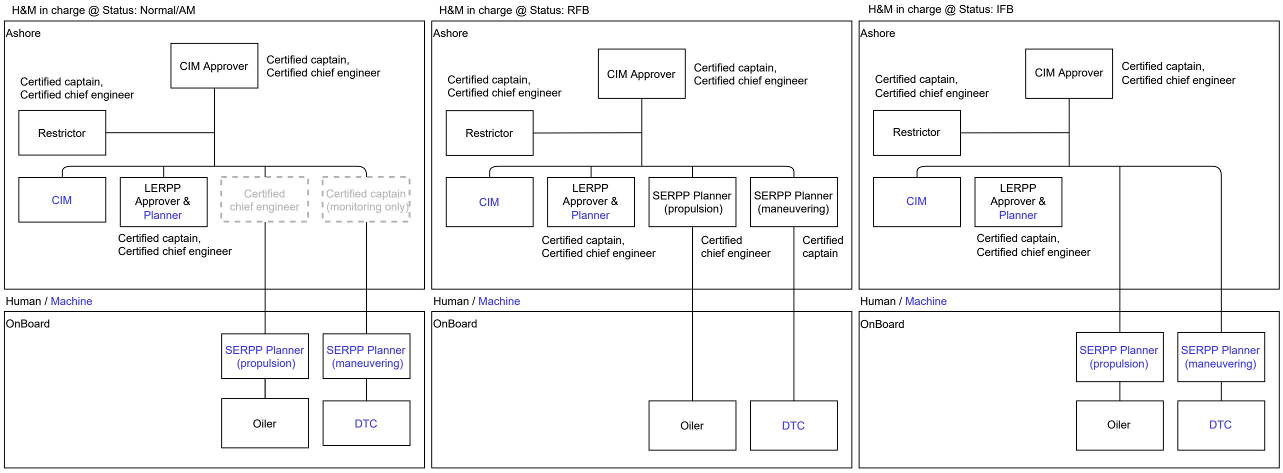


Figure 5. Human Machine Roles in each status. (Left: Normal and Active Monitoring, Centre: RFB, Right: IFB)

In Step 0-1, the accidents and hazards of the system and the Safety Constraints (SCs) that the system should guarantee are defined. Collisions and groundings were set to be our focus, which account for more than half of all accidents. Note that fire and other incidents are excluded from the scope of this analysis. In general, Safety Constraints seem to be defined as close to the final consequences as possible. However, in considering a complex system such as this one, it seems difficult to extract the Unsafe Control Actions (UCAs) exhaustively with abstract Safety Constraints, as some control actions can be too far from the consequences. Therefore, a chain of events that could lead to ”close to obstacles' and 'loss of seaworthiness' in operation has been assumed and these intermediate events were defined as Safety Constraints, which are shown in Table 11 and Figure 6.

In Step 0-2, the control structure should be developed, which has already been created in the ConOps phase (Figure 4).

In Step 1, the UCAs are extracted by checking the Control Actions among the subsystems described in the control structure one by one. The following four words are used as guide words referring to [23]: *1. A control action required for safety is not provided or is not followed, 2. An unsafe control action is provided that leads to a hazard, 3. A potentially safe control action is provided too late, too early, or out of sequence, 4. A safe control action is stopped too soon or applied too long (for a continuous or non-discrete control action).* Based on this, the Unsafe Control Actions were extracted. A couple of them are shown in Table 12. The square brackets indicate the Safety Constraints that conflict.

In Step 2, the Hazard Contribution Factors (HCFs) were extracted for each UCA. The guiding words for the HCFs were those used in [23]: *failures related to the controller, inadequate control algorithm, unsafe control input, and inadequate process model.* The obtained UCAs and HCFs were organised in BowTie to increase their visibility, as shown in Figure 7. The countermeasures against the HCFs are shown as the barriers, which function as the requirements for the subsystems.

Table 11. Safety Constraints (SCs).

