Chaal, Meriam; Valdez Banda, Osiris; Basnet, Sunil; Glomsrud, Jon Arne; Basnet, Sunil; Hirdaris, Spyros; Kujala, Pentti

A framework to model the STPA hierarchical control structure of an autonomous ship

Published in:
Safety Science

DOI:
10.1016/j.ssci.2020.104939

Published: 01/12/2020

Document Version
Publisher's PDF, also known as Version of record

Safety Science 132 (2020) 104939

Contents lists available at ScienceDirect

Safety Science

journal homepage: www.elsevier.com/locate/safety

A framework to model the STPA hierarchical control structure of an autonomous ship

Meriam Chaal[a,*], Osiris A. Valdez Banda[a], Jon Arne Glomsrud[b], Sunil Basnet[a], Spyros Hirdaris[a], Pentti Kujala[a]

[a] Aalto University, Department of Mechanical Engineering (Marine Technology), Research Group on Safe and Efficient Marine Systems and Experience, Finland
[b] Group Technology and Research, DNV GL, Norway

ARTICLE INFO

Keywords:
Autonomous ship
Autonomous Navigation System
Maritime safety
System safety engineering
STAMP
STPA

ABSTRACT

The demand for risk and safety analysis is becoming greater due to the increased complexity of modern systems such as autonomous ships. Safety is one of the main motivations behind the efforts of multiple organizations to develop autonomous ships. The adoption of an early system-theoretic approach to safety such as System Theoretic Process Analysis (STPA) is an effective way to integrate safety in complex systems. Furthermore, many authors have urged the use of this method to analyse the risks of autonomous vessels in the development phases. Applying STPA requires a description of the system to model the hierarchical control structure and conduct the analysis. At this stage, the functional description of autonomous ships remains limited, which poses a challenge in building the hierarchical control structure. This paper proposes a framework for developing a hierarchical control structure of an autonomous ship. The framework is founded on the principles of the STPA control structure and its five main elements. It makes use of the current shipping operation system, the available information about autonomous ships and the experience of seafarers executing diverse tasks on-board conventional ships. The application of the framework showed that the information provided by the seafarers is essential in developing an initial functional description of an autonomous ship. Furthermore, the results revealed that in addition to the technical aspects of autonomous ships, introducing these vessels into the organizational control structure of current maritime operation also poses challenges that need to be addressed in the earliest design phase.

1. Introduction

In recent years, many research and industry organizations have started developing and designing autonomous ships (Autoferry, 2016; Kongsberg, 2018; MUNIN, 2016; Rolls Royce, 2018; Smart Ships Coalition, 2017). These new ships will apply state-of-the-art technologies to the marine environment (Brekke et al., 2019; Heffner and Rødseth, 2019; Kufoalor et al., 2019; Levander, 2017; Wilthil et al., 2017). Autonomous ships are expected to reduce maritime accidents caused by human errors and reduce the exposure of seafarers to maritime risks, which makes safety one of the main drivers for autonomy (AAWA, 2016; Blanke et al., 2018; Ramos et al., 2020, 2019; Utne, 2017; Wróbel et al., 2017). In addition, the International Maritime Organization (IMO) requires that autonomous ships must be "at least as safe as conventional ships" (IMO, 2019).

Design flaws in automation and emerging technologies may lead to even worse unforeseen accident scenarios (Ishimatsu et al., 2014; Thomas et al., 2015). The complexity of systems may pose various challenges in terms of assurance (Abdulkhaleq et al., 2015; Leveson, 2004). As complexity increases, it may be necessary to adopt an early systemic approach to safety in order to develop and operate safe and sustainable systems (Rasmussen, 1997; Renn, 2017). This is because a proactive systems approach accounts for the interactions of the system with its environment and its subsystems (Leveson, 2011; Linkov et al., 2018, 2014; Rasmussen, 1997). Emerging technologies should be designed to be safe in their operational environments throughout their life cycles (Renn and Klinke, 2004; van de Poel and Robaey, 2017).

One of the most proactive systemic hazard analysis methods that can facilitate designing for safety is System Theoretic Process Analysis (STPA) (Sulaman et al., 2019; Thieme et al., 2018). Various authors have already recommended STPA for the early stages of autonomous ship design (e.g. Basnet et al., 2019; Montewka et al., 2018; Thieme et al., 2019, 2018; Valdez Banda et al., 2019, 2018) because it is a systemic and iterative hazard analysis technique appropriate for both

* Corresponding author.
E-mail address: meriam.chaal@aalto.fi (M. Chaal).

https://doi.org/10.1016/j.ssci.2020.104939
Received 31 January 2020; Received in revised form 25 May 2020; Accepted 26 July 2020

development and design (Leveson, 2011). To date, only a few studies have applied STPA to autonomous ships (Thieme et al., 2018). This is probably due to the lack of information about the control structures of autonomous systems under development (Ventikos and Louzis, 2019). Most of these studies were based on the scarce information available concerning autonomous ships to develop the STPA control structure, which limited the results of the application of STPA to a high level of abstraction (Omitola et al., 2018; Rokseth et al., 2019; Valdez Banda and Kannos, 2017; Wróbel et al., 2019). In some cases the control structure contributed greatly to the uncertainty of the study (e.g. Wróbel et al., 2018).

Leveson (2011) suggested that the iterative nature of the STPA method can help in developing the safety control structure. However, the STPA handbook provides rather limited guidance on developing the control structure of the system in the conceptual design phase (Glomsrud and Xie, 2019). In the conceptual design phase, the starting point for the STPA hazard analysis differs from system to system depending on the level of prior knowledge about the system in question (Leveson and Thomas, 2018). With limited knowledge, developing the control structure in this phase becomes more challenging (Glomsrud and Xie, 2019). In order to tackle this issue, Fleming (2015) proposes System Theoretic Early Concept Analysis (STECA). This method aims at supporting the application of STPA by guiding the design of the safety control structure of a system at the earliest concept design stage.

In order to compensate for the lack of knowledge about autonomous ships and their functional description for use in early hazard analysis, this paper introduces a new approach to develop the hierarchical control structure of an autonomous ship. Considering that autonomous ships will navigate in waters like traditional ships (Wróbel and Montewka, 2019), the aim of this paper is to make use of the abundant knowledge gained in traditional ship operation for the safety analysis of autonomous ships. It proposes a systematic framework for applying Step 2 of the STPA method in light of the transition of the maritime industry towards autonomy. Rather than considering autonomous ships as totally new systems, the proposed framework assumes that automated controllers will replace human controllers on autonomous ships. The framework consists of three parts. Part 1 was conducted in a separate work and its results are briefly described in this study to provide clarifying information. Part 2 consists of modelling the organizational control structure of the current shipping operation system that will accommodate autonomous merchant ships. In Part 3, the framework draws on seafarers' experience within the context of a functional analogy between a human controller and an automated controller in order to refine the hierarchical control structure of an autonomous ship. This study also aims to support the implementation of STPA to autonomous shipping and contribute to the safety-integrated development of autonomous ship systems.

2. The framework foundations

2.1. System Theoretic accident model and processes (STAMP)

STAMP is an accident causality model based on systems theory. It was created as a response to the limitations of traditional causality models in the analysis of modern complex systems (Leveson, 2011). STAMP covers accidents linked to both component failures and the interactions of system components (Fleming et al., 2013; Leveson, 2015). In the past, accidents were commonly attributed to component failures or human errors. At that time, traditional systems were mostly electro-mechanical and relatively simple compared to today's software-intensive socio-technical systems. However, safety is a system property that does not rely solely on a set of separate software, hardware and human components that execute their respective missions successfully (Hollnagel, 2014; Leveson, 2004; Rasmussen, 1997). As a system property, the STAMP model treats safety at the system level (Leveson et al., 2012). STAMP is built on diverse essential principles (Leveson, 2011):

- Accidents happen when system behaviour violates the safety constraints
- Safety is a control problem – system safety relies on adequate control that enforces the safety constraints
- Systems are considered as hierarchical control structures, where each controller enforces the safety constraints on the controlled processes beneath it
- The hierarchical control structure is composed of control loops
- Any controller needs an updated model of the process it controls
- Process models are updated with different forms of feedback
- Most component interaction accidents can be traced back to errors in the process model
- The control hierarchy is based on adaptive feedback, which is essential for accident prevention

2.2. STPA

System Theoretic Process Analysis (STPA) is a hazard analysis method based on STAMP. It examines unsafe interactions among system components and gives recommendations to prevent the occurrence of hazards that could be caused by unsafe control actions. For a new design, for which no system description has been defined and a safety control structure is not available, multiple iterations of the STPA analysis are recommended (Leveson and Thomas, 2018). There are four steps in the STPA hazard analysis (Leveson and Thomas, 2018):

i. Defining the purpose of the analysis. This step includes identifying the losses, the system-level hazards and the system-level safety constraints.
ii. Modelling the hierarchical control structure. A control structure is a functional model of the system composed of control loops and developed from the available system description. Fig. 1 shows a generic control loop.
iii. Identifying the Unsafe Control Actions (UCAs). These are "the control actions that in a particular context and worst-case environment will lead to a hazard".
iv. Identifying the loss scenarios. In this step the causal factors of each unsafe control action are determined and recommendations to prevent these causes are formulated. These recommendations guide the improvements of the control structure or the other changes and mitigation measures.

