Valdez Banda, Osiris; Kannos, Sirpa; Goerlandt, Floris; van Gelder, Pieter H.A.J.M.; Bergström, Martin; Kujala, Pentti

A systemic hazard analysis and management process for the concept design phase of an autonomous vessel

Published in:
Reliability Engineering and System Safety

DOI:
10.1016/j.ress.2019.106584

Published: 01/11/2019

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

Reliability Engineering and System Safety 191 (2019) 106584

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

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

A systemic hazard analysis and management process for the concept design phase of an autonomous vessel

Osiris A. Valdez Banda[a,*], Sirpa Kannos[b], Floris Goerlandt[c], Pieter H.A.J.M. van Gelder[d], Martin Bergström[a], Pentti Kujala[a]

[a] Aalto University, Department of Mechanical Engineering (Marine Technology), Research Group on Maritime Risk and Safety, P.O. Box 15300, 00076 Aalto, Finland
[b] NOVIA University of Applied Science, Turku, Finland
[c] Dalhousie University, Department of Industrial Engineering, Halifax, Nova Scotia B3H 4R2, Canada
[d] Delft University of Technology, Faculty of Technology, Policy and Management, Safety and Security Science Group, Delft, the Netherlands

ARTICLE INFO

Keywords:
Autonomous vessels
Hazard analysis and management
STPA
Maritime system safety
Maritime safety controls
Maritime safety management strategy

ABSTRACT

Autonomous vessels have become a topic of high interest for the maritime transport industry. Recent progress in the development of technologies enabling autonomous systems has fostered the idea that autonomous vessels will soon be a reality. However, before the first autonomous vessel can be released into her actual context of operation, it is necessary to ensure that it is safe. This is a major challenge as the experience of autonomous ships is very limited. This study highlights the need for elaborating a systemic and systematic hazard analysis since the earliest design phase of an autonomous vessel. In particular, it proposes a process for elaborating an initial hazard analysis and management that provides coherent, transparent and traceable safety input information for the design of an autonomous vessel. The process is applied to analyse the hazards of two autonomous vessel concepts for urban transport in the city of Turku, Finland.

1. Introduction

The introduction of autonomous ships in the maritime industry will induce disruptive changes in the execution of maritime traffic operations. The idea of fully autonomous and unmanned ships is not new, it has been discussed for about a decade in the maritime industry [1]. However, the topic is nowadays of high interest within the entire maritime cluster, in part due to the increasing maturity of technologies linked to the support and execution of autonomous vessels. Apart from creating the enticing visions of future shipping, industry leaders provide strong arguments to convince all stakeholders that the first autonomous vessel is about to be ready for her first operation [2].

Nevertheless, autonomous vessels, as other smart vehicles, require the support of an entire smart system [3]. The organizations investing in the development of autonomous vessels are aware about this and allocate resources and efforts to create the structures needed for the constitution of an entire autonomous maritime system [4]. One essential aspect for ensuring the correct functioning of such a system is the assurance and management of safety. A criterion for an autonomous vessel is to be at least as safe as the most advance manned ships [5,6]. This represents an initial high-level demand that requires innovative approaches to develop safety management strategies for ensuring this target.

Different studies have been elaborated to analyze the initial safety and risk management challenges that autonomous ships will face. Some of these include the analysis of safety risks for the general concept of autonomous vessels, identifying concrete challenging aspects for the execution of operations and prevention of accidents [7,8]. Others include the analysis of safety risks for a particular type of vessel and its autonomous system, reviewing a semi-defined operative context and a determined escalation process representing diverse degrees of autonomy [5,9–11]. Other studies focused on the challenges for transferring the roles of personnel involved in the management of safety to the foreseen operational context of autonomous vessels [12-15]. Other studies present an initial analysis of related legal challenges [16,17]. In addition, there are studies analyzing and testing safety aspects in particular navigational operations with the use of autonomous prototypes in simulated environments [18–20].

Most of these studies have presented analyses based on data lacking specific details about the actual design characteristics of the autonomous vessel, its operative context, and the practices for managing the safety of its operation. This is a common limitation to researchers as the most update developments of this topic are mainly proprietary knowledge, discussed internally in the industrial organizations competing for

* Corresponding author.
E-mail address: osiris.valdez.banda@aalto.fi (O.A. Valdez Banda).

https://doi.org/10.1016/j.ress.2019.106584
Received 5 December 2017; Received in revised form 6 July 2019; Accepted 14 July 2019
Available online 15 July 2019

the leadership of autonomous shipping [21]. Nevertheless, the listed studies have remarkably achieved the identification of safety management gaps, challenges, and potential demands for the design of autonomous maritime systems. In fact, some of these studies have provided initial solutions for the management and assurance of safety of autonomous vessels. These studies have also evidenced the need for considering the safety management of an autonomous vessel from different angles of the entire autonomous system where it belongs. This requires to design and implement tools for hazard and risk analysis, accident prevention, and safety management which are capable of supporting the design of such systems.

In the analysis of the risks of the current operational mode of the maritime traffic, a significant number of studies have been elaborated. This includes the analysis of the risk of ship to ship collision [22–33], the risk of ship grounding [34–40], and the risk of fire on-board [41–45].

These studies provide operational information which is used as a basis to develop and update frameworks for the risk analysis of maritime transportation systems [24,46] and risk-based ship design [47–49]. These frameworks provide valuable feedback of the current functioning of the maritime traffic operations and crucial information about the integrated elements in the design of vessels. In the context of autonomous vessels, the application of these frameworks has to be considered for transferring crucial components of maritime safety into the design of autonomous vessels and autonomous maritime systems. This approach has been utilized in a preliminary assessment of the potential impact of unmanned vessels on maritime transportation safety in [8], making a coherent combination of existing accident information and their evaluation in the operational context of autonomous vessels.

In this study, a systemic and systematic hazard analysis and management process for the concept design phase of an autonomous vessel within its operative context is presented. The aim is to create a process capable of executing an initial analysis of safety hazards in the earliest design phase before the planning of the ship design, materials, structures, components, systems and the services linked to the functioning of the autonomous vessel. This analysis aims at producing valuable information to make the systemic and systematic integration of safety controls that need to be implemented in the development of the initial safety management strategy of the autonomous vessel and the entire autonomous ecosystem where it operates.

This proposed process is applied to analyze the safety hazards in the foreseen functioning of two concepts of autonomous ferries operating in specific urban waterways in and near the city of Turku in Finland. The application considers the outcome produced in previous risk analyses of maritime traffic, including those executed for the analysis of the current operation mode and analyses elaborated to assess anticipated operational contexts of autonomous shipping. Based on this information, the main type of accidents and hazards in the operational context of these ferries are identified. Then, with the support of maritime safety experts and experts of automation and technologies related, high-level safety controls to mitigate the hazards are proposed. These controls are used to develop an initial safety management strategy for the autonomous ferries. This provides a systemic representation of safety controls in the operative context of these autonomous ferries, supporting the initial delegation of safety management roles, tasks, and responsibilities.

The rest of the article is organized as follows. Section 2 defines the theoretical foundation for the hazard analysis. Section 3 introduces the background describing the purpose and mission of the two autonomous ferries. Section 4 presents the process of analysis. Section 5 presents the implementation of the proposed process. Section 6 discusses the research findings, limitations and future research. Section 7 provides the final conclusions of this study.

2. Hazard analysis perspective

This study adopts a constructivist basis for hazard analysis, i.e. based on the views of experts about the possible occurrence of events of interest with the most up to date information [23]. With this approach, the presented hazard analysis aims to be considered as a means for reflection and provision of the most reliable and up to date knowledge for safety assurance and the development of a safety management strategy.

The proposed process of analysis is based on a safety engineering approach linked to the System- Theoretic Process Analysis (STPA) included within the Systems-Theoretic Accident Modeling and Processes (STAMP) [50]. STAMP is an approach to depict and review the function of safety from a systemic perspective. It analyses accidents by making a review of the entire socio-technical system [51–53]. Thus, it provides a more systemic way to model accidents and safety for producing a better and less subjective understanding about how accidents occur and how they can be prevented [54–56].

STAMP promotes hazard analysis going beyond component failures. For this, it introduces the STPA which is a hazard analysis technique that identifies accident scenarios that encompass the entire accident process by including design errors, component interactions, and other social, organizational, and management factors in the analysis [50]. Previously, both STAMP and STPA have been satisfactorily applied in the analysis of the safety of autonomous systems in other transportation domains such as the automobile [57] and aviation [58–60].

In line with the STPA, the process focuses on defining accidents that can occur in a certain operational context of an autonomous vessel. It identifies and analyses hazards that can lead to these accidents. The process incorporates the description of the hazards causal factors, and a comprehensive definition and review of risk mitigation actions. It includes a systemic representation of safety controls and the initial definition of the safety management strategy. Moreover, it supports the identification of new potential safety roles and tasks, and a preliminary delegation of safety responsibilities.

For the implementation of the process for hazard analysis, existing accident information, judgments and assumptions are utilized. The purpose is to provide a systematic and itemized initial list of safety controls in order to establish a consistent initial safety management strategy for further development in later design stages.

3. Background

The application of the hazard analysis and management process presented in this study focuses on the analysis of two specific concepts of autonomous ferries for urban transport.

3.1. Autonomous ferry “A”

This first concept has a mission to transport passengers from one side to the Aura River in the city of Turku to the other, as the potential route presented in Fig. 1. The distance navigated by this ferry is about 100 m in total. The passenger capacity for this ferry is not yet defined, current ferries (man controlled) with similar mission and operations in the same area have a capacity of 75 passengers. The operational function of the ferries is described as follows:

a) Passengers aboard the ferry while it is docked
b) The boarding process is finalized
   b.1) The access gate in the pier is closed
   b.2) The access door in the vessel in closed
c) The ferry undocks
d) The ferry begins its voyage
e) The ferry reach the other side of the river and it is docked
f) The passengers disembark the ferry (after this is concluded operation “a” is repeated)

Fig. 1. Hypothetical operational routes for ferries "A" and "B" in urban waterways of the city of Turku.