SC	Description
SC1	Own vessel states must be detected: system conditions and sensor-detected values etc.
SC2	Other vessels and those states must be detected: existence and course, heading, speed and positions.
SC3	Natural environments which affect the system must be detected: wind, wave, tidal stream, temperature, etc.
SC4	Static constraints which are essential to achieve voyage must be obtained.
SC5	Navigation and/or action plan must be established.
SC6	Control signal must be calculated based on navigation/action plan.
SC7	Geographic information to navigate must be detected.
SC8	Seaworthiness including condition of equipment and hull must be analysed and actions must be selected based on own status and surrounding environment.
SC9	Dynamic constraints must be analysed based on static constraints and internal/external environment (e.g., short stopping distance, Turning circle).

Table 12. Examples of Unsafe Control Actions (For interaction between subsystem).

Control Action	Not Providing	Providing	Too early / Too late
Sending constraints from CIM to Maneuvering (LERPP)	The subsystem is unable to work. [SC5]	The subsystem works improperly. [SC5]	N/A (Small delay of providing constraints does not trigger hazardous situation.)
Sending constraints from Maneuvering (SERPP) to CIM	CIM is unable to decide system status. [SC8]	CIM decide improper system status. [SC8]	CIM is unable to decide system status at suitable timing. [SC8]

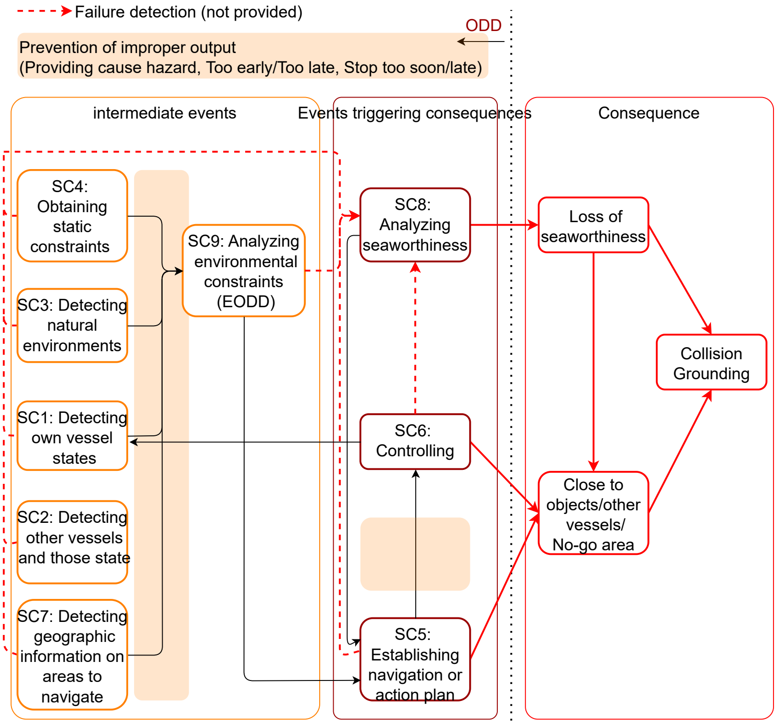

Failure detection (not provided)
ODD
Prevention of improper output
(Providing cause hazard, Too early/Too late, Stop too soon/late)
intermediate events
Events triggering consequences
Consequence
SC4: Obtaining static constraints
SC3: Detecting natural environments
SC1: Detecting own vessel states
SC2: Detecting other vessels and those state
SC7: Detecting geographic information on areas to navigate
SC9: Analyzing environmental constraints (EODD)
SC8: Analyzing seaworthiness
SC6: Controlling
SC5: Establishing navigation or action plan
Loss of seaworthiness
Collision Grounding
Close to objects/other vessels/ No-go area

Figure 6. Flow Diagram of Safety Constraints.

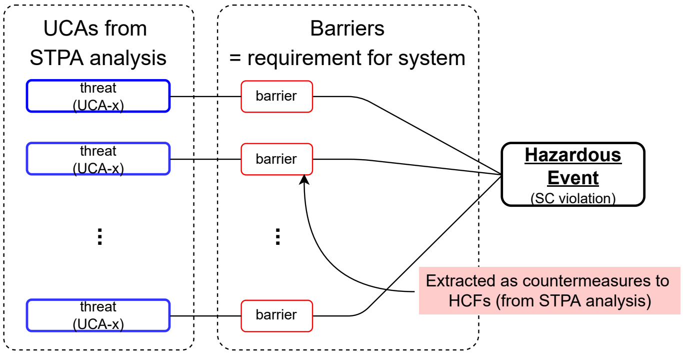


Figure 7. Schematic image of BowTie analysis.