2.3. System theoretic early concept analysis (STECA)

STECA is a method based on STAMP, which analyses the system concepts to identify hazards and provides a safety-driven approach for developing the concept (Fleming, 2015). It utilizes the Concept of

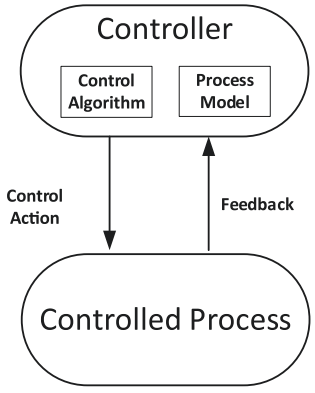


Fig. 1. Generic control loop.

Operations (ConOps) document to create a hierarchical safety control structure of the system concept. This control structure is then analysed to identify the hazardous scenarios. Unlike STPA, STECA focuses on verifying the control structure for completeness, safety-related responsibilities, coordination and consistency (Fleming and Leveson, 2015). STECA consists of six major iterative steps (Fleming, 2015):

i. Identify system hazards
ii. Derive system safety constraints
iii. Identify control concepts
iv. Identify hazardous scenarios and causal factors
v. Derive refined safety constraints
vi. Refine, modify control structure

3. STPA applications in autonomous shipping

In autonomous shipping, the application of STPA started recently with attempts to foresee the hazards associated with the operation of autonomous ships and guide their design. Some of these studies omit the development of the hierarchical control structure (Step 2 in STPA), which is challenging when limited information is available about the system in question. These studies focus on the application of Steps 3 and 4 to identify critical safety information to guide the design of autonomous ship concepts (Omitola et al., 2018; Valdez Banda and Kannos, 2017). Valdez Banda and Kannos (2017) proposed a process to identify and mitigate the hazards associated with the operation of two autonomous ferries for urban transport, while Omitola et al. (2018) focused on the hazards of cyberattacks during navigation applied to an autonomous ship concept.

Wróbel et al. (2018) conducted a preliminary STPA hazard analysis of autonomous merchant vessels with the support of a defined safety control structure. The author mentioned that the control structure was a major limitation of the study due to the lack of data and information about autonomous vessels. The control structure depicted a simplified model of the autonomous vessel operation system and it made a major contribution to the analysis of uncertainties (Wróbel et al., 2018). A more recent article by Wróbel et al. (2019) presented the preliminary results of the STPA hazard analysis on a model of a fully autonomous ship that uses the same control structure introduced in Wróbel et al. (2018).

Solberg (2018) applied STPA to a prototype of an autonomous ship called ReVolt. The author developed an advanced control structure specific to the ship prototype and suggested improvements to the ReVolt model based on the results of the hazard analysis. Zou (2018) applied STPA to the operation of a fully autonomous ship concept with a control diagram including three simplified ship functions. The aim of the study was to compare STPA to other hazard analysis methods. The results of the comparison suggested a means of improving the identification of the unsafe control actions in STPA to identify the hazard causes. The author applied STPA to the ReVolt safety control structure in order to develop a more detailed control model.

Rokseth et al. (2019) presented an approach to obtaining autonomous ship system requirements and verification based on STPA. The authors suggested a hierarchical control structure in order to apply the methodology presented in their study. The control structure includes four simplified systems: the automatic sailing system, the autopilot, the motion control system and the power system. Their study provided a set of generic functional requirements for autonomous ships.

Utne et al. (2020) applied STPA to an autonomous ship concept in a case study. The safety control structure in the case study was at a high level of abstraction under three levels of control namely monitoring, guidance and execution. The aim of their study was to present a viable approach for the online risk control of autonomous systems that uses the STPA results in a Bayesian Belief Network model. The focus in its application was the guidance layer, which is responsible for decision making based on online risk factors.

Glomsrud and Xie (2019) applied STPA to safety and security co-analysis of unmanned surface vessels. The authors claimed that STPA provides limited guidance to model the control structure of the system when prior knowledge is scarce. They presented an approach to connect Step 1 and Step 2 of STPA to support developing the control structure of the system. It starts by defining the functional requirements from the identified system-level hazards in the first step of STPA. The functional requirements are then used to draw the control structure of the system at a high level of abstraction.

The limitations of the results presented in most of the above-mentioned studies were related to the lack of information about the autonomous ship and its functional description. This information is necessary to develop the control structure in the second step of STPA and conduct an advanced hazard analysis that leads to safe design solutions. All these studies develop the safety control structure based on scarce knowledge about autonomous ships. In addition, only the hierarchical control structure by (Wróbel et al., 2018) considered the organizational level of autonomous shipping operation. The organizational level is also important for the safe development of autonomous ships, as it is believed to be the cause of many systemic hazards (Hollnagel, 2014; Leveson, 2004; Rasmussen, 1997). Furthermore, the organizational aspect of autonomous and remotely operated ships is a research gap that was identified in a recent literature review by (Wróbel et al., 2020). In the same review, (Wróbel et al. (2020) also concluded that few studies have focused on the impact of this new kind of ships on safety of maritime operation.

4. The framework methodology

In order to build the hierarchical control structure of an autonomous ship during the transition of the maritime industry towards autonomy, this new framework proposes a set of steps. The basis of the proposed framework is rooted in STPA, which emphasizes the importance of the functional description of the system and its hierarchical control to improve system safety. On an autonomous ship, software controllers replace crew members. In this framework, the steps to be followed are intended to show how human controllers can be replaced by software controllers that will perform the same functions as humans do in traditional ship operation. In STPA, there are two types of hierarchical control structures, one for the development of the system and one for the operation of the system. This framework is meant to build the hierarchical control structure of the operation of autonomous ships, which aims at influencing their design. The framework uses the current knowledge about the maritime operation system in addition to the autonomous ship functions and the knowledge of experienced seafarers in performing their functions on-board conventional ships.

The framework consists of three parts, which are introduced in the following sections.

4.1. Autonomous ship control structure (Part 1)

This part reviews the available knowledge about autonomous ships in combination with the seafarers functions in the International Convention on Standards of Training, Certification and Watch-keeping (STCW). This work was presented in a previous study by (Chaal et al., 2020) and other parts of the framework will draw on its results. Part 1 shows the control structure of an autonomous ship at a high level of abstraction, including the functions to be performed by the autonomous ship systems that will replace human controllers. However, the structure does not include the links between the different functions. These details are not yet available because the system designers are focusing on the technology capabilities of each autonomous ship system separately. The literature devotes greater efforts to collision avoidance algorithms and machine learning algorithms for object detection and identification separately. Information about system integration is still not available.

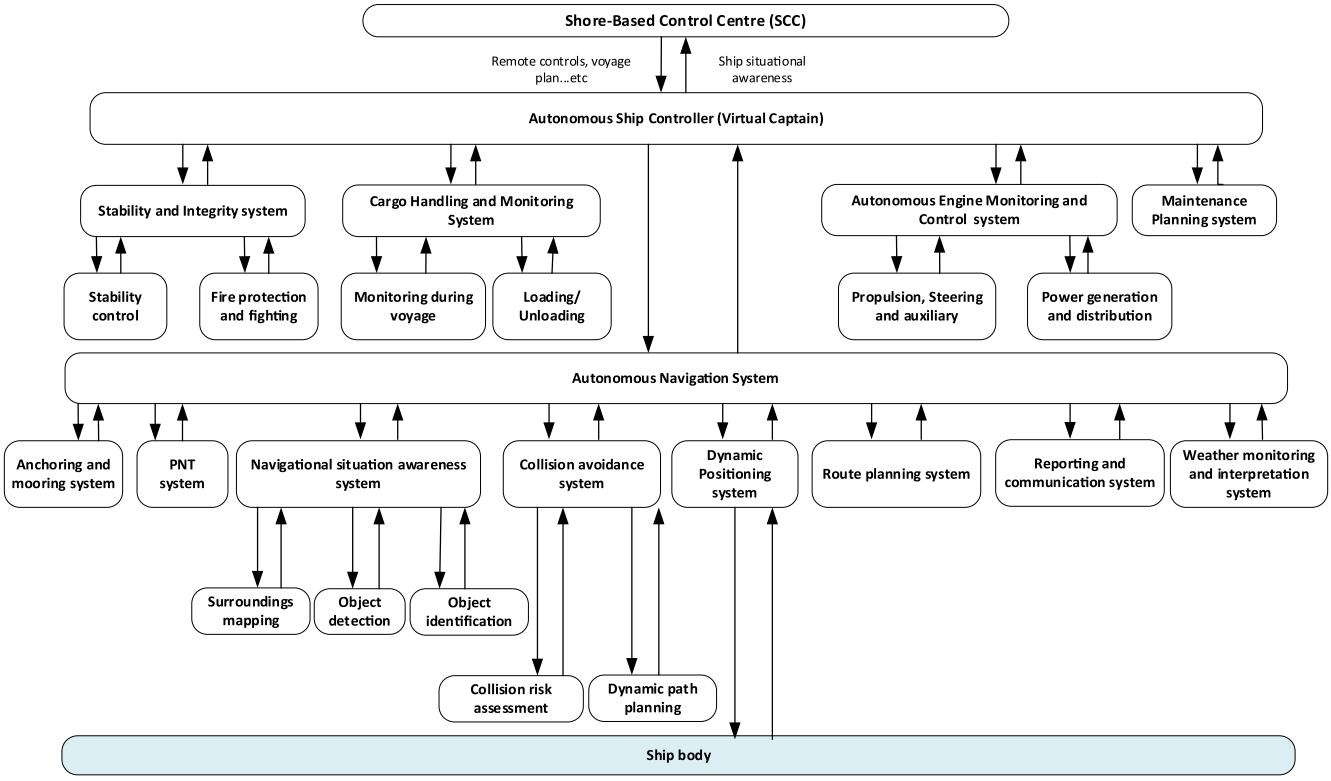


Fig. 2. The hierarchical control structure of an autonomous ship adopted from Chaal et al. (2020).