3.2. Autonomous ferry "B"

This second concept has the mission to transport passengers from a location close to downtown of the city of Turku at the Aura River to a new pier to be located in the Ruissalo Island, see Fig. 1 for an approximate route location. The ferry starts its buoyancy from a pier located at the Aura River in Turku downtown, it navigates through a sheltered sea area for a short time, and reach its destination in Ruissalo Island. The distance navigated is around 8 km. Also in this concept, the passenger capacity is not yet defined. The boarding and disembarking processes are similar to the one specified for ferry "A". Technical and design characteristics of these ferries are not yet defined. In order to support this task, this study utilizes the described ferry missions as the context to implement the hazard analysis and management process presented in this study.

4. Process for hazard analysis and management

4.1. Process foundations

As specified in Section 2, the content and structure of the process for hazard analysis introduced in this section are based on the foundations of system safety engineering, particularly in STAMP and STPA. The foundations of STAMP and STPA enable the development of analysis processes that can be used in an early design phase, providing initial information necessary to guide later design stages. The aim is to consider safety in the earliest conceptual design phase to efficiently influence the design process [50].

The process foundations are also linked to the ship design spiral presented in Evans (1959). The spiral introduces a process for affecting ship design [61]. In the spiral, the specification of the ship mission is the starting point for the concept design phase, continuing with preliminary power estimations, a propulsion system, a hull shape, a general arrangement, preliminary hydrostatic and hydrodynamic calculations and preliminary cost estimations.

The elements of the spiral are elaborated and reviewed in four phases: concept design, and preliminary design, contract design, and detail design. The elements are continuously reviewed with the main customer to find the most efficient overall design [62]. Incorporating risk assessment and goal-based design for accident prevention is an important part of the ship design spiral [63]. However, the approach to assess the risks and the goal-based design in the spiral is focused on the safety regulations of the current maritime traffic operations and the specifications defined mainly by the customer [47].

Fig. 2 describes the aim of executing the proposed process for hazard analysis before the concept design phase of the autonomous vessel. In the figure, the process is introduced in a phase called level 0 (pre-concept design). This phase aims at executing the systematic hazard analysis and management process when the general description of the mission and the potential operational context of the autonomous vessel are defined. The objective is to define safety controls for the initial safety management strategy of an autonomous vessel.

In order to define the safety controls, the study considers the view of diverse stakeholders involved in the entire autonomous system. This includes suppliers and business partners, safety authorities and regulators, emergency response organizations, among others. The controls and the formulated safety strategy has to be assessed and continued in the following design phases of the spiral. The aim is to systematically develop a dynamic safety management strategy which continuously evolved during vessel design process. Thus, the information in this initial safety management strategy focuses on providing systematic and systemic information to support the design of the elements in the subsequent phases of the ship design spiral.

Finally, the process foundations included the ideology behind the Design for Responsibility concept [64]. The concept remarks that safety cannot be achieved thought technical means only and that the absence of risks is not a possible target when designing new technologies and dealing with their uncertainties. Therefore, the concept proposes to design the delegation of responsibility by focusing on three key aspects: completeness, fairness and effectiveness. Section 4.3 describes the incorporation of this concept in the proposed process.

4.2. The systematic and systemic hazard analysis and management process

4.2.1. Definition of accidents and identification of hazards: step one

The initial step in the process is to define the type of accidents covered in the analysis. For this, we utilize the concept presented in [66]:

> Accident represents an undesired and unplanned event that result in a loss and affectations, including the loss of human life or injury, property damage, equipment damage or environmental pollution, delays in the system operations and repair costs.

The accident identification specifies the accident types which may cause loss and affectations during the operational functioning of the autonomous vessels. In this initial phase, the identification of accidents focuses on determining and describing the most critical accidents which the safety controls and the initial safety management strategy aim to prevent and/or provide a post-accidental response to.

The hazard identification focuses on detecting those hazards which can lead to the defined accidents. The aim is to detect a certain system state or set of conditions, which in a particular set of worst-case conditions in the operational context, lead to the defined accidents [50]. This enables the development of the initial systematic and systemic connection between the accidents and their linked hazards.

4.2.2. Detailed hazard description and initial definition of mitigation actions: step two

This step elaborates detailed descriptions of the hazards, providing a comprehensive argumentation about the relevancy of specific hazards, and a qualitative estimation of their potential severity and type of consequences. The step continues with the identification of the potential causal factors of the hazard. This describes the hazard as a combination of system state and conditions that could influence the effect of the hazard occurrence.

The step concludes with the definition of hazard mitigation actions. These actions represent the initial specifications of the safety controls which are the core element of the initial safety management strategy [67]. The actions are flexible to include diverse forms of mitigation strategies, including the implementation of technology, management procedures, diverse assessments, and testing programs. The aim is to create an extensive and coherent list of mitigation actions. The actions are preliminarily assessed to estimate the complexity and costs of their

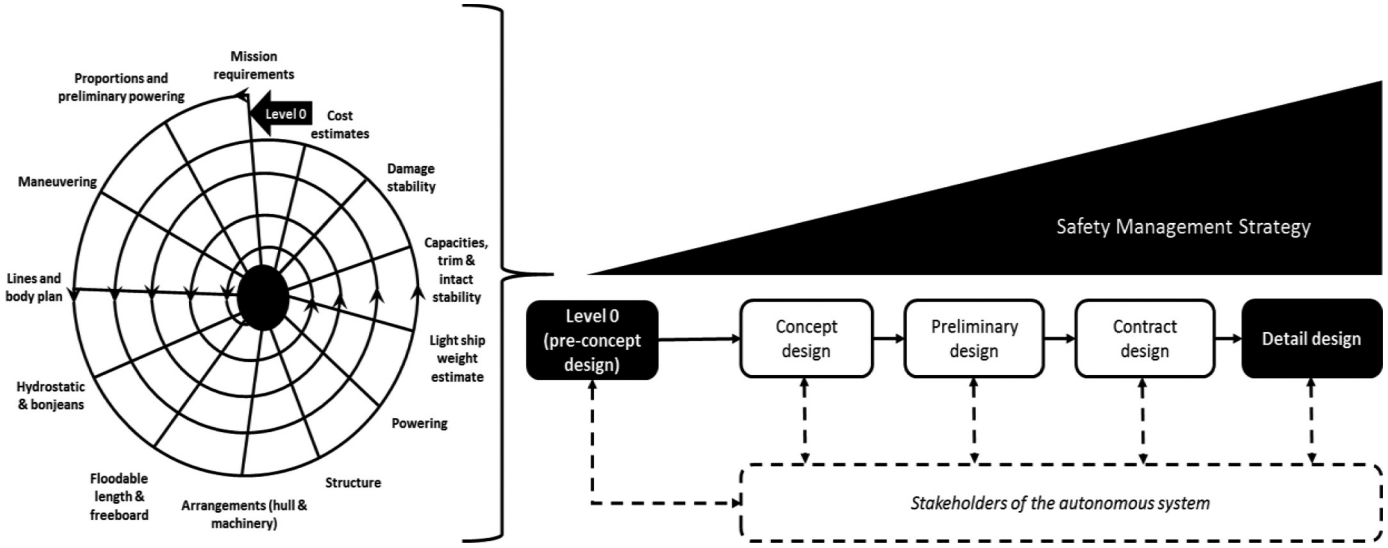


Fig. 2. The ship design spiral [65] and the implementation of the proposed process of hazard analysis before the initial phase in the spiral.

implementation. Finally, each mitigation action has to be categorized based on their intended mitigation control strategy. For this, the process includes the following four categories:

i. The defined mitigation action attempts to reduce the damage if the accident occurs
ii. The defined mitigation action attempts to reduce the likelihood that the hazard results in an accident.
iii. The defined mitigation action attempts to reduce the likelihood that the hazard will occur.
iv. The defined mitigation action attempts to completely eliminate the hazard

4.2.3. Definition of the safety controls: step three

Step three focuses on defining safety controls based on the adopted mitigation actions. The controls focus on providing structured actions to ensure the safety of the operational context under analysis. This task demands the review and prioritization of mitigations actions that will be further developed as the safety controls of the initial safety management strategy. This states if these actions have potentially a significant effect on the mitigation of the hazard. The aim is to assess if the safety controls are objective and relevant to continue their analysis and development into the initial safety management strategy of the autonomous vessel.

4.2.4. Identification of unsafe control actions (UCAs) and redefinition of the safety controls: step four

The identification of UCAs and redefinition of the safety controls are executed by following the process of analysis in the steps of the STPA. The objective is to analyze each hazard and its defined safety controls. The steps of the STPA process are:

– One: For each defined safety control, identify unsafe control actions (UCAs) that could lead to a hazardous state in the system. Hazardous states result from inadequate controls or enforcement of the safety control. These can occur because:
  ○ A control action for safety is not provided or followed
  ○ An unsafe control action is provided
  ○ A safety control is provided too early or too late
  ○ A safety control is stopped too soon or applied too long
– Two: Define why and how UCAs could occur
  ○ Examine the elements included in the functioning of the safety control
  ○ Consider how the safety control could degrade over the time

Moreover, the STPA process is extended to include a redefinition of the function of the safety control. This states how the safety control mitigates the identified UCAs. This provides a clear definition of the actual logic principle behind the functioning of the safety control.

4.2.5. Representation of the initial safety management strategy: step five

The execution of step one to step four produce itemized information that is systemically connected. Step five focuses on representing the main components emerged from the analysis: the hazards, their safety controls, the logic principle of the safety controls, and the link to the accidents that these aim to prevent or respond to. This step provides a detailed representation of the initial safety management strategy of the autonomous vessel.

4.3. The definition of safety roles, tasks and responsibilities

The development of the hazard analysis and management process proposed in this study provides information to define loops among different components in the safety control. This supports the definition of preliminary roles, tasks, and responsibilities in the implementation of the safety control. This task is based on the elements established in the Design for Responsibility concept introduced in [64]. The concept remarks the importance of designing the responsibility for safety in the earliest design phase in order to complement the design of technologies and the final design of the system. The aim is to define who is involved in the implementation and assurance of the controls and define new potential roles and demands for the functioning of the safety controls. The focus is on providing information to implement and maintain the safety controls by ship manufacturers, ship operators, ship service and business providers, authorities, and other system stakeholders. This definition and distribution of responsibility have to be complete, fair and effective. Complete refers to the delegation of at least one actor for a certain task. Fair means a balanced sharing of the responsibility among the actors in the safety controls. Effective refers to the distribution of the responsibility to effectively deal with the risks mitigated by the safety control.