4.3. Requirement Definition, Decomposition and Architecting

Based on ConOps and STPA, and referring to the framework of SysML, the model diagrams of the system have been organised, clarifying the relationships among them. Requirements for the system have been set based on the Hazard Causal Factors (HCFs) described above.

The Block Diagram and N2 Diagram of the CIM subsystem are shown to specify the functions and the system configuration in Figure 8 and 9. The Block Diagram shows the process flow, and the N2 Diagram shows the flow of information generated in each process.

As a result, the system configuration, including the modules and components in each subsystem, has been detailed. The modules in each subsystem correspond to some of the functions in the above diagram.

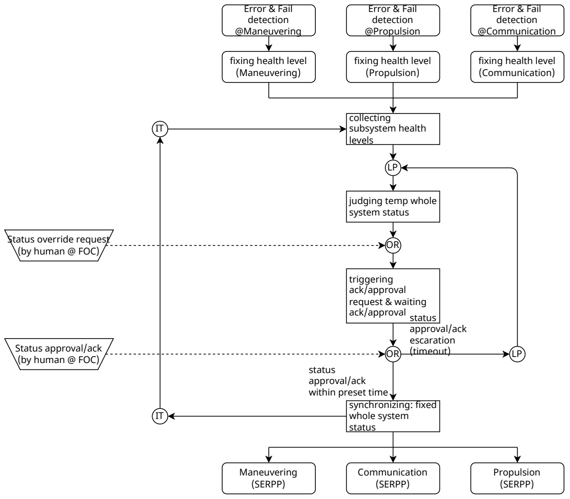
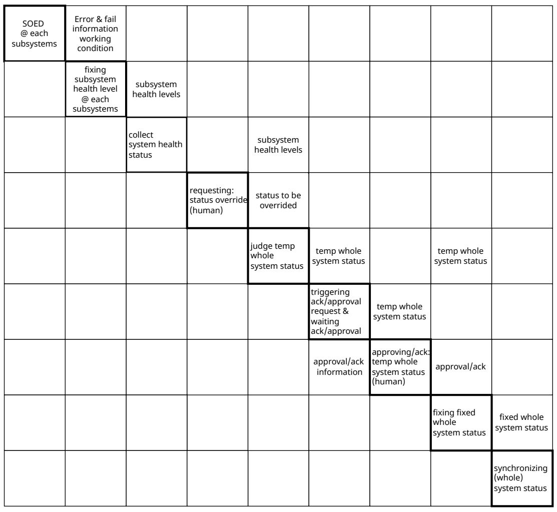

Error & Fail detection @Maneuvering
Error & Fail detection @Propulsion
Error & Fail detection @Communication
fixing health level (Maneuvering)
fixing health level (Propulsion)
fixing health level (Communication)
IT
collecting subsystem health levels
LP
judging temp whole system status
Status override request (by human @ FOC)
OR
triggering ack/approval request & waiting ack/approval
status approval/ack escaration (timeout)
Status approval/ack (by human @ FOC)
OR
LP
status approval/ack within preset time
IT
synchronizing: fixed whole system status
Maneuvering (SERPP)
Communication (SERPP)
Propulsion (SERPP)

Figure 8. Block Diagram of CIM subsystem.



SOED @ each subsystems	Error & fail information working condition							
	fixing subsystem health level @ each subsystems	subsystem health levels						
		collect system health status		subsystem health levels				
			requesting: status override (human)	status to be overrided				
				judge temp whole system status	temp whole system status		temp whole system status	
					triggering ack/approval request & waiting ack/approval	temp whole system status		
					approval/ack information	approving/ack: temp whole system status (human)	approval/ack	
							fixing fixed whole system status	fixed whole system status
								synchronizing (whole) system status

Figure 9. N2 Diagram of CIM subsystem.

