Reliability Engineering and System Safety 178 (2018) 209–224

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

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

Towards the development of a system-theoretic model for safety assessment of autonomous merchant vessels

Krzysztof Wróbel[a,b,*], Jakub Montewka[b,c,d], Pentti Kujala[b]

[a] Faculty of Navigation, Department of Navigation, Gdynia Maritime University, Jana Pawła II av. 3, 81-345 Gdynia, Poland
[b] Department of Mechanical Engineering, Marine Technology, Research Group on Maritime Risk and Safety, Aalto University, Tietotie 1C, 02150 Espoo, Finland
[c] Faculty of Navigation, Department of Transport and Logistics, Gdynia Maritime University, Morska str 81-87, 81-225 Gdynia, Poland
[d] Finnish Geospatial Research Institute, Geodeetinrinne 2, 02430 Masala, Finland

ARTICLE INFO

Keywords:
Autonomous ships
STAMP
STPA
Safety of transportation
Safety assessment
Uncertainties

ABSTRACT

As the initiatives to develop and implement autonomous merchant vessels into the global shipping industry are gaining momentum, their safety remains in the spotlight. It is argued that every effort shall be taken to ensure that the safety of maritime transportation is not reduced in the process, but the question of how to achieve it remains open. Meanwhile, the systemic approach is more widely being used to analyse innovative systems' safety. We therefore apply a System-Theoretic Process Analysis to develop a model suitable for safety analysis and design recommendations' elaboration for future autonomous vessels. Furthermore, we introduce a method of evaluating and communicating uncertainties pertaining to the method. The results indicate that the system-theoretic safety analysis' outcome can be affected by manageable uncertainties despite the fact that the system in question is yet to be implemented.

1. Introduction

Recent R&D projects have investigated the feasibility of implementing a merchant vessel which would traverse the ocean without having any crew on board or even being controlled remotely. The results of such projects were encouraging, resulting in concepts and models attempting to quantify the safety of autonomous maritime navigation, see for example [1–3]. A body of literature focuses on safety quantification of prospective autonomous ships adopting risk assessment techniques that employ causal models [4]. To this end the Formal Safety Assessment has been utilised [5], resulting in the identification of major hazardous scenarios the unmanned ships can induce and their initial assessment in terms of safety as well as potential risk control options [4–7]. Although the apparent lack of data has been acknowledged, it was concluded that risk analysis is in favour of unmanned ships being generally safer than manned ones, provided that certain safety precautions are fulfilled [2]. Moreover, a general overview of potential failure propagation in case of an accident based on Bayesian framework is given in [8], arguing that particular aspects of a ships' operations, such as navigation, stability or cargo conditioning are mutually related in a variety of ways and must not be analysed separately [9].

However, the proposed risk-based approaches feature several shortcomings. Firstly, they require empirical data, which are non-existent since the autonomous shipping is still in the development phase. Secondly, the modelling techniques adopted therein do not allow for the detailed analysis of potential interactions between system's components but often assume simplified, causal, one-way relations instead. Thirdly, the safety is seen as a variable to be quantified rather than a feature to be controlled. This implies the limited applicability of the existing approaches to define the measures to effectively control the safety of the prospective autonomous ships. Therefore, the issue of ensuring such vessels' safety remains open, as argued in [8,10,11]. As the aforementioned vessels' expected implementation is a matter of years rather than decades [12], certain steps must be taken in order to ensure that the safety of marine transportation is not compromised in the process.

Thus another approach is needed to allow for the safety-driven design of the prospective autonomous merchant vessel's (AMV) system, [13]. The method should be able to examine it holistically, mimicking all relevant interactions between its components and surrounding environment. Within the maritime domain quantitative methods prevail, pertaining to ship and waterways design, or accident response, see for example [14–18]. Rarely, qualitative methods to evaluate safety are used, [19,20]. The former requires numbers and quantifiable parameters, which often may be missing, or unknown. The latter allows the

[*] Corresponding author at: Faculty of Navigation, Department of Navigation, Gdynia Maritime University, Jana Pawła II av. 3, 81-345 Gdynia, Poland.
E-mail address: k.wrobel@wn.am.gdynia.pl (K. Wróbel).

https://doi.org/10.1016/j.ress.2018.05.019
Received 26 May 2017; Received in revised form 17 March 2018; Accepted 31 May 2018
Available online 05 June 2018

incorporation of non-quantifiable (or difficult to quantify) factors such as organisational issues or human performance, [21].