5. Application of the hazard analysis and management process: case study ferry "A" and "B"

5.1. Data of analysis

5.1.1. Accident data and existing frameworks for risk analysis

The main information to identify the most common accidents for the ferries A and B considers the accidents statistics on the European maritime context. For this, the European annual overview of marine casualties and incidents in 2016 is utilized. This report presents that grounding, contacts and collision represent about 50% of the casualties reported, loss of control 26%, damage to ship and equipment 15%, fire/explosion represents 5%, flooding 3% and capsizing/listing less than 1% [68].

This information is certainly representing the trends to the justified foundations in the existing analysis of the risks of the current operational mode of the maritime traffic. These are utilized to create the existing frameworks for maritime risk analysis that are mainly focused on ship collisions and groundings (see references in Section 1). Loss of control and damage to ship and equipment are commonly associated to casualties which may provoke collisions and groundings, and flooding and capsizing are associated to the produced effect after a collision or grounding [23,24,37]. The analysis of these type of casualties, together with the fire/explosions commonly originated in the engine room either from fire in the engine room or engine internal fire/explosion [41,44], represent the main input information to begin the initial step (Step one) of the process proposed together with the consulted experts.

5.1.2. Expert judgment and information processing

In order to apply the proposed process to analyze the hazards of the described Ferry A and B, experts in different industry domains were consulted. Initially, two experts have executed the steps one and two of the process. The personal knowledge and characteristics of these two experts are described in Appendix 1 (Expert A and B).

The execution of steps one and two (see Section 4) produced preliminary information which is further analysed with other experts with specialization and knowledge in relevant fields linked to the initial hazard mitigation actions. These experts participated in four organized workshops to continue and finalize the hazard analysis. Table 1 presents the tasks for the experts in the workshops. Appendix 1 describes the knowledge and characteristics of these experts.

5.2. The outcome produced with the process application

5.2.1. Defined accidents and identified hazards: step one

Step one defined 10 accidents to be considered when determining the initial safety management strategy for ferry A and B. The hazard identification detected 15 hazards which can lead to the occurrence of the 10 accidents. Table 2 presents the list of accidents and the identified hazards. The workshop numbers refer to the safety workshop where the hazards were analysed by the experts (see Appendix 1).

5.2.2. Detailed hazard description and definition of mitigation actions: step two

Step two provides detailed descriptions and the effects of the previously listed hazards, the definitions of the potential causal factors of the hazards, the definition of initial mitigation actions, an initial estimation of the difficulty and cost for their implementation, and the definition of the initial mitigation actions. Table 3 presents the detailed description and the hazard H1 (Object detection sensor error) and its initial mitigation actions. The description of the other hazards can be found in [69].

5.2.3. The defined safety controls: step three

Once the initial hazard mitigation actions are included, the experts assess which of those actions should be further analysed in the process. The experts decided that all the proposed actions are relevant to control the safety of the two vessel concepts under analysis. They agreed that at this level, all the available information is useful to plan the initial safety management strategy. Anyhow, the experts decided to modify the name of some actions in order to make them more purpose specific. Table 4 presents the list of defined safety controls for each hazard, including the mitigation approach of these controls. Safety controls for hazards H4 and H5 are grouped together as the mitigation actions resulted in the step two can be implemented for the mitigation of both hazards, similar integration is done to hazard pairs H12 and H13, and H14 and H15. In the table, each safety control with a certain type of mitigation approach has a code with a sequential number (e.g. SC1). These numbers are grouped in the respective hazard category and mitigation approach, creating safety controls code numbers across the analysis which are used for traceability.

5.2.4. Analysis and redefinition of the safety controls: step four

The analysis of the safety controls provides the identification of Unsafe Control Actions (UCAs) that could lead to the identified hazards. The consulted experts detected UCAs and their potential causes by

Table 1
Tasks description during the arranged safety workshops with experts.

Process Step	Task
One	Define accidents and identified the hazards that can lead to those accidents: • *Are the defined accidents the most relevant for analysis?* • *Is the list of identified hazards complete?*
Two	Review the preliminary hazard analysis by giving answer to the following questions: • *Is the hazard description relevant and accurate?* • *Is the list of the causal factors sensible?* • *Are the mitigation actions relevant?* • *Is there any other mitigation action to be included?* • *Do you agree with the scales given to the cost/difficulty and the categorization of the mitigation control actions?*
Three	Based on the mitigation actions, define which of these should be further analysed and redefined as safety control.
Four	STPA implementation a) Define potential unsafe control actions for each safety control. Considering the following aspects: • The function of the safety control is not provided and/or enough • There is a wrong provision of the function of the safety control • The function of the safety control is provided in wrong time • The function of the safety control is provided for too long or too short b) Define the potential causes of the unsafe controlled actions (UCAs) c) Redefine the safety control and specify how it mitigates the hazard and the defined UCAs
Five	Representation of the initial safety management strategy

Table 2
Define accidents and identified hazards for the context of operation of *ferry A and B,* the table includes the specification of the workshop number where the hazards are analysed.

Accident	Hazards	Workshop number/ hazard analysed
1. Allision with a pier	H1. Object detection sensor error	Workshop 1/ H1; H2 and H6
	H2. Al software failure	Workshop 2/ H12; H13; H14; H15
	H3. Technical fault (e.g. mechanical failure)	Workshop 3/ H3; H4; H5; H7; and H8
	H4. Heavy weather/sea conditions	Workshop 4/ H9; H10; H11
	H5. Strong currents	
	H6. Position reference equipment failure	
2. Collision with a moving object		
2.1 Collision with another vessel	H1. Object detection sensor error	
	H2. Al software failure	
	H3. Technical fault (e.g. mechanical fault)	
2.2 Collision with a small moving target (e.g. canoe, SUP-board, etc.)	H1. Object detection sensor error	
	H2. Al software failure	
	H3. Technical failure (e.g. mechanical failure)	
3. Collision with a fixed object (e.g. buoys, beacons, etc.)	H1. Object detection sensor error	
	H2. Al software failure	
	H3. Technical fault (e.g. mechanical failure)	
	H4. Heavy weather/sea conditions	
	H5. Strong currents	
	H6. Position reference equipment failure	
4. Grounding	H2. AI software failure	
	H3. Technical failure (e.g. mechanical failure)	
	H6. Position reference equipment failure	
	H4. Heavy weather/sea conditions	
	H5. Strong currents	
5. Bottom touch	H2. AI software failure	
	H3. Technical failure (e.g. mechanical failure)	
	H6. Position reference equipment failure	
	H4. Heavy weather/sea conditions	
	H5. Strong currents	
6. Capsizing/ Sinking	H7. Overloading of the vessel	
	H8. Shifting of weights	
	H9. Flooding	
7. Fire on board	H10. Ignition of electrical equipment or wiring	
	H11. Passenger starting a fire	
8. Man over board	H12. Unintended falling overboard	
	H13. Intended jumping overboard	
9. Medical emergency on board	H14. Person(s) getting injured	
	H15. Person(s) medical condition	
10. Medical emergency on pier	H14. Person(s) getting injured	
	H15. Person(s) medical condition	

analysing the safety controls and identifying when UCAs could affect their effective implementation. Once UCAs are detected, the experts redefine the functioning of the safety control. Table 5 exemplifies the implementation of step four with the analysis of Hazard H1 (Object detection sensor error). The description of the analysis and redefinition of the other safety controls can be found in [69].

5.2.5. The representation of the initial safety management strategy for ferry a and B: step five

This step focuses on making a systemic representation of the main components generated from the application of the process. For this, a database is developed in order to present the safety controls for each hazard. The database provides a definition of the logic principle of the safety control which is adapted from the redefinition of the safety controls (see Table 5). The database also presents a description of the actual risks mitigated with the implementation of the controls. Table 6 presents an extraction of the database. The database is available in [69].

The initial safety management strategy for ferries A and B is composed of 73 safety controls. These have different approaches for mitigating the hazards and for preventing and responding to the defined accidents. Table 7 presents the summary of the safety controls included in the safety management strategy. Fig. 3 presents a matrix describing the type of safety controls, including the specification of the hazards that the controls aim to mitigate, the mitigation approach of the controls, and a grouping of the safety controls into the accidents that these attempt to prevent or respond to.

5.3. Definition of safety roles, tasks and responsibilities

The information produced in the application of the proposed process is utilized to exemplify how the potential definition of safety roles, tasks, and responsibilities can be done. Fig. 4 presents an example of the definition of roles, tasks, and responsibilities for the safety control sensor system and equipment redundancy (SC 1).

The figure presents an initial structure for managing the functioning of the safety control. It initially specifies who is the main responsible for ensuring the functioning of the safety control. It also points out other potential partners sharing this responsibility. The responsibility is clearly given to at least one actor. This identifies the vessel manufacturer as the main responsible for the bidding process in the acquisition of the sensor system and equipment redundancy. The other responsible stakeholders include the installation and maintenance providers and auditor (e.g. class society), these two share also the responsibility of ensuring the proper functioning of the sensor system and equipment redundancy.

Table 3
Detailed description and initial mitigation actions for hazard H1 (Object detection sensor error).