Fig. 2 shows the hierarchical control structure of an autonomous ship adopted from (Chaal et al., 2020). Each function is performed by a system of the autonomous ship. At the top level of the hierarchy is the Shore-based Control Centre (SCC), which supervises autonomous operation and can take control depending on the autonomy level. The autonomous ship controller is the virtual captain that monitors all the other ship functions most of the time.

In Fig. 2, the possible interactions between the different controllers and controlled processes are represented by arrows. The arrows are only vertical, linking components under each other in the hierarchy.

4.2. Control structure of the current maritime operation system (Part 2)

This part develops a control structure for the current maritime operation system at a high level of abstraction. This system should include the autonomous ship as a controlled process. The control structure of the maritime operation system at a high level of the hierarchy and abstraction will be the same for the autonomous ships at least during the period when manned ships still operate. This structure includes the known organizations that are currently involved in the maritime transportation system, with the International Maritime Organization (IMO) at the top hierarchy level. The more detailed levels of abstraction can show the differences in operating autonomous ships compared to conventional ships and therefore identify the additional maritime subsystems required to ensure safety.

This part of the framework is conducted based on the IMO Instruments Implementation Code (III Code), which explains the duties of the IMO member states in the implementation of IMO regulations and standards (IMO, 2013). The code is an important regulatory instrument that summarizes the member states' responsibilities in ensuring safe and efficient ship design and operation. The control structure in this paper focuses on ship operation and thus only includes the ship operation responsibilities of the member states. In addition to the IMO, the International Association of Marine Aids to Navigation and Lighthouse Authorities (IALA) and the International Hydrographic Organization (IHO) are two intergovernmental organizations that contribute to the standardization of ship operation practices. The IALA is in charge of harmonizing and maintaining aids to navigation worldwide by issuing guidelines and recommendations to the member states (IALA, 2020). The IHO is responsible for chartering and surveying the sea waters and setting unified standards for nautical charts (IHO, 2020). These organizations have an important role and are therefore considered in the hierarchical control structure of the current shipping operation system.

Part 2 of the framework is intended to locate the autonomous ship in the hierarchical control structure of the maritime operation system. This can show interactions within the shipping operation system in order to account for them during further analysis. The autonomous ship is introduced in this system as a controlled process including the SCC, as it is considered to be involved in the ship operation (Fig. 2). The SCC is expected to perform administrative tasks and handle emergencies, complex scenarios and distress situations. In this part of the framework, the interactions of the SCC with the control structure of the maritime operation system are considered based on the tasks that a SCC is expected to perform for the autonomous ship. This provides an idea about the operational challenges of autonomous shipping once introduced into the organizational control structure of the maritime system and helps in solving these challenges to ensure safety.

4.3. Refining the autonomous ship functions (Part 3)

Part 3 identifies the controls, feedback and other interactions between the elements of the control structure. Part 3 is based on the analogy of a function that was performed by a human controller before being delegated to an automated controller. It draws on the knowledge of experienced seafarers in performing their functions on-board ships. In traditional ship operation, humans and automation systems work together to perform all the ship functions, with humans retaining a high level of control. In their daily work on-board ships, seafarers collect information from different equipment to update their mental model of

the ship and make decisions. These decisions are transformed into certain actions using another piece of equipment or an automated system. Humans are responsible for the integration of the ship components to make decisions and take the correct actions. When navigating the ship, seafarers take different actions depending on the encountered scenarios and vessel situation. Thus, experienced seafarers acquire practical knowledge of safe navigation decisions using ship system information and situational awareness. This knowledge is contained within the humans' own control model of the ship, which they have built during their work experience. This control model includes the human decision-making process, the necessary information from the ship systems and the set of actions to take for safe navigation.

The controllers of an autonomous ship will also process input information in order to take actions (outputs). An autonomous ship will make decisions based on the information from its different systems. The integration of the different ship systems is necessary for autonomous operation. This integration ensures the flow of information and actions among the ship systems. In an attempt to transfer this information from human to autonomous ship controllers, Part 3 of the framework seeks to reveal the information that humans use to update their process model and the control actions for each function.

With the autonomous ship control structure in hand, a discussion with the seafarers (and the application of a questionnaire) provides the missing details and interactions of the selected functions within the control structure. According to the STPA handbook, a control structure contains five main element types: the controllers, the controlled processes, the control actions, the feedback, and the other inputs and outputs from components. While the questionnaire follows these element types, it was formulated based on the STECA methodology to identify the control concepts.

Considering the analogy between a conventional ship and an autonomous ship in Part 3, it is assumed that each function has a software controller instead of a human controller. Therefore, the controller is not included in the questions because the operators are asked about a known function/controller. Table 1 shows the main questions for the analysis of Part 3 in the framework and the related element types. The questions start with the information needed to perform the selected function. The additional questions in Table 1 are formulated to specify the element type if the answer can be more than one option. For element type D, the answer includes other information that can influence the operator's decision and change the action he/she was planning to take. This information could also be necessary to perform the function, but was not given in the previous questions.

In order to simplify the representation and explanation of the framework, the five types of elements are replaced by letters as follows:

- Type A: Feedback
- Type B: Control actions
- Type C: Controlled processes
- Type D: Other inputs to and outputs from components
- Type F: Controllers

Fig. 3 summarizes the different steps of the proposed framework. It shows the main three parts in red text. Part 3 is further detailed to show the iterations that can refine each function of the autonomous ship systems. The execution of these steps results in the control structure of the autonomous ship at a detailed level of abstraction.

5. Case study

5.1. Case study description

The case study applies Part 3 of the framework to one of the ship functions, namely Autonomous Navigation. This function was selected because it is the most challenging ship function in the transition towards autonomy, as it relies heavily on human senses and decision-making. In addition, more extensive information is available about the Autonomous Navigation System (ANS) than any other function of the autonomous ship. This available information was reviewed by Chaal et al. (2020). The case examined in this paper is the same one described by Chaal et al. (2020). It involves an autonomous cargo ship supervised by the SCC operator that handles administrative tasks and intervenes in case of emergency and complicated tasks, which can be considered to represent AL4-Constrained Autonomy (Lloyds Register, 2017; Rodseth et al., 2018). The case study is also considered as AL4 in the autonomy scale defined by IMO (IMO, 2018).

For the purpose of simplification, this case study only analyses the open sea autonomous operation mode.

5.2. Data

In order to apply Part 3 of the framework, the questions are answered in a brainstorming session with experienced seafarers. The function selected for the case study is navigation and thus the participants are mainly ship bridge crew. A group of experienced deck officers and ship captains answered the systematic questions of Part 3. The obtained data served to finalize the control structure of the ANS. The expert group consisted of:

- Two ship captains who have been working on-board ships for eighteen and twenty years, respectively,
- One chief mate who has been working on-board for twelve years,
- One deck officer who has an experience of five years on-board,
- One engineer officer who had been working for five years on-board.

Appendix B presents a sample of the data collected during the brainstorming discussion. The data includes information on the function "Positioning, Navigation and Timing", the function "Collision

Table 1
The questions of Part 3 of the framework and the related element types.

Element type	Main questions	Possible answers	Additional questions
A – Feedback	1 – What information does the operator need to perform the specified function?	– *Type A* if the source of information is from a controlled process under the specified function – *Type D* if the source of information is another function	2 – From where is the information provided?
B – Control action	1 – What are the actions taken as output of the specified function?	– *Type B* if the output is an action sent to a controlled process under the specified function – *Type D* if the output is information sent to another function	2 – To which function, subfunction or component is the output assigned?
C – Controlled process	– To which function, subfunction or component is the output assigned?	– *Type C* if the output is given to a component under the specified function – *Type D* if the output is sent to another function	NA
D – Other inputs to and outputs from components	– What other information can influence the operator actions?	NA	NA