Therefore, in this paper we delve into the safety of AMVs by applying the System-Theoretic Process Analysis (STPA), a tool rooted in System-Theoretic Accident Model and Processes (STAMP). STPA is a method of safety analysis that has been developed to elaborate on design recommendations for innovative technical systems, where safety is seen as a control problem, rather than an object of quantification [22]. The core of system-theoretic methods is to analyse interactions between a system's components and ensure that these remain safe rather than focusing on the reliability of every single component. Such an approach is believed to better encompass potential hazards and help create feasible measures to mitigate them [22]. The method has been used for the safety assessment of systems of varying natures like vessels' traffic management [23,24], automated driving vehicles [25] and offshore supply vessel dynamic positioning [26]. Despite various authors claiming that the system-theoretic approach delivers good predictions [21,27] of systems' safety performance in the presence of limited knowledge regarding their actual design, little attention has been devoted to the evaluation of potential uncertainties which exist in the process of safety recommendations' development and communication to a decision-maker, see for example [15].

The aim of this paper is two-fold. Firstly, it applies STPA to develop a model of autonomous ship's safety during high-seas operations and to elaborate on safety recommendations for future developers of such a system. Secondly, we introduce a simple solution to assess and communicate the uncertainties pertaining to the safety control model developed. The latter supports the former, with the intention of providing a decision-maker with an honest message on the type and extent of the uncertainty lying behind the resulting recommendations on how to control the safety within the anticipated system.

By focusing on the interactions between the system's components or their groups rather than a particular segments' reliability, the developed model advocates various ways to control the safety: technical, organisational and operational patterns, providing the end-user with a set of hazard mitigation measures. Furthermore, the conducted uncertainty assessment gives the system developers a preliminary insight into the expected effectiveness of those mitigation measures, also informing about the areas of the system that call for more thorough investigation.

The proposed model can be used by various stakeholders, such as system developers to incorporate the holistic safety approach to ship design, ship operators to develop safer operational procedures and maritime administrations to facilitate the process of rule-making for the AMVs' safety.

The paper is structured as follows: firstly, the materials and methods are described, including the System-Theoretic Process Analysis and prospective uncertainties assessment. Section3 introduces the results of the study, which are then discussed in Section4. Last but not least, the conclusions are drawn.

2. Materials and methods

2.1. Autonomous vessels' concept

Recently completed research projects concluded that, from the technical and economical point of view, the implementation of autonomous cargo ships can be feasible [2,5], although some legal issues must first be resolved [28,29]. Throughout the projects' deliveries [1,4,30,31] and in the increasing number of scientific papers based on the former, the general vision of an unmanned vessel is consistent [10,32–34], but the actual shape of the system remains in fact unknown. Therefore, we based our study on the literature review of the available sources pertaining to autonomous navigation and then on the experts' opinions. The general view emerging from these is given in this Section.

Although unmanned by design, such vessels might be required to unberth and leave the harbour waters under a direct control of a 'conning crew', due to the relative complexity of such manoeuvres [35,36] and port authorities' likely reluctance to accept unmanned vessels' operations in restricted waters [37]. The vessel would therefore need to accommodate a crew of a size comparable to today's ones for a limited period of time. Such crew would need to be capable of controlling the vessel and most of her equipment in a similar way to today's.

The 'conning' crew would then disembark the vessel by a launch boat or helicopter as soon as she leaves the port and it is considered safe to leave her, and leave her under the supervision of a shore-based operator. Such a person would assume an overall command and navigate the vessel from the office-like facility located ashore. Both-way communication would most likely be provided by the satellite communication link, perhaps augmented by other means of short-range data transfer, if applicable [38]. The feasibility of such a solution has been to some extent proven in August 2017 when an Offshore Supply Vessel performed several operations in the North Sea while being remotely controlled from California [39]. The operator would make system-level decisions based on data received from the shipborne sensors. Both data and decisions would be relayed to the vessel by a communication link [40] and executed by actuators including thrusters and rudders. Nevertheless, certain fail-to-safe mechanisms would still be required in order to maintain system's safety should the communication link fail for any reason.

The vessel would in such case be left on her own and would need to handle the situation autonomously. This might require going dead in the water or navigating to a safer area [6]. Since the autonomous navigation mode needs to be built-in to handle such emergencies, it can also be used to a greater extent – for the whole process of navigation itself. Herein, as soon as the vessel leaves high traffic density areas, operator's attention could be directed to other unmanned ships facing more difficult conditions. The level of ship's autonomy might be increased up to the point where she would require no more attention than a periodical check. Information provided by sensors would be analysed by highly sophisticated data fusion algorithms in order to automatically create decisions regarding virtually all aspects of navigation, cargo conditioning, machinery operations, stability and any other aspect of a vessel's operation [33]. The human operator will retain a position of merely a passive supervisor, person in charge of strategic decision-making (i.e. general passage planning) or a trouble-shooter. It is the vessel's control algorithms that will be responsible for making operational decisions and performing routine tasks.