Hazard	H1. Object detection sensor error		
Hazard effect/description	*Provide extra details regarding the designated severity rating* In case of object detection sensor error, the information about objects around the vessel is not reliable and thus the vessel may not be able to navigate safely and avoid collisions with moving objects according to the rules of the road or collisions with fixed objects. This hazard may not affect the ship operation significantly in most cases, but in a more severe scenario, the hazard can have a negative impact on people, property, and environment. It can result in injuries, the loss of human life, severe damage or loss of property (own and others property) and environmental effects such as oil spills or other damage of a sensitive waterway or sea area.		
Causal factors	*Describe the hazard as system state. What conditions could influence the effect of the hazard occurrence?* - Loss of power - Equipment malfunction - Dirt - Icing - Overheating - Equipment interference - Inappropriate maintenance - Incorrect sensor set and/or positioning of the sensors - Targets impossible to detect - Corrupted readings - Complete equipment failure		
Mitigation actions		Cost/Difficulty	*Approach (1–4)*
	- Sensor system redundancy and diversity	High	*
	- UPS (Uninterrupted Power Source)	Low	4
	- Appropriate heating, cooling and cleaning systems	Medium	3
	- Thorough commissioning of equipment set	Medium	3
	- Appropriate and continuous maintenance program	Low	4/3
	- Continuing system diagnosis and proof testing	Low	3
	- Autonomous Integrity monitoring	Low	3
**Mitigation approach*	*Level*	*Detailed description*	
	4	Attempt to completely eliminate the hazard	
	3	Attempt to reduce the likelihood that the hazard will occur	
	2	Attempt to reduce the likelihood that the hazard results in an accident	
	1	Attempt to reduce the damage if the accident occurs	

6. Discussion

6.1. The purpose of the proposed process for hazard analysis and management

The implementation of the process produces initial itemized information which can guide the initial design process of an autonomous vessel and its entire operational system. The process is based on a system engineering approach which focused on supporting the design and management of complex systems and maintaining it functional during its complete operational life [70]. The aim is to initiate the design of safety in the earliest conceptual design phase for engineering a safer system [50]. The proposed process represents a truly systemic and systematic approach which is capable to analyse accidents and hazards in different contextual scenarios. Moreover, this approach is capable of formulating safety controls to prevent and or to react to those accidents and hazards.

The process adopts the foundations for ship design established in the ship design spiral and it anticipates other operational issues. The spiral represents a generally accepted approach in ship design projects [71]. The components of the spiral are developed in four different phases with the aim of ensuring an efficient culmination of the ship construction project. However, the incorporation of the elements focused on the safety management of the ship begins until the actual culmination of the concept design phase of the spiral. This provokes the creation of a safety management strategy which is ruled and decided by the view of shipbuilders, designers and operators, creating a limited scope which cannot include other key safety issues that influence the proper functioning of the ship and its entire operational system.

With the implementation of the proposed hazard analysis process at such called level 0 (pre-concept design), designers and builders can be early informed about safety hazards and potential ways to control them. This represents an initial safety management strategy which considers the views of different stakeholders of the operating system of an autonomous vessel. This represents an important initial support to the development of the elements and phases included in the design spiral and other operational aspects of the autonomous vessel and its autonomous system. This strategy provides the description of safety controls influencing the following phases in the design process. The 73 controls defined in this study have an effect on the four following design phases, influencing the architectural and engineering characteristic defined in the concept deign, the detailed ship characteristics for ensuring the performance of the vessel defined in the preliminary design, the final general arrangements in the contract design, and the final working plans for the detailed design.

6.2. The implementation of the proposed process for hazard analysis

6.2.1. Implementation of step one

The implementation of the process focuses on the definition of initial safety management strategy which influences the design of an autonomous vessel. This strategy should evolve during the different design phases. For this, the step one defines the main accidents that may result in damages and injuries during the operations of the autonomous vessel and its entire operational system. In the implementation of this step for the analysis of the described *ferry A and B*, ten accidents have been defined. Linked to these accidents, fifteen hazards that in combination with a worst-case scenario can lead to one or more of the contemplated accidents have been identified. These hazards represent the obvious initial states of the system which endanger the mission and operation of the vessel.

6.2.2. Implementation of step two

This step provides a detailed description of the identified hazards,

Table 4
The defined safety controls for the identified and analysed hazards.

Mitigation approach*	Code	Safety controls
H1. Object detection sensor error		
4	SC 1	Sensor system redundancy and diversity
3	SC 1	UPS (Uninterrupted Power Source)
	SC 2	Appropriate heating, cooling, and cleaning systems
	SC 3	Thorough commissioning of equipment set
	SC 4	Appropriate and continuous on board maintenance program
	SC 5	Continuing system diagnosis and proof testing
2	SC 1	Autonomous Integrity monitoring
H2. AI software failure		
4	SC 2	Thorough planning, testing and commissioning of AI software
	SC 3	Robust system design
3	SC 6	Computer and software redundancy
	SC 1	UPS (Uninterrupted Power Source)
	SC 7	Appropriate cooling for computers
	SC 4	Appropriate and continuous on board maintenance programs
	SC 8	Appropriate system (software) design and maintenance processes
H3. Technical fault (e.g. mechanical failure)		
4	SC 4	Redundancy of critical systems
	SC 5	Thorough planning, testing and commissioning of all technical systems
3	SC 9	Planned and predictive maintenance programs
	SC 10	Remote monitoring and fault detection of the technical systems
H4. Heavy weather/sea conditions		
H5. Strong currents		
4	SC 6	Correctly set and followed operational limits
3	SC 11	Weather routing and constant weather and sea state monitoring
	SC 12	Vessel equipped with adequate environmental sensors for detecting local conditions
2	SC 2	Keeping the vessel steady against the wind and waves or heading to an emergency harbour or anchorage
	SC 3	Knowledge of local currents and other local environmental conditions
	SC 4	Constant monitoring of the currents and adjusting the steering accordingly
	SC5	Constant monitoring and predictions of vessels capability
H6. Position reference equipment failure		
4	SC 7	Equipment (sensor) redundancy
	SC 8	Thorough installation and commissioning of equipment set
3	SC 13	Satellite positioning equipment with jamming detection and/or anti-jamming function
	SC 1	UPS (Uninterrupted Power Source)
	SC 14	Appropriate heating, cooling and cleaning for local position reference systems
	SC 15	Appropriate and continuous on board maintenance programs
	SC 16	Continuing system diagnosis and proof testing
2	SC 6	Combination of local and satellite position reference systems
	SC 7	Autonomous Integrity monitoring
H7. Overloading of the vessel		
4	SC 9	Automated door type passenger gates which do not allow more than maximum number of passengers on board
	SC 10	Clear rules, weighing and monitoring of the cargo taken on board
	SC 11	In case of adding permanent weights on board stability calculations and tests to be redone
	SC 12	Automatic continuous monitoring of the vessel's stability (draft, trim, list and GM), vessel programmed not to leave pier if over the limits.
H8. Shifting of weights		
4	SC 13	Firefighting systems that use very little water or no water at all
	SC 14	Anti-heeling system
3	SC 17	Passenger instructions on quay and on board
	SC 18	Vessel design
2	SC 8	Remote monitoring center monitors vessels stability and instructs people by voice if necessary
H9. Flooding		
4	SC 15	Double hull and compartments
	SC 16	Well planned and built piping system
3	SC 19	Fire extinguishing systems that use very little water or no water at all
	SC 20	Good drainage system on the deck
2	SC 9	Automatic monitoring system for tanks, pipes and cofferdams
	SC 10	Effective bilge pumps
H10. Ignition of electrical equipment and wiring		
4	SC 17	Circuit breakers and fault current protection
3	SC 21	Thorough planning and commissioning of electrical equipment and wiring
	SC 22	Appropriate cooling and heating for electrical systems
	SC 23	Preventive maintenance programs
1	SC 1	Automatic fire extinguishing systems inside electrical cabinets
	SC 2	Automatic fire detection, alarm and extinguishing systems in engine spaces

(*continued on next page*)

Table 4 (*continued*)

Mitigation approach*	Code	Safety controls
H11. Passenger starting a fire		
3	SC 24	No smoking signs
	SC 25	Use of inflammable and fire resistant materials in passenger spaces
2	SC 11	Smoke detectors and automatic fire extinguishing system in passenger spaces
	SC 12	Video surveillance system**
	SC 13	Both automatic and manual fire alarm systems on the passenger spaces with direct access to remote monitoring centr
1	SC 3	Possibility for the passengers to extinguish a fire
H12. Unintended falling overboard		
H13. Intended jumping overboard		
4	SC 18	Vessel design with closed and "unclimbable" reeling i.e. transparent inward curved plastic.
	SC 19	Vessel design with automated sliding door type passenger gates which don't open unless the vessel is firmly in pier
3	SC 26	Video surveillance system**
		Passenger instructions on quay and on board for mob situation
1	SC 4	Manual alarm systems on the passenger spaces and piers with direct access to remote monitoring center and rescue center
	SC 5	Remote monitoring center to calm down and instruct people by voice after the alarm
	SC 6	Vessel to stop automatically in case of a man over board alarm
	SC 7	Well planned and rehearsed procedure, suitable equipment and clear roles between authorities for recovering a person from the water
	SC 8	Possibility for other passengers to assist or recover a person from the water
	SC 9	Automatic warning message to be sent to the surrounding vessels
H14. Person(s) getting injured		
H15. Person(s) medical condition		
4	SC 20	Unobstructed access and non-slippery floor materials in piers and the vessel
3	SC 27	Good lighting and air conditioning
	SC 26	Video surveillance system**
1	SC 9	Manual alarm systems on the passenger spaces and piers with direct access to remote monitoring center and rescue center
	SC 10	Vessel re-routes to the closest medical evacuation pier and informs her location to the rescue center if medical assistance is needed
	SC 11	Passenger instructions on piers and on board for medical emergencies
	SC 5	Remote monitoring center to calm down and instruct people by voice after the alarm
	SC 12	Well planned and rehearsed procedure for medical evacuation
	SC 13	Possibility for other passengers to give first aid to an injured person
*Mitigation approach	*Level*	*Detailed description*
	4	Attempt to completely eliminate the hazard
	3	Attempt to reduce the likelihood that the hazard will occur
	2	Attempt to reduce the likelihood that the hazard results in an accident
	1	Attempt to reduce the damage if the accident occurs

**Safety control which can have two mitigation approaches*

including their potential effect on different components of the vessels and its operating system. This description incorporates a justification of why the hazard analysis is relevant and the initial estimation of its severity and its consequences. Moreover, potential causal factors are also identified and analysed in this step. These are based on the view of different safety management stakeholders of the system, providing a systematic and systemic identification of factors which can emergence from different components attached to the functioning of the autonomous vessel. The step concludes with the definition of hazard mitigation actions. These actions are the point of reference regarding the approach to be followed in the initial safety management strategy of the vessels. The purpose of the actions and the preliminary evaluation of their feasibility is fundamental to assess their potential for further development.