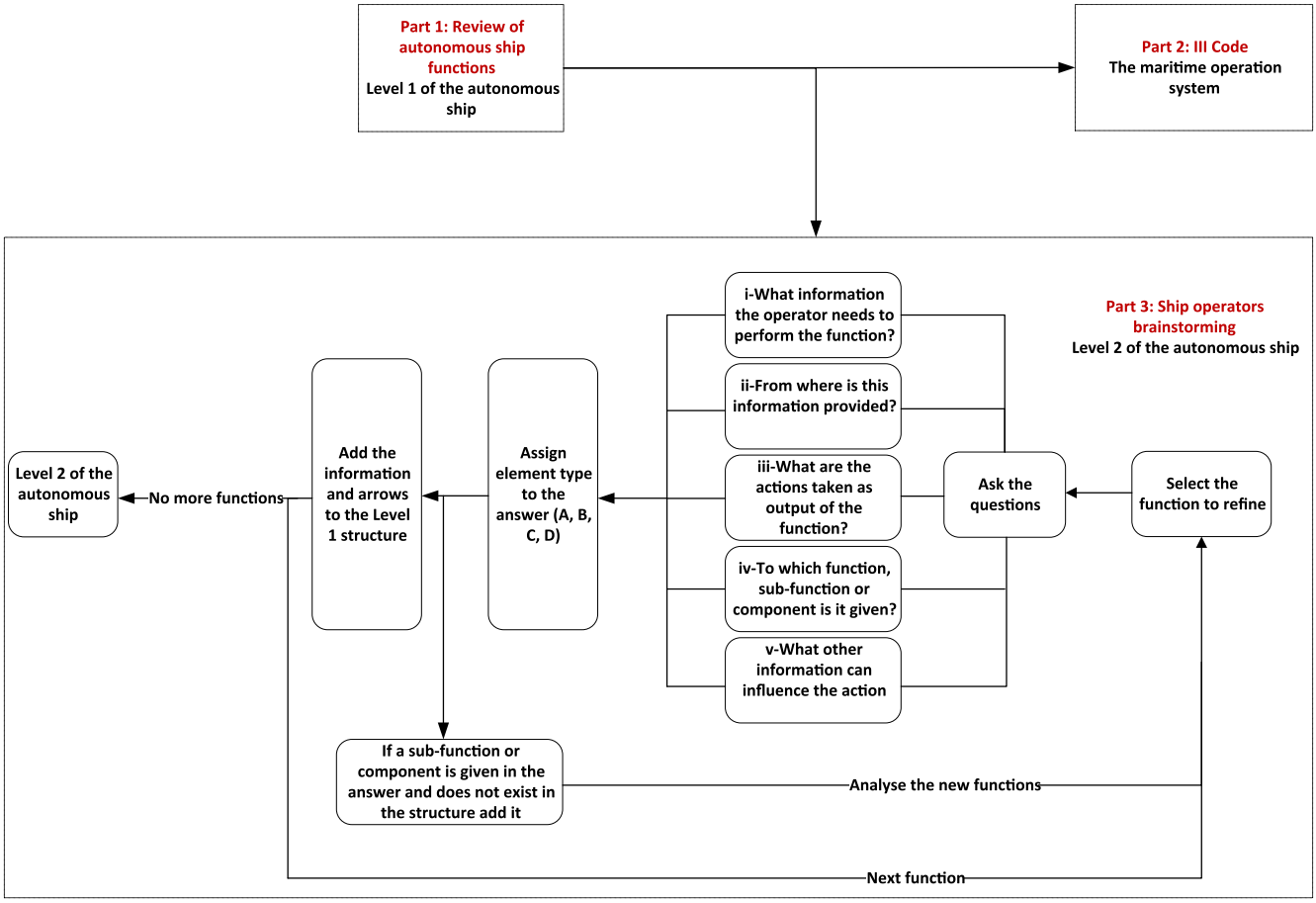


Fig. 3. The proposed framework to develop the hierarchical control structure of an autonomous ship.

Avoidance" and the sub-function "Dynamic Path Planning".

6. Results

The application of Part 2 and Part 3 of the framework, as indicated in Fig. 3, resulted in two hierarchical control structures. These are the control structure of the maritime operation system and the control structure of the Autonomous Navigation System at a more detailed level of abstraction.

Each box in the control structures is a controller at its level of the hierarchy and a controlled process at a higher level of the hierarchy. This hierarchy follows the STPA control structure as described in Section 2. The arrows represent the different types of interaction among the controllers and controlled processes, which are the control actions, feedback and other inputs to or outputs from components.

Fig. 4 shows the control structure of the shipping operation system with an autonomous ship placed as the controlled process in the system instead of a conventional ship. The structure includes the system elements as described in the III Code. The IMO, which issues the regulation that controls international shipping, is at the top of the control structure. Under the IMO, a member state can be a coastal, port and/or flag state and enforces international regulations to ensure safe ship operation. At the state level, the maritime administration is the controller that implements international regulations through national legislation. The maritime administration can at the same time play the role of the port, coastal and flag state administration depending on the maritime policy of the state. At a lower level of hierarchy, the controllers in the structure are the companies and organizations that implement the national rules depending on their role in the system. Under the maritime administration, most of the companies and organizations are designated by their functions in the system structure. First, a port state maritime administration provides cargo handling, tug, pilotage, bunkering and other technical or commercial services. Furthermore, a port state provides different waste reception facilities that help prevent the pollution of the marine environment. Second, a flag state maritime administration nominates and controls the recognized organizations that act on their behalf to ensure that the local shipping companies and the ships with the state flag comply with both national and international regulations. Finally, a coastal state maritime administration provides effective aids to navigation in its coastal waters as well as provides and updates the hydrographic information and nautical charts. It also sets up a vessel traffic service (VTS) centre to guide vessels if traffic density and criticality require it. In addition, it offers radio-communication and meteorological services essential for the safe navigation of ships. It also sets up Search and Rescue Services to identify and rescue ships in distress.

In Fig. 4, the IHO works in coordination with the national hydrographic offices at the state level. These offices are placed as a controlled process under the maritime administration of the coastal state because their function is a responsibility of a coastal state. The SCC in Fig. 4 is placed simultaneously under the control of the flag state (through the shipping company), port and coastal states. The shipping company implements the safety rules through its own procedures and audits to verify compliance of the SCC. Fig. 4 shows that the SCC interacts with the Search and Rescue because one of its tasks is to handle the distress situations.

Appendix A (**it can be seen in a larger format by clicking this hyperlink**) shows the control structure of the navigation function that was developed based on the ship operators' brainstorming session. Some of the feedback or controls added in the structure were self-

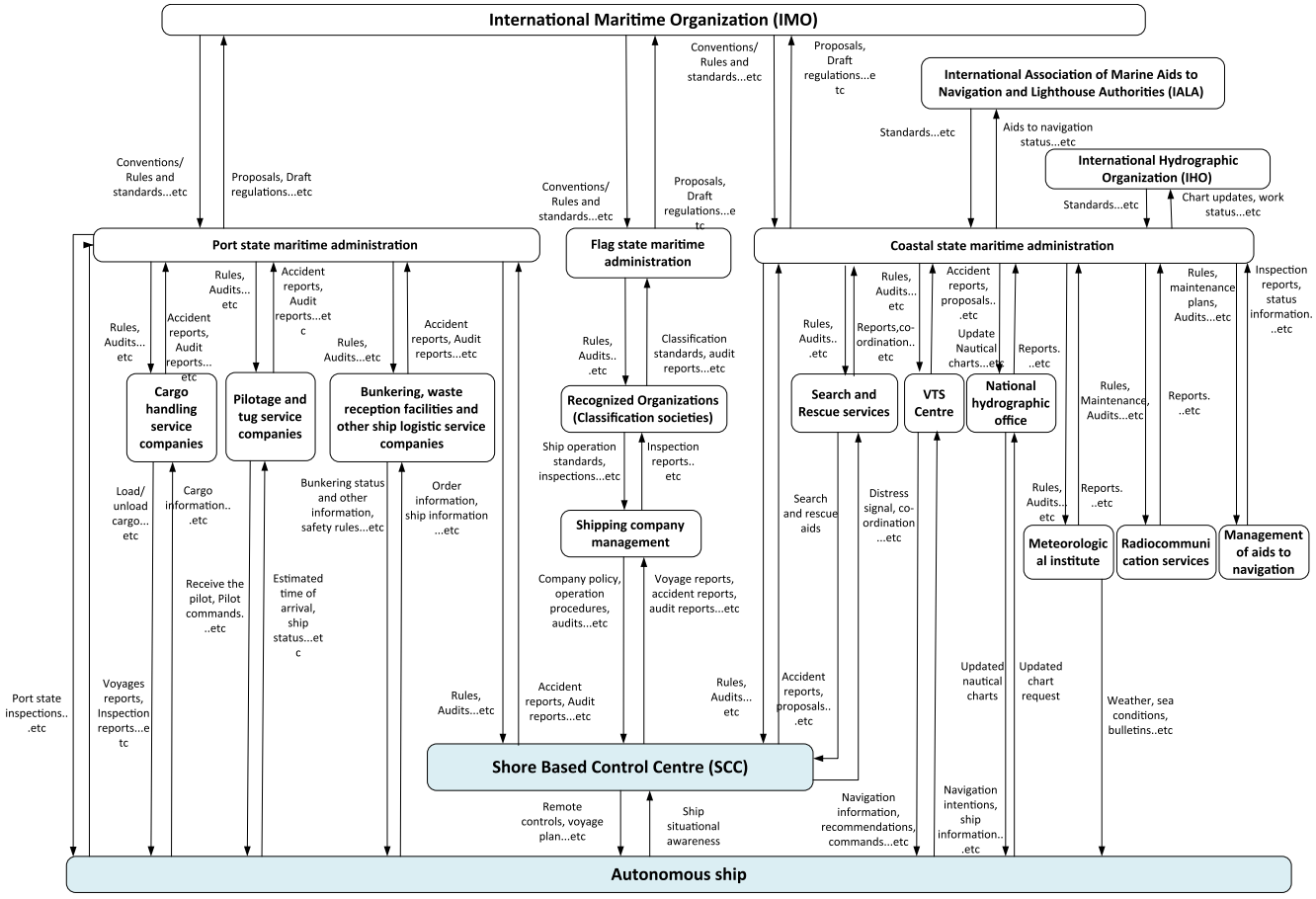


Fig. 4. The hierarchical control structure of the maritime operation system.

evidently necessary, as suggested in the STPA handbook, such as status reports or mode activation. The other types of feedback and controls added to the structure were provided in the operators' answers. At the top of the hierarchy is the autonomous navigation controller, which controls all the other subfunctions contributing to the navigation function. The boxes coloured in grey are the subfunctions that were provided by the operators. These were not previously included in the structure presented in (Chaal et al., 2020). One of the grey boxes is the grounding avoidance system, which verifies that the new generated route path does not pose a risk of grounding. In case of high grounding risk, the system gives an alarm, which was the information given to the ship captain in traditional ship operation. The other grey box added to the structure is the lights system. The operators mentioned that some actions need to be communicated to other ships with a specific light combination. In Appendix A, the anchoring and mooring function is drawn with a dashed line and was not further discussed in the case study because the analysis is limited to autonomous navigation in the open sea. Table 2 below contains a detailed description of the diagram in Appendix A.