Although the vision might look tempting, there are some social [41], legal [28,42] and technical issues that need resolving. The main source of potential problems is the performance of control algorithms and, as within a remote control mode, inability to manually operate any of the vessel's equipment [11]. Nevertheless, this mode could be used until the condition is detected that would require more direct intervention of the human operator which would, by definition, need to be taken and executed remotely as there will be nobody on board. As soon as the situation is resolved, the system might switch back to the autonomous mode. With the vessel successfully reaching the port of destination, the 'conning crew' might be required again for berthing. After the cargo transfer or any other operations are completed, the cycle could repeat.

By that, the vessels are anticipated to follow an 'adjustable autonomy' scheme depending on the condition of the ship herself and a mission being executed. Expected levels of autonomy in the maritime industry as elaborated by Lloyd's Register of Shipping [43] are listed in Table 1 below, although other frameworks have also been developed [44,45].

Fully autonomous mode of unmanned ship's operation (AL-5) is expected to be the primary and the most extensively used one, particularly for ocean crossings. Autonomous operation can help exploit the

Table 1
Ship autonomy levels, based on [43].

Autonomy level	Description
AL-0	No autonomous function – all decision making is performed manually, i.e. a human controls all actions at the ship level.
AL-1	On-ship decision support – all actions at the ship level are taken by a human operator, but a decision support tool can present options or otherwise influence the actions chosen, for example DP Capability plots and route planning.
AL-2	On and off-ship decision support – all actions at the ship level taken by human operator on board the vessel, but decision support tool can present options or otherwise influence the actions chosen. Data may be provided by systems on or off the ship, for example DP capability plots, OEM recommendations, weather routing.
AL-3	'Active' human in the loop – decision and actions at the ship level are performed autonomously with human supervision. High-impact decisions are implemented in a way to give human operators the opportunity to intercede and over-ride them. Data may be provided by systems on or off the ship.
AL-4	Human on the loop: operator/supervisory – decisions and action are performed autonomously with human supervision. High impact decisions are implemented in a way to give human operators the opportunity to intercede and over-ride them.
AL-5	Fully autonomous – unsupervised or rarely supervised operation where decisions are made and actioned by the system, i.e. impact is at the total ship level.
AL-6	Fully autonomous – unsupervised operation where decisions are made and actioned by the system, i.e. impact is at the total ship level.

full potential of unmanned shipping by involving humans in the process to only a very limited extent and using automated systems instead. It is also the most challenging of all modes as less scientific and technical data is available to properly assess its actual feasibility and safety. The recent publication of numerous scientific papers on unmanned shipping does not change the fact that empirical data is required to validate statements contained within. Data pertaining to the safety of autonomous transportation is only available for other domains such as automotive or underwater [46,47]. It can, however, be considered incomplete as most of the technologies are still in their early stages of development.

In this paper, we focus on AL-5 and analyse the safety of vessel operating in this mode, using the methods presented in Sections 2.2.1–2.2.3. Security and cybersecurity issues in general remain outside of this study's scope, although it must be understood that they might pose a significant threat to system's integrity and negatively affect its safety in multiple ways [4,5].

2.2. Methods

Methods used to perform the safety assessment are described throughout this Section. Sections 2.2.1 and 2.2.2 present a brief description of System-Theoretic Process Analysis as well as a method of modelling the system, while Section 2.2.3 gives an overview of a mitigation potential elaboration. Section 2.2.4 in turn presents a method of assessing and communicating the uncertainties related to the safety analysis.

2.2.1. System-Theoretic Process Analysis – STPA

STPA is a method of examining a given system's safety by analysing the interactions between its components [26] and the ways in which those can be unsafe [22]. The nature of such interactions shall ensure that the system as a whole remains within safety limits [48,49]. As a consequence of the above, any violation of the defined safety constraints leads to the emergence of a hazard (*a system state or set of conditions that, together with a particular set of worst-case conditions, will lead to an accident*). It is recommended to refrain from calculating the probabilities of a system transitioning to an unsafe state [15] due to lack of empirical data, particularly in initial phases of the system development [22].