4.4. Detailed Safety analysis using STPA

In this phase, the same analysis as in *4.2* is performed on the system that has been concretised to the module level within the subsystem, and more detailed safety requirements are extracted. Part of UCAs in the subsystem are shown in Table 13.

The extracted requirements have been classified into those reflected in the system design, the operational procedures, and the training requirements. The classified requirements have been referred to in the verification phase, i.e., integration test, demonstration test, etc.

Table 13. Examples of Unsafe Control Actions (For interaction inside subsystem).

Control Action	Not Providing	Providing	Too early / Too late
Sending Temporary whole system status	CIM is unable to make output fixed status. [SC8]	CIM chooses an improperly fixed status. [SC8]	CIM is unable to choose fixed status at suitable timing. [SC8]
Sending Long term Re-route request	LERPP cannot establish a navigation plan. [SC5]	LERPP cannot establish a proper navigation plan. [SC5]	N/A (Even if the re-route request is given delay, LERPP has some delay, but not critical.)

4.5. Summary

The overall flow up to this point is shown in Figure 10. In defining the requirements for the safe autonomous system, STPA has been conducted to concrete and design the behaviour and structure step by step. To conduct the safety analysis, it is not possible to extract appropriate requirements unless the system's behaviours and structures are defined to some extent. By introducing the MBSE and STPA concepts to the development of an autonomous vessel, an actual example of the appropriate granularity and methodology has been presented.

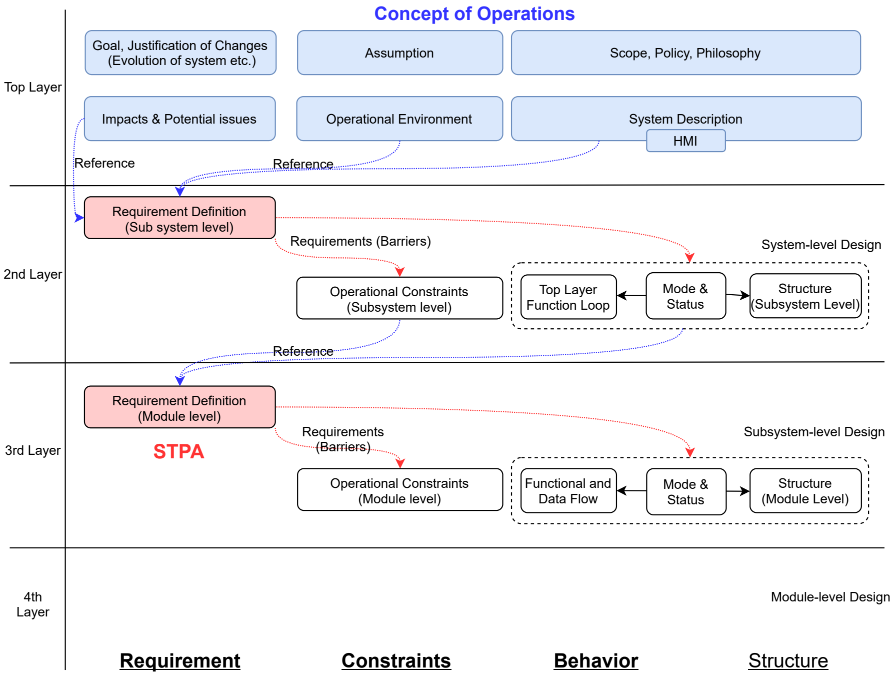


Figure 10. Model-based design for a crewless vessel with STPA.

5. Conclusions

In this paper, a methodology for model-based design of autonomous navigation systems has been described using real system development as an example. The appropriate ConOps elements for the autonomous navigation system have been studied and a set of functions and subsystems is designed in relation to the system's objectives, assumptions etc. This paper also proposes a new system concept for managing the system status.

A step-by-step safety analysis method has been conducted using STPA to implement them at an appropriate granularity according to the actual system development phase to extract appropriate safety requirements. Appropriate Safety Constraints for the autonomous navigation system are also proposed, which will be an effective method of STPA for such a complex system.