7. Discussion

7.1. The framework

The proposed framework allows the development of the control structure of an autonomous ship at different levels of abstraction. The three parts of the framework support the functional description of the autonomous ship. In Part 1, the review of the autonomous ship concept represented an effective method to identify the important functions of the autonomous ship. In Part 2, the III Code is a useful document for the development of the control structure of shipping operation. The code enabled a good understanding of the control and hierarchy of the maritime operation system. Understanding current maritime operation is necessary for the safety analysis of the new generation of ships that will belong to the same system in the future. All the controllers added to the organizational control structure have important roles in shipping operation according to the III Code. Part 3 of the framework enabled utilizing the experience of the bridge crew. The information provided by the crew was valuable and the questions were adequate to guide the discussion with the STPA control structure model in hand. The questions framed the discussion and served as a systematic plan to identify the missing elements of the structure. However, separating Type A (feedback) and Type D (other inputs to and outputs from components) elements was not necessary and did not make difference in developing the control structure. At this stage, when using this framework to uncover the different elements of the control loops from the seafarers' knowledge, it was not useful to separate Type A and Type D elements. The seafarers answered the first question and the last question almost in the same manner. They did not see any essential differences between an instance of feedback and another input and between a control action and another output. Answering the first question of Part 3 was sufficient to provide the information necessary to perform the function. As a result, these two STPA element types can be combined in this framework into one element and referred to as feedback. The feedback could then include any information needed to update the process model and understand the situation before taking actions. Later, when applying the hazard analysis, the difference between these two element types can be determined while tracing back the causal factors of the hazard to define the safety requirements.

Although the STPA handbook gives guidance on developing the

Table 2
Description of the hierarchical control structure of the autonomous navigation system in Appendix A.

Controller	Description and subsystems
Anchoring and mooring	It is in charge of anchoring and mooring functions. It is the controller of the equipment necessary for this function.
Positioning Navigation and Timing (PNT)	It is in charge of defining the ship position heading and speed using the information it receives from the satellite positioning equipment and the ship sensors. It receives the control action from the ANS to provide the Position, Heading and Speed (P,H,S) of own ship and to provide the sensor integrity report. It sends the P,H,S to all the other controllers and subsystems, which need this important information to perform their functions.
Navigational situation awareness	It is in charge of situational awareness related to navigation. It receives the control actions from the ANS to start the lookout in the ship surroundings, to activate the night or day mode and the operation mode (open sea, port approach, keeping position…). It sends feedback to the ANS controller about the status of the ship surroundings for navigation purposes. It also sends feedback about sensor integrity and alarms in addition to the actual mode of navigation. It is the controller of subsystem object detection, object identification and surroundings mapping. It sends data on the detected and identified objects to the collision avoidance system. **Subsystems:** ***Object detection:*** It uses the equipment previously operated on-board by humans to detect objects on the ship route in addition to the Lidar and the equipment replacing human vision and hearing capabilities (cameras and microphones). It receives the control action from the Navigational Situation Awareness controller to start object detection and it receives the range at which to look for the objects. It receives the visibility range and the night/day mode that it considers for the settings it sends to the equipment. It sends feedback to the Navigational Situation Awareness controller as a warning when a new object is detected and it sends data on the detected object. It sends control actions as range settings to the Radar and Lidar depending on the navigation area and visibility level. It also sends zoom and direction settings to the camera. It sends data to the ECDIS and AIS about the area where to look for static objects and ships on the ship route. The received images and data are merged to detect objects in the given range of detection with their location, size and speed. It sends the detected object data to the collision risk assessment controller in order to calculate the risk of collision and enable reaction as early as possible. ***Object identification:*** It uses the same equipment for the identification of the detected objects. It receives the control action from the Navigational Situation Awareness controller to identify the detected object. It also receives data on the detected object in addition to the night/day mode it should consider. It sends feedback to the Navigational Situation Awareness controller about the status of the actual identification of the object and precise data on the object once identified. It also sends feedback about sensor integrity. It sends control actions to the equipment, including camera zoom and direction settings to focus on the location of the detected object. It sends the settings to the Radar and Lidar to focus on the object location and size in order to classify it. It also sends the area to scan to the ECDIS and AIS to establish the identity of the detected object if it is a ship or an aid to navigation or other static object in the MAP. The received images and data from the sensors and equipment are merged to classify and identify the detected objects. It sends data on the identified objects to the surroundings mapping controller, which uses it to update the surroundings map and track the identified objects. ***Surroundings mapping:*** It collects the data on the detected objects and the identified objects and plots them with the map data in order to track them for the rest of the ship voyage. It receives the control action from the Navigational Situation Awareness controller to start surroundings mapping. It sends feedback to the Navigational Situation Awareness controller as a surroundings map with dynamic data.
Collision avoidance	It is in charge of avoiding collisions with objects encountered during navigation. In addition, it is in charge of avoiding grounding during navigation. It is the controller of the subsystems collision risk assessment, dynamic path planning and grounding avoidance. It receives control actions to avoid collision. It also receives the predefined CPA and TCPA (Closest Point of Approach CPA and Time to Closest Point of Approach TCPA) limits it should respect. It compares the calculated CPA and TCPA with the limits to decide on the action to take. It sends feedback to the ANS controller about the actual collision risks and a warning when a high collision risk is identified. It also sends feedback about the collision avoidance manoeuvre status and a warning when the situation is too complex to be managed by the system. It also sends feedback about the grounding risk and a warning in case of high grounding risk. **Subsystems:** ***Collision risk assessment:*** It calculates the risk of collision with the detected objects. It receives the control actions from the Collision Avoidance controller to check the collision risk. It sends feedback to the Collison Avoidance controller as collision risk metrics CPA and TCPA. The speed and heading of dynamic objects is compared to the ship route to calculate the CPA and TCPA. ***Dynamic path planning:*** It generates a new path, different from the actually tracked path in order to avoid collision. It receives control actions from the Collision Avoidance controller to generate the new path. It also receives data on the target object that it should avoid. It receives the COLREGs rule to apply when planning this path. It sends feedback to the Collision Avoidance controller about the status of the path planning and a confirmation when the path is generated. It sends the generated path to the DP system to execute it instead of the actual route plan in order to avoid the collision. ***Grounding avoidance:*** It identifies the risk of grounding during navigation, calculates the under keel clearance and defines the safe contour for the ship. It receives a control action from the Collision Avoidance controller to check the risk of grounding. It sends feedback to the Collision Avoidance controller about the risk of grounding, the under keel clearance and the safe contour. It receives information from the Eco sounder and data on sea depths from the ECDIS map to compare with ship draft and determine the grounding risk and the safe contour. It sends the safe contour to the Dynamic Path Planning to generate a new path that will not pose a risk of grounding.

(*continued on next page*)

Table 2 (*continued*)

Controller	Description and subsystems
Route planning	It is in charge of generating the route plan (the route legs with the ship speed and heading). It receives the control action from the ANS controller to generate the route plan, and also receives the voyage plan information to consider in route planning. It sends feedback to the ANS controller about the current status of route planning and the generated route plan once confirmed. It sends the route plan to the DP system that executes it. It also sends the route plan to the Collision Risk Assessment controller, which compares it with the location of the encountered objects to anticipate and calculate the risk of collision. It sends the route plan to the Collision Avoidance controller to apply the rules for the collision avoidance manoeuvre.
Reporting and communication	It is in charge of communicating with other ships and authorities about the intentions and situation of the ship. It receives control actions from the ANS controller to communicate the planned collision avoidance actions with encountered ships, communicate an emergency or distress situation through the appropriate channels, and automatic reporting through the AIS system. It sends feedback to the ANS about the status of the reporting and communication and the messages received from encountered ships.
Lights system	It is in charge of activating the lights system according to the regulation. The light should communicate certain messages to other ships. A distress situation can be communicated through lights. In case of very low visibility, collision avoidance messages can also be communicated using lights. It receives the control action "activate lights" from the ANS and sends feedback to the ANS about the actual light status.
Weather monitoring and interpretation	It is in charge of monitoring the weather and sea state using the weather information received from different sources and through different channels. It receives information through NAVTEX, one of the pieces of equipment that provides automatic weather and sea forecasts. It also receives wind state information from the on-board wind sensor. It receives the control action "provide weather information" from the ANS. It sends feedback to ANS as compiled weather information necessary for navigation. The visibility level is one of the important items of information that this subsystem identifies and sends to the ANS. It sends the weather and sea information to the Route Planning controller, which uses it to generate a safe and efficient route plan (weather routing).
Dynamic positioning	It is in charge of executing the route plan and keeping the ship in position when ordered. It controls the ship motion through the steering and propulsion system. It receives control actions from the ANS to track the route plan or switch to tracking the collision avoidance path to avoid a collision. It sends feedback to the ANS about the current mode of operation, its alarms, the ship motion and the actual steering and propulsion power. It sends control actions to the steering and propulsion system, which are transferred as motion to the ship body to follow the predefined track. It receives data on actual ship motion from the motion sensors connected to the ship structure. **Subsystems:** ***Steering and propulsion system:*** It is the actuator that transforms the DP commands into ship motion. It gives propulsive power to the ship body and steers it in the required direction (heading).

control structure of a new design by iterating all the hazard analysis steps, starting with the available concept knowledge, this guidance does not always provide the necessary level of support. Each new design involves a different level of available knowledge and therefore a different starting point to the development of a new system. In the case of autonomous ships, the framework proposed in this paper is a supporting tool for using the available knowledge about the concept of an autonomous ship and knowledge on traditional ship operation to define an autonomous ship control structure. It gives additional support to applying STPA to autonomous ships in the current design phase, employing detailed results to develop safe autonomous ships. Applying STPA at this stage is more effective than mitigating hazards when design choices are made.. The framework supports the development of the control structure of an autonomous ship in the current transition efforts towards higher autonomy in shipping. On the other hand, the control structures developed in this paper are not prescriptive. These are functional descriptions of the system that show how future automated controllers can operate the ship if they were to replace human controllers. In addition, the control structure of the maritime operation system shows the challenges facing the safe operation of autonomous ships if they were to be introduced to the current system.