6.2.3. Implementation of step three

This step transforms the selected hazard mitigations actions into defined safety controls. In this step, the implementation of the process has evidenced the importance of keeping all valuable information produced with the initial actions. The implementation of this step, together with the support of the consulted experts, demonstrated a proactive approach to continue the development of these actions and transform these into the safety controls of the initial safety management strategy. This approach provides valuable information for designers, manufacturers, operators and other decision makers.

6.2.4. Implementation of step four

This step executes a final review of the functioning of the safety controls. It assesses the function of the safety controls to detect unsafe control actions that provoke the existence of the identified hazards. This identification is strengthened by incorporating the reasoning behind the existence of those unsafe control actions. This supports the development of more concrete descriptions about what the safety controls should do.

6.2.5. Implementation of step five

The implementation of the process to ensure the safety of the ferries A and B produced 73 safety controls. The 37% of these controls focuses on implementing actions to reduce the likelihood of the hazard occurrence. The 27% of the controls focuses on implementing actions which attempt to eliminate the hazard. The 18% of the safety controls focuses on implementing actions to reduce the likelihood that the hazard will result in an accident. The 18% of the controls focuses on implementing actions to reduce the damage if the accident occurs.

The safety controls and their included control logic principle provide an itemized safety management strategy which presents essential information in the earliest design phase. This supports decision makers to elaborate plans, conceptual designs, ship arrangements, and setting of other crucial elements for designing and building the autonomous vessels.

6.3. Defining safety roles, task and responsibilities

The definition of the safety controls and their logic principle provide information to make an initial estimation of how the roles and tasks for the functioning of the controls can be defined, making a preliminary

Table 5
Implementation of step four (STPA process) for analysis and redefinition of the safety controls in hazard H1 (Object detection sensor failure).

Safety controls (mitigation approach)
SC 1 (4) Sensor system redundancy and diversity
SC 1 (3) UPS (Uninterrupted Power Source)
SC 2 (3) Appropriate heating, cooling, and cleaning systems
SC 3 (3) Thorough commissioning of equipment set
SC 4 (3) Appropriate and continuous on board maintenance program
SC 5 (3) Continuing system diagnosis and proof testing
SC 1 (2) Autonomous Integrity monitoring
Detecting potentially Unsafe Controlled Actions (UCAs) and redefining the safety control
SC 1 (4). Sensor system redundancy and diversity
UCA 1. Sensor does not function properly and there is no other sensor available
Potential causes
- Lack of economic resources
UCA 2. Equipment chosen to provide the redundancy are not suitable
Potential causes
- Lack of economic resources
- Lack of knowledge of sensors characteristics when planning the equipment set needed
UCA 3. Sensor failure is not detected
Potential causes
- Not enough coverage with the diagnosis
UCA 4. External or common cause failures takes several equipment down at the same time
Potential causes
- Inappropriate system design
SC 1 (3). UPS (Uninterrupted Power Source)
UCA 1. There is a disturbance in vessel's power system and the equipment is not backed up with UPS
Potential causes
- Lack of economic resources
- Lack of understanding of the importance of the UPS
UCA 2. The UPS does not work
Potential causes
- UPS is not charged
- UPS is not connected correctly
- UPS is broken
UCA 3. The UPS takes too long to switch on
Potential causes
- Errors in UPS function
UCA 4. The capacity of the UPS is not sufficient to provide power for the equipment as long as needed or the capacity in terms of power and/or energy of the UPS is exceeded
Potential causes
- The disturbance lasts longer than expected in the planning stage
- Wrong type of UPS
Redefining of the safety control
UPS (Uninterrupted Power Source):
- If there is a disturbance in the vessel power system the UPS can temporarily provide power for the critical equipment
- When the UPS setup is planned, installed and maintained properly, the user can count on a reliable backup system
SC 2 (3). Appropriate heating, cooling and cleaning systems
Equipment is not able to function properly in winter conditions
Potential causes
- Equipment does not have heating function
- Extremely low temperatures
- Icing
Equipment is not able to function properly due to the high temperature
Potential causes
- Equipment does not have cooling function
- Extremely high temperatures
- The systems are located close to high temperature sources
Equipment lens is dirty
Potential causes
- Sea water sprays
- Bird faeces
Condensation inside equipment
Potential causes
- Leaking
- Temperature changes
- Fault on the equipment design
- Humid climate
- Location on-board
Redefining of the safety control
Appropriate heating, cooling and cleaning systems:
- By applying sensors with proper heating and/or cooling systems it can be ensured that they function properly in all operating conditions
- By applying sensors with proper automatic cleaning systems it can be ensured that they function properly outdoors
SC 3 (3). Thorough commissioning of equipment set
UCA 1. The equipment set has not been properly tested or not tested at all before operation
Potential causes
- Lack of economic resources

(*continued on next page*)

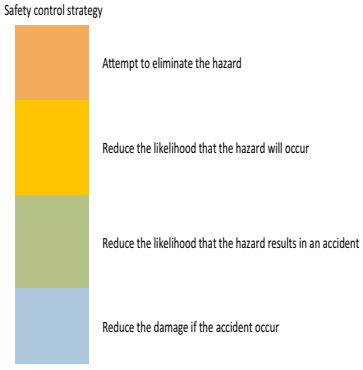
Table 5 (*continued*)

Safety controls (mitigation approach)
- Test plan is not appropriate - Lack of time *Redefining of the safety control* Thorough commissioning of equipment set: When the equipment set is thoroughly tested and certified (preferably by an independent body) it ensures that the equipment function properly, are compatible and the operation can be run safely. **SC 4 (3). Appropriate and continuous on board maintenance program** UCA 1. There is no on board maintenance program *Potential causes* - Lack of economic resources - Lack of understanding of the importance of the maintenance program UCA 2. The maintenance program does not cover the necessary elements and the life cycle of the hardware. *Potential causes* - Lack of competence UCA 3. The maintenance program is not followed *Potential causes* - Lack of time (work overload) - Lack of economic resources - Lack of understanding of the importance of the maintenance program UCA 4. Maintenance is not done properly *Potential causes* - Lack of commitment - Lack of competence - Human error or mistake - Lack of economic resources *Redefining of the safety control* Appropriate and continuous maintenance program: - By implementing an on board maintenance program it can be ensured that all critical systems remain functional at all times - A well planned maintenance program covers all necessary areas on board and it is adjusted separately for each vessel - Maintenance done timely and accordingly to the program by competent personnel ensures the smooth operation of the sensors **SC 5 (3). Continuing system diagnosis and proof testing** UCA 1. There is no continuing system diagnosis and proof testing Potential Causes - Lack of economic resources - Lack of planning - It cannot be performed due to the effects on operation UCA 2. The continuing system diagnosis and proof testing do not cover all necessary functions Potential causes - Lack of economic resources - Lack of planning - Test cannot be performed due to the effects on operation UCA 3. The test is not able to recognize problems Potential causes - Wrong test design - Changes in the system *Redefining of the safety control:* Continuing system diagnosis and proof testing: - Continuing system diagnosis and regular proof testing ensures that the system functions as it should - Test design should be planned carefully and updated after changes in the system in order to cover all the necessary functions and recognize potential problems - Possible effect on the operation should be taken into account in planning **SC 1 (2) Autonomous Integrity monitoring** UCA 1. There is no integrity monitoring Potential causes - Lack of economic resources - Lack of planning - Lack of understanding UCA 2. Integrity monitoring gives wrong information Potential Causes - Common cause failure - Wrong design - Changes in the system *Redefining of the safety control:* Autonomous Integrity monitoring: - Well designed and up to date integrity monitoring system ensures that the data has not been damaged or manipulated

delegation of responsibilities among the stakeholders involved in the management of the safety controls. This information has to be transmitted and further processed in the subsequent phases of the vessel design and construction. The information has to evolve to obtain a clear definition of safety roles and responsibility in the functioning of the autonomous vessels and its entire operational ecosystem. Based on the approach to Design for Responsibility proposed in [64], this defined responsibility has to be fairly distributed among the actors involved. It has to be flexible to allow changes on the defined responsibilities in order to dynamically update and improve this delegation. Finally, it has to constantly foster the virtues and capabilities of the defined responsible.

Table 6
Extraction (H1 Object detection sensor error) of the database created to present the logic principle and the risks mitigated by the safety controls.

Hazard	Safety Control (SC)	Control logic principle	Risks mitigated
1	1. Object detection sensor error		
1. Object detection sensor error	1. Sensor system redundancy and diversity	If one sensor fails the redundancy ensures there is going to be another sensor functioning. The quipment chosen to provide the redundancy has to be the correct in order to provide the user with the required information at all times	> Innapropriate functioning and availability of the sensor > Correctness on the selection of redundancy equipment on time detection sensor failure > External failures affecting the functioning of the sensor
	1. UPS (Uninterrupted Power Source)	If there is a disturbance in the vessel power system the UPS can temporarily provide power for the critical equipment. When the UPS setup is planned, installed and maintained properly, the user can count on a reliable backup system	> There is a disturbance in vessel's power system and the equipment is not backed up with UPS > The UPS does not work or take too long to switch on > The capacity of the UPS is not sufficient to provide power for the equipment
	2. Appropriate heating, cooling and cleaning systems	By applying sensors with proper heating and/or cooling systems it can be ensured that they function properly in all operating conditions. Proper automatic cleaning systems can ensure the appropriate function of the sensors outdoors	> Equipment is not able to function properly in winter conditions > Equipment is not able to function properly due to the high temperature > Equipment lens is dirty > Condensation inside equipment
	3. Thorough commissioning of equipment set	When the equipment set is thoroughly tested and certified (preferably by an independent body) it ensures that the equipment functions properly, is compatible and the operation can be run safely.	> The equipment set has not been properly tested or not tested at all before operation
	4. Appropriate and continuous on board maintenance programs	By implementing a maintenance program it can be ensured that all critical systems remain functional at all times. A well planned maintenance program covers all necessary areas on board and it is adjusted separately for each vessel. Maintenance done timely and accordingly to the program by competent personnel ensures the smooth operation of the sensors.	> There is no maintenance program > The maintenance program does not cover the necessary elements and the life cycle of the hardware > The maintenance program is not followed or it is wrongly applied
	5. Continuing system diagnosis and proof testing	Continuing system diagnosis and regular proof testing ensures that the system functions as it should. Test design should be planned carefully and updated after changes in the system in order to cover all the necessary functions and recognize potential problems. Possible effect on the operation should be taken into account in planning	> There is not continuing system diagnosis and proof testing > The continuing system diagnosis and proof testing does not cover all necessary functions > The test is not able to recognize problems
	1. Autonomous integrity monitoring	Well designed and up to date integrity monitoring system ensures that the data has not been damaged or manipulated	> There is not integrity monitoring > Integrity monitoring gives wrong information



6.4. Limitations

6.4.1. Process limitations

The main process limitation is linked to the decision about to what level of details the analysis needs to be concluded [72]. This particularly refers to step four of the process where unsafe control actions need to be identified. This limitation influences the development of the expert consultations. The process demands a deep analysis of the potential unsafe control actions. Thus, the implementation of this step is challenging and time-consuming.