Being rooted in STAMP, STPA shares all of its major features, both on advantages' and drawbacks' sides. As for the former, the underlying assumption of probability-based thinking being not suitable for the comprehensive analysis of today's modern and complex systems is the major one [22]. Therefore, the interactions and mutual relationships between the system's components are studied instead of its reliability structure. For instance, system-theoretic analysis of the '*Sewol-Ho*' ferry sinking helped identify numerous contributing factors that could be overlooked when analysing the ferry's reliability structure [50]. Evoking the classic Swiss cheese model [51], system-theoretic methods strive to keep the cheese slices in proper positions in relation of one to another rather than ensuring that their holes are sufficiently small. The latter approach, however, must not be neglected as the reliability remains one of the means of ensuring safety [52].

2.2.2. Safety control structure elaboration and analysis

In a generic control process, as depicted in Fig. 1, system integrity depends on ensuring that interactions between components do not lead to safety constraint violations. The study follows the most frequently used classification of causal factors, where four potential ways of inadequate control can be distinguished (although some argue that this number can be increased to six, see for Ref. [49]):

(a) a control action required for safety is not provided or not followed;
(b) an unsafe control action is provided;
(c) a potentially safe control action is provided at the wrong time or in the wrong sequence;
(d) a control action required for safety is stopped too soon or applied too long [22,49,53].

As a preparation for the STPA, a model of the system's safety control structure, depicting mutual relationships between system's components, is created. This was achieved by reviewing the available literature pertaining to AMVs, see for instance [1,10,31,34,37,54–57] and a Delphi-based workshop with a wide selection of experts involved in the research project resulting in the design concepts of several unmanned vessels, including coastal ferry, costal container carrier and middle size, sea-going container carriers. The group of 15 experts was comprised of

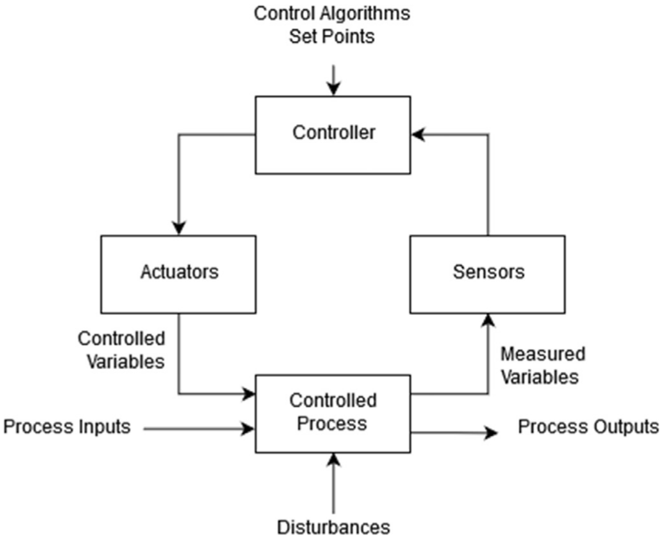


Fig. 1. A generic control loop, as given in [22].

ship designers, naval architects, ship operators (navigators and captains), traffic controllers, representatives of the maritime authorities and researchers in various field of technical sciences (mechanical, telecommunications and electrical engineering, IT, maritime studies, law, naval architecture, system safety).

Similarly, a list of hazards (see Table 3) was created in order to systematise knowledge regarding the safety of an autonomous generic merchant vessel and identify potentially hazardous conditions that may be encountered by the system during its operations.

Thence, control loops within a safety control structure were investigated and a potential for inadequate control was sought. In the next step, each control action was examined with respect to above potential ways of inadequacy. Components involved and failure scenarios were identified and ways of mitigating the potential for inadequacy – recommended [21].

Such 'generic' ship is defined as not having any particularly demanding requirements pertaining to cargo stowage. This was based on the assumption that the autonomous shipping technology will first be tested on vessels carrying commodities not requiring a complicated conditioning. If the prototype tests prove the technology's feasibility, more challenging cargoes could be accommodated by augmenting the design with new functionalities [30]. Bulk carriers, general cargo or container vessels can be good candidates for the prototype [58,59]. Although they can be technologically advanced even nowadays, their cargo conditioning equipment and technology as well as safety features are far simpler than those of tankers or passenger vessels, for instance. The notable exemption can be the river-crossing ferry as its mission's relative simplicity and being close to river banks at all times also makes such a vessel a good candidate for the prototype of an autonomous ship [1].

As the entire concept of an autonomous vessel capable of crossing oceans is still at a relatively early design phase as this paper is being written, some vital information pertaining to the system's actual shape can be lacking or incorrect. Therefore, the paper should be considered as merely an initial insight and elaboration of basic safety recommendations rather than a complete and final safety assessment. This is in line with the concept of safety-guided design, a process of an iterative cooperation between system developers and safety analysts [22]. Such recommendations are presented in the form of mitigation measures and evaluated by an assignment of a 'mitigation potential' value.