7.2. The control structure of the maritime operation system

The control structure of the maritime operation system describes the system in its current form. Other specific elements could be added based on the structure and policy of a specific maritime administration. The structure includes the controls of the organizational and regulatory system of shipping operation. The structure developed in this part of the framework is necessary for the next steps of the hazard analysis in order to identify the missing elements compared to traditional ship operation. The SCC in this structure is one of the known elements in future autonomous ship operation. Remote operation and ship monitoring from SCCs will be a part of open sea operation, port maneuverers and navigation in areas with dense traffic. However, it is not yet known which administration will provide the service of remote operation and monitoring. For this reason, the SCC was added under the control of the flag state, port state and coastal state administration simultaneously. This shows some of the challenges of introducing autonomous ships in the current shipping system and will help to solve these challenges and guide the development of the system to ensure safe autonomous operation.

The control structure of the maritime operation system does not exist in the literature and it represents one of the main outcomes of the framework presented in this study. Only a part of the organizational level of the maritime operation structure was developed for the STPA analysis by (Wróbel et al., 2018) and was considered to be a major contributor to the uncertainty of their analysis. The structure of maritime operation, the result of Part 2 of the framework in this study, is an essential prerequisite for the STPA analysis of autonomous ships. It will help safety practitioners to consider the organizational layer of autonomous shipping in their analysis. At this early stage, such analysis will oversee the safety-related limitations in the current maritime system and define the recommendations and modifications necessary to

accommodate the new generation of ships and ensure their safe operation. The results of such analysis are also important for the maritime regulators to draft adequate law instruments that will regulate the safety of autonomous shipping.

On the other hand, the structure only includes the system as described in the III Code and presents a possible integration of the autonomous ship and the SCC in the current maritime operation system. The organizations included in this structure might lack the elements necessary to operate autonomous ships, such as a unique controller for the SCC that implements a unified standard for the remote ship operation. These new elements of the structure could be identified by further applying the STPA hazard analysis iteratively in collaboration with maritime regulators and experts.

7.3. The control structure of the autonomous navigation function

The control structure of autonomous navigation is a functional description of the system that could be utilized as a platform to develop new design solutions. This structure is inspired by the control tasks performed by seafarers who have unique practical knowledge. Drawing on this knowledge is valuable in the development of autonomous ships since no experience has yet been gained from their operation. In the case of manned ships, we lean on the seafarers' abilities and experiences to operate the ship safely, due to which many safety requirements do not need to be explicitly specified. However, due to the lack of operational experience from autonomous shipping and from automating seafarers' tasks, their abilities should be captured and all the requirements need to be identified and clearly expressed. Part 3 of the framework was a method to capture the experience and understanding of humans and their control models of the ship in order to add it to the hierarchical control structure. With STPA analysis based on this structure, more detailed safety requirements can be identified.

Nevertheless, the structure is not a prescription for autonomous ship design. Instead, it is a control structure that serves as a basis to conduct the STPA and detect hazardous scenarios and prevent them with adequate changes in the structure. In literature, the applications of STPA to autonomous shipping have adopted hierarchical control structures that considered the limited description of autonomous ships. These structures were simplified initial structures that did not include the different functions of an autonomous ship. Even though the structure presented in this paper has not been validated yet, it can serve as an advanced starting point in applying STPA to an autonomous ship. It may be also used to derive novel design solutions.

The results of Part 3 of the framework (Section 4.3) demonstrated that the autonomous navigation function will be difficult to implement. Two examples that confirm this complexity are object detection and object identification, which both use the same equipment. The deck officers mentioned that they prioritize the use of equipment differently depending on the area of navigation. If the sea area is close to the coast, they perform lookout duties primarily with ECDIS, as it shows the coastline and the aids to navigation on the route. Binocular lookout is performed to double check the objects seen in the ECDIS. However, far from the coast, the operators rely more on radar while adjusting the range to double check the visual observations. In addition, for the object identification function, the bridge crew rely more on the AIS and the ECDIS to confirm if the detected object is a ship shown in the AIS or a static object shown in the ECDIS. The time of day (night or day) also affects which equipment is prioritized in the detection and identification functions. Radars gain more importance than visual lookout during night-time. The visibility level is another factor that affects the choice of equipment during the detection and identification of objects. The visibility level for example is added to the structure with arrows forwarded to the navigational situation awareness subfunction. Depending on the visibility level, navigational situational awareness can then change the mode of object detection and identification. This change affects the control settings given to the equipment and the usage of the images they provide. All the human capabilities of adaptation to the equipment and the external environment must be considered when designing software controllers for the ship functions that will replace human controllers.

Another critical function performed by the operators during navigation is collision avoidance. The operators pointed out that they check the risk of collision with any detected object and change the route path to avoid collision even before identifying the object. These measures comply with COLREGs rules on taking action as early as possible to avoid collision. Thus, in the control structure, the detected object data was first forwarded to the collision avoidance system. During navigation, the operators normally follow the route plan defined after receiving the voyage plan from the captain. In case of risk of collision, the path has to be changed and after the avoidance manoeuvre, the operator returns to the planned route. In order to transfer these conditional actions to the ANS, two modes of operation were added to the DP system, which controls both the propulsion and steering system. These modes are the route tracking mode and the collision avoidance mode. The DP system normally follows the planned route and once a risk of collision is identified and a collision avoidance path is generated, the DP switches from route tracking mode to collision avoidance mode.

The operator's decisions are influenced by the status of the other ship systems and the external environment. The interactions between the ship systems are important also during complex situations. In this application for example, the operators mentioned that they inform the captain in case of complex situations and emergencies such as an eminent risk of collision. Similarly, in the case of an autonomous ship, this information is transferred to the virtual captain. It could also be reported to the SCC if the situation requires human intervention. Other information such as ship stability, manoeuvrability, power availability and other inner capabilities is also important for seafarers in assessing risk and making the right decisions. In the case of autonomous navigation function, the DP system provides information on ship motion in addition to the propulsion and steering status and capabilities. The information from other ship systems such as the stability and integrity system or the autonomous engine monitoring and control system (Fig. 2) was not fully determined in this application. Nevertheless, the interactions among different ship systems to provide information on the inner status of the ship or to solve complex situations could be defined once the other functions are refined. Other details could also be defined when the identification of hazards during autonomous navigation is conducted.

Although the questions answered in Part 3 of the framework guided the process of developing the control structure and identified more interactions among the ANS components, the proposed structures must be further analysed and developed. The validation of the proposed structures is also an essential aspect for further research. The validation process will follow the analysis of the three main aspects marked in STECA (Fleming and Leveson, 2015): completeness of the proposed structures, a detailed analysis of safety-related responsibilities in the controls of the structures, and the review of the coordination of roles and their implications and consistency in the structure.

Nevertheless, we (the authors) believe that the dissemination of the results of this study at this stage can contribute to the work of scientists and industry involved in the development of autonomous ship concepts. They can build on top of the current structures to change or add more organizational, operational and design safety decisions. The results of this study provide evidence on how humans currently perform their tasks on board ships and how this knowledge could be transferred to automated controllers without affecting the current safety levels. Moreover, the proposed controls can also guide the development of new technology for manned ships and gradually develop a path towards autonomous shipping.

8. Conclusion

This study presents a framework to develop a hierarchical control structure of autonomous ships for implementing the STPA hazard analysis and safety-integrated design of these ships. The framework consists of three parts that are based on the foundations and methodologies of STPA and STECA.

The application of the framework seems to be suitable for modelling a hierarchical control structure of the maritime operation system that will accommodate autonomous ships. The autonomous ship and the Shore-based Control Centre (SCC) were integrated as controlled processes in the structure and their possible interactions with the other components of the structure were identified. The organizational control structure of the maritime operation was lacking in previous safety analysis of autonomous ships, which makes the outcome of this framework essential for future analysis. In addition, the application of the framework to the navigation function as a case study succeeds in utilizing the valuable experience of seafarers to develop an advanced hierarchical control structure for the Autonomous Navigation System (ANS). The discussion with experienced seafarers added substantial features to the control structure of the ANS and identified important interactions among its components.

The control structure will then be used as an advanced starting point to apply STPA analysis to enhance the control structure and identify the eventual safety, resilience and reliability requirements of autonomous ships. The developed control structures should be validated for completeness and consistency. This task will be conducted in the future by following the validation approach proposed in the STECA methodology. In addition, the framework could be extended to other ship functions. This extended analysis will support a better understanding of the interactions between the ship system functions.