6.4.2. Results limitations

Linked to the referred process limitation, the results are limited to set an initial safety management strategy focused on the mitigation, prevention, and response to 10 accidents and 15 hazards. Initially, the incorrect interpretation or execution of the international regulations for preventing collisions at sea (COLREGs) was listed as one hazard. However, as the hazard is actually composed of different elements and complex interactions, the experts mentioned that implementation of the COLREGs in autonomous vessels has to be analysed carefully and separately.

Table 7
The safety controls of the initial safety management strategy for *ferry A and B*.

Safety control mitigation approach	Safety controls defined
Attempt to completely eliminate the hazard	20
Attempt to reduce the likelihood that the hazard will occur	27
Attempt to reduce the likelihood that the hazard results in an accident	13
Attempt to reduce the damage if the accident occurs	13

Safety Control (SC)	Accident 1	2,1	2,2	3	4	5	6	7	8	9	10
1	H1 H1 H1	H1 H1 H1	H1 H1 H1	H1 H1 H1	H1	H1		H10			
2	H2 H1 H4	H2 H1	H2 H1	H2 H1 H4	H2 H4	H2 H4		H10			
3	H2 H1 H4	H2 H1	H2 H1	H2 H1 H4	H2 H4	H2 H4		H11			
4	H3 H1 H4	H3 H1	H3 H1	H3 H1 H4	H3 H4	H3 H4			H12	H12	H12
5	H3 H1 H4	H3 H1	H3 H1	H3 H1 H4	H3 H4	H3 H4			H12	H12	H12
6	H4 H2 H4	H2	H2	H4 H2 H4	H4 H2 H4	H4 H2 H4	H8		H12		
7	H4 H2 H4	H2	H2	H4 H2 H4	H4 H2 H4	H4 H2 H4	H9		H12		
8	H4 H2	H2	H2	H4 H2	H4 H2	H4 H2	H7 H9		H12		
9	H3	H3	H3	H3	H3	H3	H7	H11	H12		
10	H3	H3	H3	H3	H3	H3	H7	H11		H14	H14
11	H4			H4	H4	H4	H7	H11		H14	H14
12	H4			H4	H4	H4	H8			H14	H14
13	H6			H6	H6	H6	H8			H14	H14
14	H6			H6	H6	H6	H9				
15	H6			H6	H6	H6	H9				
16	H6			H6	H6	H6	H8	H10			
17							H8		H12		
18							H9		H12		
19							H9			H14	H14
20								H10			
21								H10			
22								H10			
23								H11			
24								H11			
25									H12	H12	H12
26									H12		
27										H14	H14
Total SC	31	16	16	31	25	25	15	12	10	9	9

SC control strategy:

- Attempt to eliminate the hazard
- Reduce the likelihood that the hazard will occur
- Reduce the likelihood that the hazard results in an accident
- Reduce the damage if the accident occur

Fig. 3. The matrix of the safety controls included in the initial safety management strategy for *ferry A and B,* the matrix describes the type of control utilized for the prevention and response to the defined accidents. Accidents and Hazards presented in Table 2 and Safety Controls in Table 4.

The scope covered with the defined safety controls represents only an initial reference for the further development of the strategy. Thus, no claims are made about the presented accidents and hazards being the only possible ones. The main intention is to set the initial structure of an analysis which has to evolve during the phases of the vessel design and construction. This represents the need for continuing the hazard and risk analysis during the implementation of the subsequent design phases. This analysis has to make a consistent review of the cost and difficulty of the selected safety controls, the current rating is subjective to an analysis based on expert judgement. This requires a validation process that includes a sensitivity analysis of the preliminary rating.

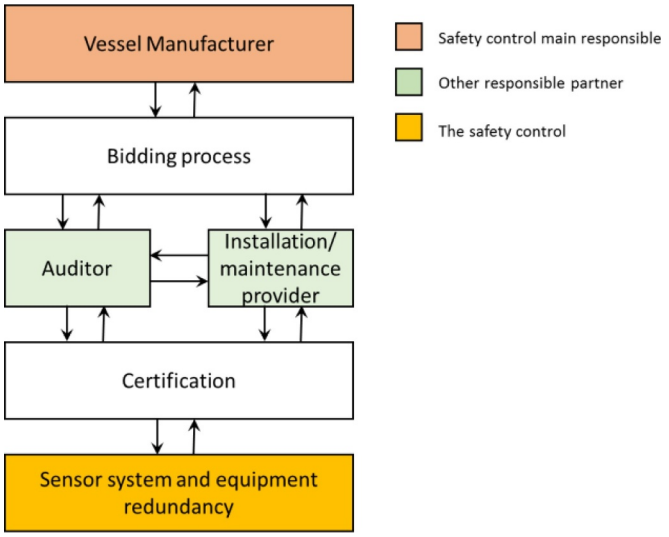


Fig. 4. The initial structure for defining safety roles, tasks, and responsibilities in the implementation of safety control SC 1 “Sensor system and equipment redundancy”.

6.5. Future work

The work to continue the development of the safety management strategy focuses on the validation of the obtained results and a clear representation about how the strategy could differently evolve in ferry A and ferry B. The aim is to assess the relevancy of the strategy in both cases to select and further develop the safety controls in the actual concept design phase. The development of the strategy has to be executed by the actual stakeholders responsible for designing, constructing and operating the autonomous vessel and the other components of its operating system. The participation of these stakeholders is essential as information has to be generated in order to make an evaluation of the analysed aspects of each safety control. This includes the definition of the technical characteristics of the controls (based on the defined logic principle) and a sensitivity analysis of the rating allocated to the cost and difficulty of the controls.

The proposed hazard analysis and management process is applied in the context of the so-called design spiral. Specifically, the process is applied as a part of level 0 (pre-concept design). The aim to define a safety management strategy already as a part of the definition of the mission requirements. However, the application of the proposed process could be extended to the context of some other wider design process such as the goal- and system-based approach proposed in [73] and the extension of such approach presented in [74]. In this design process model, an individual vessel is treated as a component of a wider maritime system. This creates the interaction of different concept designs which are split into certain sub-system categories that are designed in terms of a set of parameter values determined to meet certain goals and functional requirements. This model executes a performance assessment which can select the most cost-efficient alternative. This represents a link to a subsequent stage where the safety management

strategy ensures the efficiency of the proposed safety controls. The linking and extending of the proposed process in this study to the above mentioned model will consume more time and resources, but it would likely result in a more systematic and efficient solution than using the traditional design spiral. This approach can enable the linking of the safety controls with other essential constraints such as environmental pollution controls.

7. Conclusions

This study presents a systemic and systematic hazard analysis and management process for the concept design phase of an autonomous vessel within its operative context. The process is composed of five different steps to elaborate an analysis of hazards and to define safety controls for mitigating and preventing the identified hazards. These controls are the basis of the initial safety management strategy of the autonomous vessels and its operating system.

The implementation of the process seems to be proficient for analysing hazards and proposing safety controls with a systematic and systemic approach that covers the operational context of the autonomous vessel. The application of the process to analyze two concepts of autonomous ferries operating in urban waterways in Finland results in the analysis of 10 defined accidents and 15 identified hazards. The analysis concludes with the definition of an initial safety management strategy composed of 73 safety controls. This initial safety management strategy provides itemized information that is relevant to plan, design and construct the autonomous vessel and its entire operational system.

The definition of the safety management strategy and its incorporated safety controls facilitates the initial identification of new safety tasks and a systematic delegation of responsibilities for management of safety of the vessels. This promotes the involvement of different key stakeholders in the management of safety for the autonomous vessels and their operating system.

Acknowledgments

The work presented in this article is part of the research project “Smart City Ferries” (ÄLYVESI) and the Design for Value (D4 Value) program. ÄLYVESI is funded by the European Regional Development Fund (ERDF). Additional financiers are Finnish Transport Safety Agency and the cities of Helsinki and Espoo. The D4 Value program is partially funded by the Finnish Funding Agency for Innovation (TEKES). The contributions by the third author are in part supported by the project ‘Safe Navigation and Environmental Protection’, funded by the Ocean Frontier Institute. The authors want to thank all the experts who participated in the workshops and the three anonymous reviewers, whose constructive comments have helped to improve a previous version of this article.

Supplementary materials

Supplementary material associated with this article can be found, in the online version, at doi:10.1016/j.ress.2019.106584.

Appendix

Appendix 1
The characteristics of the experts who participated in the safety workshops.