One of the future challenges is model-based validation and verification. Safety argumentation methods for autonomous vessels and simulation systems with appropriate scenarios should be considered.

Acknowledgments

This research was supported by The Nippon Foundation's "demonstration tests of The Nippon Foundation MEGURI2040 Fully Autonomous Ship Program". We would also like to express our sincere gratitude to Prof. Yan Jin and his colleagues at Impact Lab, Nippon Kaiji Kyokai (ClassNK), and the National Maritime Research Institute for helpful discussions.

References

[1] IMO, Guidelines for the Approval of Alternatives and Equivalents as provided for in Various IMO Instruments, MSC.1/Circ.1455, 24 June 2013.
[2] L. Andreas and L. Wennersberg, AUTOSHIP D3.2 Autonomous-ship-design-methods-and-test-principles v1.1, 2021.
[3] International Council on Systems Engineering, Systems Engineering Vision 2020, INCOSE-TP-2004-004-02, 2007.

[4] N.G. Leveson, Engineering a Safer World: Systems Thinking Applied to Safety. MIT Press, Cambridge, MA., 2011.

[5] ISO 26262:2018 Road vehicles – Functional safety

[6] ISO/DIS 21448: 2021, Road vehicles – Safety of the intended functionality

[7] C. A. Thieme, C. Guo, I. B. Utne, and S. Haugen, Preliminary hazard analysis of a small harbor passenger ferry-results, challenges and further work, J. Phys. Conf. Ser., vol. 1357, no. 1, 2019.

[8] K. Wróbel, J. Montewka, and P. Kujala, Towards the development of a system-theoretic model for safety assessment of autonomous merchant vessels, Reliab. Eng. Syst. Saf., vol. 178, no. June, pp. 209–224, 2018.

[9] M. Chaal, O. A. Valdez Banda, J. A. Glomsrud, S. Basnet, S. Hirdaris, and P. Kujala, A framework to model the STPA hierarchical control structure of an autonomous ship. Safety Science, 132, 2020.

[10] B. Rokseth, O. I. Haugen, I. B. Utne, Safety Verification for Autonomous Ships., MATEC Web of Conferences, 273, 2019.

[11] O. A. Valdez Banda, S. Kannos, F. Goerlandt, P. H. A. J. M. van Gelder, M. Bergström, and P. Kujala, A systemic hazard analysis and management process for the concept design phase of an autonomous vessel. Reliability Engineering and System Safety, 191, 2019.

[12] NASA, NASA System Engineering Handbook Revision 2, Natl. Aeronaut. Sp. Adm., p. 297, 2016.

[13] American Bureau of Shipping, Guide for Autonomous and Remote Control Functions, 2021.

[14] ClassNK, Guidelines for Automated/Autonomous Operation of ships Design development, Installation and Operation of Automated Operation Systems/Remote Operation Systems , 2020.

[15] Bureau Veritas, Guidelines for Autonomous Shipping, 2019.

[16] DNVGL, Class Guideline DNVGL-CG-0264 Autonomous and remotely operated ships, 2018.

[17] S. Yamaguchi, Evaluation of the Application of the Safety Analysis Method Based on System Theory "STAMP/STPA" to Requirement Development Phase, Keio University, 2019, PhD thesis. (Japanese)

[18] ISO/IEC/IEEE 29148:2011 Systems and software engineering – Life cycle processes – Requirements engineering

[19] The Federal Aviation Administration, Concept of Operations for Urban Air Mobility (UAM) (ConOps 1.0), 2020.

[20] K. Kutsuna, H. Ando, T. Nakashima, S. Kuwahara, and S. Nakamura, NYK's Approach for Autonomous Navigation-Structure of Action Planning System and Demonstration Experiments, J. Phys. Conf. Ser., vol. 1357, no. 1, 2019.

[21] Ø. J. Rødseth, L. A. Lien Wennersberg, and H. Nordahl, Towards approval of autonomous ship systems by their operational envelope, J. Mar. Sci. Technol., no. 0123456789, 2021.

[22] American Bureau of Shipping, Guide for Dynamic Positioning Systems, 2021.

[23] N.G. Leveson and J.P. Thomas, STPA Handbook, 2018.