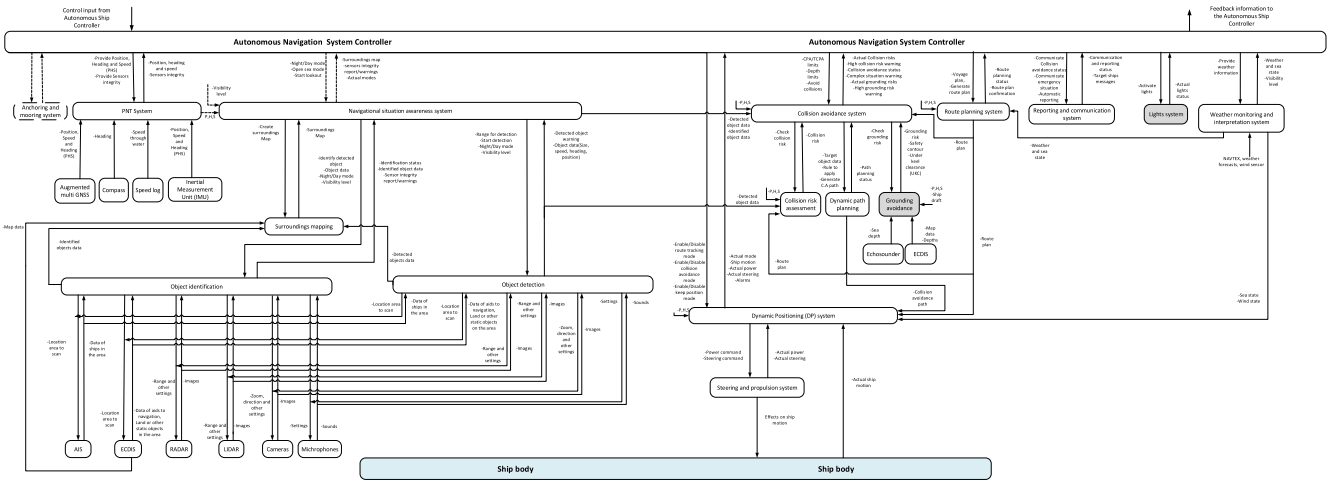
Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

The study presented in this article is part of the work carried out in the RTF (Operational Design) in the Rethinking Autonomy and Safety (RAAS) research initiative in Finland, and it is extended for the application of the work carried out in the Sea for Value (S4V) – Fairway research programme, which is partially funded by Business Finland. Spyros Hirdaris acknowledges financial support from the Academy of Finland University competitive funding award (SA Profi 2-T20404). The authors would like to express their gratitude to all the seafarers who participated in the brainstorming sessions as part of this work.

Appendix A



Appendix B

See Tables 3–5.

Table 3
Brainstorming data of the function Positioning Navigation and Timing (PNT).

Element type	Main question	Answer to the main question	Additional question	Answer to the additional question
A-Feedback	1-What information does the operator need for the positioning, Navigation and Timing	The ship position from different sources. The ship speed from different sources. The ship heading from different sources.	2-From where is the information provided?	One source of the position, heading and speed (over ground) is the GNSS. The speed log is another source for the speed (through water). The magnetic compass is another source of heading when needed. The inertial measurement unit gives the position, heading and speed (over ground) but with a accumulated error.
B-Control action	3-What are the actions taken as output of the specified function?	We identify the status of the sensors by comparing the different measurements. We inform the captain in case we lose position or we have a critical problem with the sensors. We use the determined position, heading and speed to navigate.	4-To which function, sub-function or component is the output given?	The ship captain should know about the sensors problem.
C-Controlled process	5-To which function, sub-function or component is the output given?	(Given in the previous answer)	NA	
D-Other inputs to and outputs from components	6-What other information can influence the operator actions	No more answers	NA	

Table 4
Brainstorming data of the function collision avoidance.

Element type	Main question	Answer to the main question	Additional question	Answer to the additional question
A-Feedback	1-What information does the operator need to avoid collisions	The own ship position, heading and speed. The own ship route. The position, speed and heading of the objects in the ship vicinity. The defined CPA and TCPA by the company. The collision avoidance rules.	2-From where is the information provided?	The position, heading and speed are checked from the PNT equipment. The own ship route is defined when planning for the voyage. The objects in the vicinity are detected during lookout. The CPA and TCPA are given by the company (ship captain). We study the collision avoidance rules and use the COLREGs convention case by case (it could be coded in the Collision Avoidance controller).
B-Control action	3-What are the actions taken as output of the specified function?	We check the risk of collision with the objects in the ship vicinity. We inform the captain in case of high collision risk. In case there is a risk of collision, we identify the COLREGs rule to apply. We inform the captain if we have a difficult situation. We change the ship path if we have to do it. We check that the new path does not drive the ship aground.	4-To which function, sub-function or component is the output given?	Normally the object is plotted in the (ARPA) Automatic Radar Plotting Aid, which assesses the risk of collision. The captain is informed with warnings about high risk of collision and about the difficulty to handle the situation. The collision rule to apply is used to define the collision avoidance path. The grounding risk is checked with a cross verification of different means: the safety contour from ECDIS, the UKC from echo sounder, and the depth provided in the map with the ship draft.
C-Controlled process	5-To which function, sub-function or component is the output given?	(Given in the previous answer)	NA	
D-Other inputs to and outputs from components	6-What other information can influence the operator actions	No more answers	NA	

Table 5
Brainstorming data of the sub-function dynamic path planning.

Element type	Main question	Answer to the main question	Additional question	Answer to the additional question
A-Feedback	1-What information does the operator need to generate a collision avoidance path	The own ship position, heading and speed.	2-From where is the information provided?	The position, heading and speed are checked from the PNT equipment.
		The position, speed and heading of the object to avoid.		The data of the object to avoid is provided when the object is confirmed to be a collision target.
		The collision avoidance applicable rule.		The rule to apply is provided from the Collision avoidance controller.
B-Control action	3-What are the actions taken as output of the specified function?	We define a route path to avoid collision with the target object with a minimum deviation from the route plan.	4-To which function, sub-function or component is the output given?	The collision avoidance path is executed as commands to the steering and propulsion system manually or through the autopilot (DP for autonomous ships)
C-Controlled process	5-To which function, sub-function or component is the output given?	(Given in the previous answer)	NA	
D-Other inputs to and outputs from components	6-What other information can influence the operator actions	The type of cargo influences the rate of turn of the new path. Some cargo can move rapidly and affect stability if the rate of turn is high.	NA	

References

AAWA, 2016. Remote and autonomous ships the next steps.

Abdulkhaleq, A., Wagner, S., Leveson, N., 2015. A comprehensive safety engineering approach for software-intensive systems based on STPA. Procedia Eng. 128, 2–11. https://doi.org/10.1016/j.proeng.2015.11.498.

Autoferry, 2016. Autoferry - NTNU [WWW Document]. URL https://www.ntnu.edu/autoferry (accessed 1.21.20).

Basnet, S., Valdez Banda, O.A., Hirdaris, S., 2019. The management of risk in autonomous marine ecosystems – preliminary ideas. Proceedings of the First International Workshop on Autonomous Systems Safety.

Blanke, M., Henriques, M., Bang, J., 2018. A pre-analysis on autonomous ships.

Brekke, E.F., Wilthil, E.F., Eriksen, B.-O.H., Kufoalor, D.K.M., Helgesen, Ø.K., Hagen, I.B., Breivik, M., Johansen, T.A., 2019. The Autosea project: Developing closed-loop target tracking and collision avoidance systems. J. Phys.: Conf. Ser. 1357. https://doi.org/10.1088/1742-6596/1357/1/012020.

Chaal , M. , Valdez-Banda , O.A. , Basnet , S. , Hirdaris , S. , Kujala , P. , 2020 . Proceedings of the international seminar on safety and security of autonomous vessels (ISSAV) and European STAMP Workshop and Conference (ESWC) 2019. Sciendo, Warsaw, Poland . https://doi.org/10.2478/9788395669606-012.

Fleming, C.H., 2015. Safety-driven Early Concept Analysis and Development.

Fleming, C.H., Leveson, N., 2015. Integrating systems safety into systems engineering during concept development. INCOSE International Symposium 25, 989–1003. https://doi.org/10.1002/j.2334-5837.2015.00111.x.

Fleming, C.H., Spencer, M., Thomas, J., Leveson, N., Wilkinson, C., 2013. Safety assurance in NextGen and complex transportation systems. Saf. Sci. 55, 173–187. https://doi.org/10.1016/j.ssci.2012.12.005.

Glomsrud, J.A., Xie, J., 2019. A Structured STPA Safety and Security Co-analysis Framework for Autonomous Ships. Presented at the ESREL 2019.

Heffner, K., Rødseth, Ø.J., 2019. Enabling technologies for maritime autonomous surface ships. 012021. J. Phys.: Conf. Ser. 1357. https://doi.org/10.1088/1742-6596/1357/1/012021.

Hollnagel, E., 2014. Safety-I and safety-II: the past and future of safety management. Ashgate Publishing Company, Farnham, Surrey, UK England, Burlington, VT, USA.

IALA, 2020. About IALA [WWW Document]. IALA AISM. URL https://www.iala-aism.org/about-iala/ (accessed 1.19.20).

IHO, 2020. Home | IHO [WWW Document]. URL https://iho.int/ (accessed 1.19.20).

IMO, 2019. Autonomous shipping [WWW Document]. URL http://www.imo.org/en/MediaCentre/HotTopics/Pages/Autonomous-shipping.aspx (accessed 8.13.20).

IMO, 2018. Report of the maritime safety committee on its one hundredth session.

IMO, 2013. IMO instruments implementation code (III CODE), Resolution A. 1070(28).

Ishimatsu, T., Leveson, N., Thomas, J.P., Fleming, C.H., Katahira, M., Miyamoto, Y., Ujiie, R., Nakao, H., Hoshino, N., 2014. Hazard analysis of complex spacecraft using systems-theoretic process analysis. J. Spacecraft Rockets 51, 509–522. https://doi.org/10.2514/1.A32449.

Kongsberg, 2018. YARA selects Norwegian shipbuilder VARD for zero-emission vessel Yara Birkeland - KONGSBERG [WWW Document]. URL https://www.kongsberg.com/news-and-media/news-archive/2018/yara-selects-norwegian-shipbuilder-vard-for-zero-emission-vessel-yara-birkeland/ (accessed 7.5.19).