Workshop number	Consulted expert
1	A) A master mariner and a master of marine technology with over 14 years of seagoing experience as marine officer, and about 5 years of experience from maritime administration as a senior inspector and a marine safety investigator. B) A senior researcher with about 4 years of practical experience in quality and safety management of maritime traffic and port logistics, and over 5 years of experience in the research of safety and risk management practices implemented in the maritime industry. C) A shipbuilding engineer with over 14 years of experience in ship design and technical management in maritime industry and about six years of experience from the classification societies. D) A design and production engineer with over six years of experience as project manager and director in smart mobility and transport automation projects. E) A captain with ten years of seagoing experience as a marine officer and shipmaster, and 20 years of experience in the maritime simulator training and simulator environment development in a maritime college. F) A doctor of technology specialized in control engineering, automation and system identification. The expert has over six years of experience in the marine electric and automation industry and is currently a manager of intelligent shipping in one of the a leading technology companies in the field. G) A doctor of philosophy specialized in positioning technologies. The expert has over ten years of experience in the development of GNNS products and over four years of experience in researching geodesy, geoinformatics, navigation, remote sensing and spatial data infrastructure. H) A software engineer with over ten years of experience as designer of software and algorithms for automation and energy domains. Specialized in critical and high-reliability systems.
2	A) A master mariner and a master of marine technology with over 14 years of seagoing experience as marine officer, and about 5 years of experience from maritime administration as senior inspector and marine safety investigator B) A senior researcher with about 4 years of practical experience in quality and safety management of maritime traffic and port logistics, and over 5 years of experience in the research of safety and risk management practices implemented in the maritime industry. I) A naval architect with 14 years of experience in the ship design and construction, and works currently as a managing director of a shipyard. The expert has also over 9 years of technical ship management experience from a shipping company. J) A coast guard officer with a total of 28 years of experience of maritime search and rescue work, of which seven years as a search and rescue mission coordinator. K) A fire engineer with about ten years of rescue service experience specialized in fire inspections and contingency planning in chemical sites and harbours. Currently the expert works as a leading fire inspector in charge of developing control activities for the South West Finland rescue area. L) A ship owner with over 20 years of experience in ship management and practical ship operations, and 12 years of experience as a ferry Captain in the Finnish archipelago. The expert acts also a safety manager (DPA) of a shipping company. M) A city risk manager with a master's degree in engineering. This expert is in charge of the safety and security strategies and their implementation in one the largest cities of Finland. N) A master mariner with five years of seagoing experience as a marine officer and 11 years of experience as a survival instructor in maritime safety training center. The expert has also experience in development and evaluation of the marine lifesaving equipment.
3	A) A master mariner and a master of marine technology with over 14 years of seagoing experience as marine officer, and about 5 years of experience from maritime administration as senior inspector and marine safety investigator B) A senior researcher with about 4 years of practical experience in quality and safety management of maritime traffic and port logistics, and over 5 years of

(continued on next page)

Appendix 1 (*continued*)

Workshop number	Consulted expert
	experience in the research of safety and risk management practices implemented in the maritime industry. C) A shipbuilding engineer with over 14 years of experience in ship design and technical management in maritime industry and about six years of experience from the classification societies. F) A doctor of technology specialized in control engineering, automation and system identification. The expert has over six years of experience in the marine electric and automation industry and is currently a manager of intelligent shipping in one of the a leading technology companies in the field. O) A master mariner with three years of seagoing experience as a marine officer and 10 years of experience as a simulator instructor and a training manager in a maritime college. P) A master mariner with five years of experience in developing maritime on-board solutions. The expert currently works as a CEO of a company focusing on maritime IT/ICT/IoT/telematics and safety systems. Q) A naval architect with over five years of experience in the implementation of maritime safety regulations for ship design and construction. The expert has also over 3 years of experience in researching the interaction between sea ice and ship structures. R) A Chief engineer with 18 years of seagoing experience as a marine engineer. The expert acts also a safety manager (DPA) in a shipping company specialized in operating public transportation routes in a city area.
4	A) A master mariner and a master of marine technology with over 14 years of seagoing experience as marine officer, and about 5 years of experience from maritime administration as senior inspector and marine safety investigator B) A senior researcher with about 4 years of practical experience in quality and safety management of maritime traffic and port logistics, and over 5 years of experience in the research of safety and risk management practices implemented in the maritime industry. I) A naval architect with 14 years of experience in the ship design and construction, and works currently as a managing director of a shipyard. The expert has also over 9 years of technical ship management experience from a shipping company J) A coast guard officer with a total of 28 years of experience of maritime search and rescue work, of which seven years of experience as a search and rescue mission coordinator. K) A fire engineer with about ten years of rescue service experience specialized in fire inspections and contingency planning in chemical sites and harbours. Currently the expert works as a leading fire inspector in charge of developing control activities for the South West Finland rescue area. S) A mechanical engineer with 7 years of experience in fire safety consulting, maintenance, planning and installation of fire-extinguishing systems. T) A Marine and electrical engineer with about fifteen years of seagoing experience. The expert has also experience from marine switchboard planning, and power plant electrical network distribution operation and maintenance.

References

[1] Kretschmann L, Rødseth Ø.J., Tjora Å., Fuller B.S., Noble H., Horahan J.Maritime unmanned navigation through intelligence in networks – qualitative assessment. 2015.

[2] Levander O. Ship intelligence – a new era in shipping. Smart Sh Technol, London. RINA 2016;2016:25–32.

[3] Vermesan O, Friess P. Internet of things: converging technologies for smart environments and integrated ecosystems. River Publishers; 2013.

[4] Teivainen A. Rolls-Royce to set up R&D centre in Turku. Finland: Helsinki Times; 2017. March.

[5] Rødseth OJ, Burmeister HC. Risk assessment for an unmanned merchant Ship. Transnav. Int J Marine Navig Safety Sea Transpn 2015;9(3):357–64.

[6] Jalonen R, Tuominen R, Wahlström M. Safety of unmanned ships - safe shipping with autonomous and remote controlled ships. Aalto University; 2017 https://aaltodoc.aalto.fi:443/handle/123456789/2806.

[7] Wróbel K, Krata P, Montewka J, Hinz T. Towards the development of a risk model for unmanned vessels design and operations. TransNav 2016;10(2). nr http://yadda.icm.edu.pl/baztech/element/bwmeta1.element.baztech-4d1dfaec-e029-4e54-833f-87ee27d83730.

[8] Wróbel K, Montewka J, Kujala P. Towards the assessment of potential impact of unmanned vessels on maritime transportation safety. Reliab Eng Syst Saf 2017;165(September):155–69 https://doi.org/10.1016/j.ress.2017.03.029.

[9] Burmeister, H-C., Bruhn W., Rødseth, O.J., and Porathe T. Can unmanned ships improve navigational Safety? In Chalmers Publication Library (CPL): 2014. http://publications.lib.chalmers.se/publication/198207-can-unmanned-ships-improve-navigational-safety.

[10] Burmeister H-C, Bruhn W, Rødseth OJ, Porathe T. Autonomous unmanned merchant vessel and its contribution towards the E-Navigation Implementation: the MUNIN perspective. Int J E-Navig Marit Econ 2014:1–13. December https://doi.org/10.1016/j.enavi.2014.12.002.

[11] Porathe, Thomas, Johannes Prison, and Yemao Man. Situation awareness in remote control centres for unmanned ships. In Chalmers Publication Library (CPL). 2014; 93. http://publications.lib.chalmers.se/publication/194797-situation-awareness-in-remote-control-centres-for-unmanned-ships.

[12] Abilio Ramos M, Utne IB, Mosleh A. Collision avoidance on maritime autonomous surface ships: operators' tasks and human failure events. Saf Sci 2019;116:33–44 https://doi.org/10.1016/j.ssci.2019.02.038.

[13] Ahvenjärvi S. The human element and autonomous ships. Transnav. Int J Marine Navig Saf Sea Transp 2016;10(3). nr https://doi.org/10.12716/1001.10.03.18.

[14] Man Y, Lundh M, Porathe T, MacKinnon S. From desk to field - Human factor issues in remote monitoring and controlling of autonomous unmanned vessels. Procedia Manufacturing, 6th International Conference on Applied Human Factors and Ergonomics and the Affiliated Conferences (AHFE). 3. 2015. January2674–81 https://doi.org/10.1016/j.promfg.2015.07.635.

[15] Wahlström M, Hakulinen J, Karvonen H, Lindborg I. Human factors challenges in unmanned ship operations – Insights from other domains. Procedia Manufacturing, 6th International Conference on Applied Human Factors and Ergonomics and the Affiliated Conferences (AHFE). 3. 2015. p. 1038–45. January https://doi.org/10.1016/j.promfg.2015.07.167.

[16] Hogg T, Ghosh S. Autonomous merchant Vessels: examination of factors that impact the effective implementation of unmanned ships. Austr J Marit Ocean Affairs 2016;8(3):206–22 https://doi.org/10.1080/18366503.2016.1229244.

[17] Van Hooydonk Er. The law of unmanned merchant shippingan exploration. J Int Mar L 2014;20(3):403–23.

[18] Perera LP, Ferrari V, Santos F, Hinostroza MA, Guedes Soares C. Experimental evaluations on ship autonomous navigation and collision avoidance by intelligent guidance. IEEE J Oceanic Eng 2015;40(2):374–87 https://doi.org/10.1109/JOE.2014.2304793.

[19] He Y, Jin Yi, Huang L, Xiong Y, Chen P, Mou J. Quantitative analysis of COLREG rules and seamanship for autonomous collision avoidance at open sea. Ocean Eng 2017;140(August):281–91 https://doi.org/10.1016/j.oceaneng.2017.05.029.

[20] Zheng H, Negenborn R, Lodewijks G. Trajectory tracking of autonomous vessels using model predictive control. *IFAC Proceedings Volumes*, 19th IFAC World Congress 2014;47:8812–8 https://doi.org/10.3182/20140824-6-ZA-1003.00767.

[21] Hurst, N.What will the autonomous ship of the future look Like? SMITHSONIAN.COM. 2017; February.

[22] Brown AJ. Collision scenarios and probabilistic collision damage. Mar Struct 2002;15:335–64 https://doi.org/10.1016/S0951-8339(02)00007-2.

[23] Goerlandt F, Montewka J. Maritime transportation risk Analysis: review and analysis in light of some foundational issues. Reliab Eng Syst Saf 2015;138(June):115–34 https://doi.org/10.1016/j.ress.2015.01.025.

[24] Goerlandt F, Montewka J. A framework for risk analysis of maritime transportation systems: a case study for oil spill from tankers in a ship–ship collision. Saf Sci 2015;76:42–66 https://doi.org/10.1016/j.ssci.2015.02.009.

[25] Hänninen M, Kujala P. Influences of variables on ship collision probability in a bayesian belief network model. Reliab Eng Syst Saf 2012;102:27–40 https://doi.org/10.1016/j.ress.2012.02.008.

[26] Huang Y, van Gelder PHAJM, Wen Y. Velocity obstacle algorithms for collision prevention at sea. Ocean Eng 2018;151:308–21.

[27] Montewka J. Predicting risk of collision for oil tankers in the Gulf of Finland. J Konbin 2009;11–12:17–32.

[28] Qu X, Meng Q, Suyi L. Ship collision risk assessment for the Singapore strait. Accid Anal Prev 2011;43:2030–6 https://doi.org/10.1016/j.aap.2011.05.022.

[29] Soares CG, Teixeira AP. Risk assessment in maritime transportation. Reliab Eng Syst Saf 2001;74:299–309 https://doi.org/10.1016/S0951-8320(01)00104-1.

[30] Tam C, Bucknall R. Collision risk assessment for ships. J Mar Sci Technol 2010;15:257–70 https://doi.org/10.1007/s00773-010-0089-7.

[31] Terndrup Pedersen P, Zhang S. On impact mechanics in ship collisions. Mar Struct 1998;11:429–49 https://doi.org/10.1016/S0951-8339(99)00002-7.

[32] Valdez Banda OA, Goerlandt F, Kuzmin V, Kujala P, Montewka J. Risk management model of winter navigation operations. Mar Pollut Bull 2016;108:242–62 https://doi.org/10.1016/j.marpolbul.2016.03.071.

[33] Zhang J, Zhang D, Yan X, Haugen S, Guedes Soares C. A distributed anti-collision decision support formulation in multi-ship encounter situations under COLREGs.

Ocean Eng 2015;105:336–48 https://doi.org/10.1016/j.oceaneng.2015.06.054.
[34] Hänninen M, Mazaheri A, Kujala P, Montewka J, Laaksonen P, Salmiovirta M, Klang M. Expert elicitation of a navigation service implementation effects on ship groundings and collisions in the Gulf of Finland. Proc Inst Mech Eng Part O J Risk Reliab 2014;228:19–28 https://doi.org/10.1177/1748006X13494533.
[35] Kujala P, Hänninen M, Arola T, Ylitalo J. Analysis of the marine traffic safety in the Gulf of Finland. Reliab Eng Syst Saf 2009;94:1349–57 https://doi.org/10.1016/j.ress.2009.02.028.
[36] Macrae C. Human factors at sea: common patterns of error in groundings and collisions. Marit Policy Manag 2009;36:21–38 https://doi.org/10.1080/03088830802652262.
[37] Mazaheri A, Montewka J, Kotilainen P, Edvard Sormunen O-V, Kujala P. Assessing grounding frequency using ship traffic and waterway complexity. J Navig 2015;68:89–106 https://doi.org/10.1017/S0373463314000502.
[38] Mullai A, Paulsson U. A grounded theory model for analysis of marine accidents. Accid Anal Prev 2011;43:1590–603 https://doi.org/10.1016/j.aap.2011.03.022.
[39] Sormunen O-VE, Goerlandt F, Häkkinen J, Posti A, Hänninen M, Montewka J, Ståhlberg K, Kujala P. Uncertainty in maritime risk analysis: extended case study on chemical tanker collisions. Proc Inst Mech Eng Part M J Eng Marit Environ 2014. 1475090213515640 https://doi.org/10.1177/1475090213515640.
[40] van de Wiel, G, van Dorp, JR. An oil outflow model for tanker collisions and groundings. Ann Oper Res 2011;187:279–304 https://doi.org/10.1007/s10479-009-0674-5.
[41] Cicek K, Celik M. Application of failure modes and effects analysis to main engine crankcase explosion failure on-board ship. Saf Sci 2013;51:6–10 https://doi.org/10.1016/j.ssci.2012.06.003.
[42] Hansen HL. Surveillance of deaths on board Danish merchant ships, 1986-93: implications for prevention. Occup Environ Med 1996;53:269–75 https://doi.org/10.1136/oem.53.4.269.
[43] Lois P, Wang J, Wall A, Ruxton T. Formal safety assessment of cruise ships. Tour Manag 2004;25:93–109 https://doi.org/10.1016/S0261-5177(03)00066-9.
[44] Soner O, Asan U, Celik M. Use of HFACS–FCM in fire prevention modelling on board ships. Saf Sci 2015;77:25–41 https://doi.org/10.1016/j.ssci.2015.03.007.
[45] Vanem E, Antão P, Østvik I, de Comas FDC. Analysing the risk of LNG carrier operations. Reliab Eng Syst Saf 2008;93:1328–44. Safety in Maritime Transportation https://doi.org/10.1016/j.ress.2007.07.007.
[46] Montewka J, Ehlers S, Goerlandt F, Hinz T, Tabri K, Kujala P. A framework for risk assessment for maritime transportation systems—A case study for open sea collisions involving Ropax vessels. Reliab Eng. Syst Saf 2014;124:142–57 https://doi.org/10.1016/j.ress.2013.11.014.
[47] Papanikolaou A. Ship design: methodologies of preliminary design. Springer; 2014.
[48] Papanikolaou A. Risk-based ship design: methods, tools and applications. Springer Science & Business Media; 2009.
[49] Vassalos D. Risk-based ship design. Risk-based ship design. Berlin, Heidelberg: Springer; 2009. p. 17–96 https://doi.org/10.1007/978-3-540-89042-3_2.
[50] Leveson N. Engineering a safer world: systems thinking applied to safety. MIT Press; 2011.
[51] Chatzimichailidou M, Dokas I. The risk situation awareness provision capability and its degradation in the Überlingen accident over time. Procedia Eng 2015;128:44–53. January https://doi.org/10.1016/j.proeng.2015.11.503.
[52] Aps, R., Fetissov, M., Goerlandt, F., Kopti, M. and Kujala, P.STAMP-Mar based safety management of maritime navigation in the Gulf of Finland (Baltic sea). In European Navigation Conference (ENC). 20161–8. https://doi.org/10.1109/EURONAV.2016.7530538.
[53] Karanikas N. Human factors science and safety Engineering. Can the STAMP model serve in establishing a common Language? 32nd EAAP Conference. 2017. p. 132–49.
[54] Fleming C, Spencer M, Thomas J, Leveson N, Wilkinson C. Safety assurance in nextgen and complex transportation systems. Saf Sci 2013;55(June):173–87 https://doi.org/10.1016/j.ssci.2012.12.005.
[55] Stringfellow MV, Leveson N, Owens B. Safety-Driven design for software-intensive aerospace and automotive systems. Proc IEEE 2010;98(4):515–25.
[56] Passenier D, Sharpanskykh A, de Boer RJ. When to STAMP? A case study in aircraft ground handling Services. Procedia eng. Proceedings of the 3rd European STAMP Workshop. 128. 2015. p. 35–43. October https://doi:10.1016/j.proeng.2015.11.502.
[57] Thomas J, Suo D. STPA-based method to identify and control feature interactions in large complex systems. Procedia Eng., Proceedings of the 3rd European STAMP Workshop. 128. 2015. p. 12–4. October https://doi:10.1016/j.proeng.2015.11.499.
[58] Chen J, Zhang S, Lu Y, Tang P. STPA-Based hazard analysis of a complex UAV system in take-off. In International Conference on Transportation Information and Safety (ICTIS). 2015. p. 774–9 https://doi.org/10.1109/ICTIS.2015.7232133.
[59] Hinchman J, Clark M, Hoffman J, Hullbert B, Snyder C. Towards safety assurance of trusted autonomy in air force flight critical systems. Computer Security Applications Conference, Layered Assurance Workshop. 2015.
[60] Oscarsson J, Stolz-Sundnes M, Mohan N, Izosimov V. Applying systems-theoretic process analysis in the context of cooperative driving. 11th IEEE Symposium on Industrial Embedded Systems (SIES). 2016. p. 1–5 https://doi.org/10.1109/SIES.2016.7509433.
[61] Mistree F, Smith W, Bras B, Allen J. Decision-Based Design: a contemoporary paradigm for ship design. Annual Meeting. San Francisco: The Society of Naval Architects and Marine Engineers. 1990.
[62] Voseen C, Kleppe R, Hjørungnes S. Ship design and system integration. DMK Conference. 2013.
[63] Sulaiman OO, Saharuddin OH, Kader AS, Wan Nik WB. Environmental risk compliance for nature gas ship design and operation. Can J Environ Constr Civil Eng 2011;2(5) https://doi.org/10.1109/JPROC.2009.2039551.
[64] Poel I, Robaey Z. Safe-by-design: from safety to responsibility. Nanoethics 2017;11:297 https://doi.org/10.1007/s11569-017-0301-x.
[65] Evans J. Basic design concepts. Naval Eng J 1959:671–8.
[66] Valdez Banda OA, Goerlandt F. A STAMP-based approach for designing maritime safety management systems. Saf Sci 2018;109:109–29 https://doi.org/10.1016/j.ssci.2018.05.003.
[67] Leveson N, Dulac N, Marais K, Carroll J. Moving beyond normal accidents and high reliability organizations: a systems approach to safety in complex systems. Org Stud 2009;30(2–3):227–49 https://doi.org/10.1177/0170840608101478.
[68] EMSA. Annual Overview of Marine Casualties and Incidents 2016. 2016.
[69] Valdez Banda, O.A. and Kannos, S.Hazards analysis process for autonomous vessels. ÄLYVESI (Samart City Ferries) project report. 2018. https://www.aboamare.fi/Results.
[70] Blanchard BS. System engineering management. John Wiley & Sons; 2004.
[71] Molland AF. The maritime engineering reference book: a guide to ship design. Construction and operation. Elsevier; 2011.
[72] Hardy K, Guarnieri F. Using a systemic model of accident for improving innovative technologies: Application and limitations of the STAMP model to a process for treatment of contaminated substances. In The 15th World Multi-Conference on Systemics, Cybernetics and Informatics (WMSCI). 2011.
[73] Bergström M, Erikstad SO, Ehlers S. Assessment of the applicability of goal- and riskbased design on arctic sea transport systems. Ocean Eng 2016;128:183–98.
[74] Bergström M, Hirdaris S, Valdez Banda OA, Kujala P, Sormunen O-V, Lappalainen A. Towards the unmanned ship code. Marine Design XIII. 13th International Marine Design Conference (IMDC) 2018. 2. 2018. p. 881–6.