Kufoalor, D.K.M., Wilthil, E., Hagen, I.B., Brekke, E.F., Johansen, T.A., 2019. Autonomous COLREGs-compliant decision making using maritime radar tracking and model predictive control. In: 2019 18th European Control Conference (ECC). Presented at the 2019 18th European Control Conference (ECC), IEEE, Naples, Italy, pp. 2536–2542. https://doi.org/10.23919/ECC.2019.8796273.

Levander, O., 2017. Autonomous ships on the high seas. IEEE Spectr. 54, 26–31. https://doi.org/10.1109/MSPEC.2017.7833502.

Leveson, N., 2015. A systems approach to risk management through leading safety indicators. Reliab. Eng. Syst. Saf. 136, 17–34. https://doi.org/10.1016/j.ress.2014.10.008.

Leveson, N., 2004. A new accident model for engineering safer systems. Saf. Sci. 42, 237–270. https://doi.org/10.1016/S0925-7535(03)00047-X.

Leveson, N.G., 2011. Engineering a Safer World, < systems Thinking Applied to Safety.

Leveson, N., Fleming, C.H., Spencer, M., Thomas, J., Wilkinson, C., 2012. Safety assessment of complex, software-intensive systems. SAE Int. J. Aerosp. 5, 233–244. https://doi.org/10.4271/2012-01-2134.

Leveson, N., Thomas, J., 2018. STPA HANDBOOK.

Linkov, I., Anklam, E., Collier, Z.A., DiMase, D., Renn, O., 2014. Risk-based standards: integrating top–down and bottom–up approaches. Environ. Syst. Decis. 34, 134–137. https://doi.org/10.1007/s10669-014-9488-3.

Linkov, I., Trump, B.D., Anklam, E., Berube, D., Boisseasu, P., Cummings, C., Ferson, S., Florin, M.V., Goldstein, B., Hristozov, D., Jensen, K.A., Katalagarianakis, G., Kuzma, J., Lambert, J.H., Malloy, T., Malsch, I., Marcomini, A., Merad, M., Palma-Oliveira, J., Perkins, E., Renn, O., Seager, T., Stone, V., Vallero, D., Vermeire, T., 2018. Comparative, collaborative, and integrative risk governance for emerging technologies. Environ. Syst. Decisions 38, 170–176. https://doi.org/10.1007/s10669-018-9686-5.

Lloyds Register, 2017. LR_Code_for_Unmanned_Marine_Systems.

Montewka, J., Wróbel, K., Heikkila, E., Valdez-Banda, O., Goerlandt, F., Haugen, S., 2018. Challenges, solution proposals and research directions in safety and risk assessment of autonomous shipping. Los Angeles 12.

MUNIN, 2016. Final Report Summary - MUNIN (Maritime Unmanned Navigation through Intelligence in Networks) | Report Summary | MUNIN | FP7 | CORDIS | European Commission [WWW Document]. URL https://cordis.europa.eu/project/rcn/104631/reporting/en (accessed 6.26.19).

Omitola, T., Downes, J., Wills, G., Zwolinski, M., Butler, M., 2018. Securing navigation of unmanned maritime systems. Presented at the International Robotic Sailing Conference 2018.
Ramos, M.A., Thieme, C., Utne, I.B., Mosleh, A., 2019. Autonomous systems safety – state of the art and challenges. In: 1st IWASS. NTNU.
Ramos, M.A., Thieme, C.A., Utne, I.B., Mosleh, A., 2020. Human-system concurrent task analysis for maritime autonomous surface ship operation and safety. 106697. Reliab. Eng. Syst. Saf. 195. https://doi.org/10.1016/j.ress.2019.106697.
Rasmussen, J., 1997. Risk management in a dynamic society: a modelling problem. Saf. Sci. 27, 183–213. https://doi.org/10.1016/S0925-7535(97)00052-0.
Renn, O., 2017. Risk governance: Concept and application to systemic risk. Risk Conundrums: Solving Unsolvable Problems 243–259.
Renn, O., Klinke, A., 2004. Systemic risks: a new challenge for risk management. EMBO Rep. 5, S41–S46. https://doi.org/10.1038/sj.embor.7400227.
Rodseth, O., Nordahl, H., Hoem, A., 2018. Characterization of Autonomy in Merchant Ships, in: 2018 OCEANS - MTS/IEEE Kobe Techno-Oceans (OTO). Presented at the 2018 OCEANS - MTS/IEEE Kobe Techno-Ocean (OTO), IEEE, Kobe, pp. 1–7. https://doi.org/10.1109/OCEANSKOBE.2018.8559061.
Rokseth, B., Haugen, O.I., Utne, I.B., 2019. Safety verification for autonomous ships. MATEC Web Conf. 273, 02002. https://doi.org/10.1051/matecconf/201927302002.
Rolls Royce, 2018. Rolls-Royce and Finferries demonstrate world's first Fully Autonomous Ferry [WWW Document]. URL https://www.rolls-royce.com/media/press-releases.aspx (accessed 1.21.20).
Smart Ships Coalition, 2017. Smart Ships Coalition [WWW Document]. Smart Ships Coalition. URL https://smartshipscoalition.org/maritime-autonomy-research-site-mars/ (accessed 1.21.20).
Solberg, C.L., 2018. An STPA Analysis of the ReVolt.
Sulaman, S.M., Beer, A., Felderer, M., Höst, M., 2019. Comparison of the FMEA and STPA safety analysis methods–a case study. Software Qual. J. 27, 349–387. https://doi.org/10.1007/s11219-017-9396-0.
Thieme, C.A., Guo, C., Utne, I.B., Haugen, S., 2019. Preliminary hazard analysis of a small harbor passenger ferry – results, challenges and further work. J. Phys.: Conf. Ser. 1357, 012024. https://doi.org/10.1088/1742-6596/1357/1/012024.
Thieme, C.A., Utne, I.B., Haugen, S., 2018. Assessing ship risk model applicability to marine autonomous surface ships. Ocean Eng. 165, 140–154. https://doi.org/10.1016/j.oceaneng.2018.07.040.
Thomas, J., Sgueglia, J., Suo, D., Leveson, N., Vernacchia, M., Sundaram, P., 2015. An integrated approach to requirements development and hazard analysis. Presented at the SAE 2015 World Congress & Exhibition, pp. 2015-01–0274. https://doi.org/10.4271/2015-01-0274.
Utne, I.B., 2017. NTNU Centre for Autonomous Marine Operations and Systems: - Shipping and digitalization.
Utne, I.B., Rokseth, B., Sørensen, A.J., Vinnem, J.E., 2020. Towards supervisory risk control of autonomous ships. 106757. Reliab. Eng. Syst. Saf. 196. https://doi.org/10.1016/j.ress.2019.106757.
Valdez Banda, O.A., Kannos, S., 2017. Hazard analysis process for autonomous vessels.
Valdez Banda, O.A., Kannos, S., Goerlandt, F., van Gelder, P.H.A.J.M., Bergström, M., Kujala, P., 2019. A systemic hazard analysis and management process for the concept design phase of an autonomous vessel. 106584. Reliab. Eng. Syst. Saf. 191. https://doi.org/10.1016/j.ress.2019.106584.
Valdez Banda, O.A., Kujala, P., Goerlandt, F., Bergström, M., Ahola, M., van Gelder, P.H.A.J.M., Sonninen, S., 2018. The need for systematic and systemic safety management for autonomous vessels. Presented at the Marie Design XIII.
van de Poel, I., Robaey, Z., 2017. Safe-by-design: from safety to responsibility. Nanoethics 11, 297–306. https://doi.org/10.1007/s11569-017-0301-x.
Ventikos, N.P., Louzis, K., 2019. The Future of Risk in the Context of Autonomous Ship Operation, in: 1st IWASS.
Wilthil, E.F., Flåten, A.L., Brekke, E.F., 2017. A target tracking system for ASV collision avoidance based on the PDAF. In: Fossen, T.I., Pettersen, K.Y., Nijmeijer, H. (Eds.), Sensing and Control for Autonomous Vehicles. Springer International Publishing, Cham, pp. 269–288. https://doi.org/10.1007/978-3-319-55372-6_13.
Wróbel, K., Gil, M., Montewka, J., 2020. Identifying research directions of a remotely-controlled merchant ship by revisiting her system-theoretic safety control structure. 104797. Saf. Sci. 129. https://doi.org/10.1016/j.ssci.2020.104797.
Wróbel, K., Krata, P., Montewka, J., 2019. Preliminary results of a system-theoretic assessment of maritime autonomous surface ships'. Safety. ResearchGate.
Wróbel, K., Montewka, J., 2019. Comments to the article by Ramos et al. 'Collision avoidance on maritime autonomous surface ships: Operators' tasks and human failure events' (Safety Science Vol. 116, July 2019, pp. 33–44). Saf. Sci. https://doi.org/10.1016/j.ssci.2019.03.024.
Wróbel, K., Montewka, J., Kujala, P., 2018. Towards the development of a system-theoretic model for safety assessment of autonomous merchant vessels. Reliab. Eng. Syst. Saf. 178, 209–224. https://doi.org/10.1016/j.ress.2018.05.019.
Wróbel, K., Montewka, J., Kujala, P., 2017. Towards the assessment of potential impact of unmanned vessels on maritime transportation safety. Reliab. Eng. Syst. Saf. 165, 155–169. https://doi.org/10.1016/j.ress.2017.03.029.
Zou, J., 2018. Systems-Theoretic Process Analysis (STPA) Applied to the Operation of Fully Autonomous Vessels.