2.2.3. Mitigation potential analysis

Instead of calculating the probability of a hazardous event, a mitigation potential can be evaluated in a systemic approach, a parameter describing the effectiveness of a particular action (a mitigation measure in other words), aiming to restrict the accident's likelihood or consequences. To this end, the following mitigation potential scale is used:

1. reduction of damage if an accident does occur;
2. reduction of the likelihood that the hazard results in an accident;
3. reduction of the likelihood that the hazard will occur;
4. complete elimination of the hazard from design [22].

The design process will involve safety-driven optimisation of a system aiming primarily at the reduction of an accident's likelihood and then in confining its consequences. Thereby, it can be understood as searching for and implementing hazard control measures having higher mitigation potential assigned. Those with greatest mitigation potential are viewed as being more efficient and cost-effective when it comes to accident prevention and, in the worst-case scenario, damage reduction.

In our study, we reviewed the available literature in order to find all potentially feasible mitigation measures and recommend them as a protection against particular control action becoming inadequate. These measures were listed and their theoretical effectiveness was evaluated in the form of mitigation potential. As a result, we quantified the recommended measure's capability of ensuring that the particular control action remains adequate. This was done instead of calculating the mitigation measure's potential of preventing a hazard from leading to an accident and was caused by a low-detail level of the developed model.

Furthermore, we augmented our recommendations' elaboration by the analysis of uncertainties.

2.2.4. Uncertainty assessment and communication

Kaplan and Garrick claim that the very purpose of risk analysis is to provide an input to the underlying decision making [60]. It is therefore the obligation of analysts to consider the consequences of their error, which can only be done if the uncertainties pertaining to the study's results are identified and assessed. Wrong or weak assumptions, poor data or unreliable models may lead to unjustified conclusions within the safety assessment and wrong decisions [61–65]. With the presence of important uncertainties, decision-makers may justifiably opt for additional (and potentially superfluous) protective measures while accepting the increased costs [61].

The necessity of including the uncertainty analysis in safety assessments is therefore becoming widely acknowledged with different approaches applied [66–68]. Such a requirement was also raised with regard to system-theoretic methods of safety assessment [15]. As argued, STAMP and related tools help reduce the uncertainties by themselves as they offer a more insightful look into the system behaviour [21]. However, they must not be considered a perfect tool that eliminates the uncertainties completely. These will still exist on virtually all steps of STPA as depicted in Fig. 2. One of the main reasons for this situation is that the STPA is very often used to assess the safety of innovative endeavours, just as is the case of an unmanned merchant vessel. There are two potential solutions of this situation: (1) reduce the uncertainty by better modelling the system or (2) characterise uncertainty better [15]. The former can be difficult at the present stage of technological development as the only information pertaining to future autonomous ships' system design can be extracted from the scientific and professional literature or elicited from experts involved in the works. This has been done in the course of the present study. There is no guarantee, however, that the AMV's design will not dramatically change prior to implementation. On the contrary: the very purpose of the safety-driven design is to identify and suggest potentially beneficial revisions in order to improve future system's safety performance. It is therefore the only choice to communicate the uncertainties to the decision-makers so as they could make informed decisions.

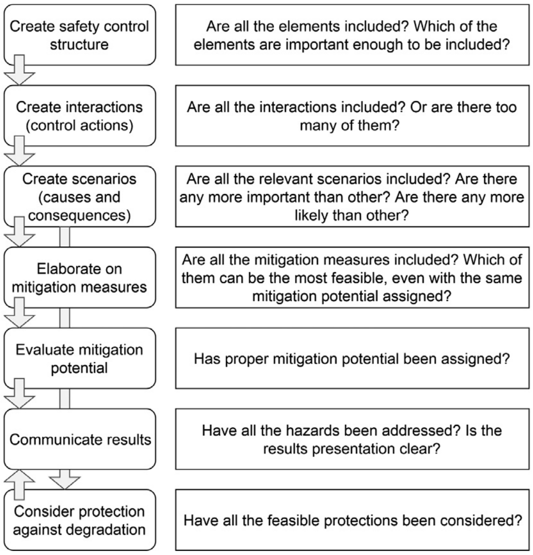

Create safety control structure
Are all the elements included? Which of the elements are important enough to be included?
Create interactions (control actions)
Are all the interactions included? Or are there too many of them?
Create scenarios (causes and consequences)
Are all the relevant scenarios included? Are there any more important than other? Are there any more likely than other?
Elaborate on mitigation measures
Are all the mitigation measures included? Which of them can be the most feasible, even with the same mitigation potential assigned?
Evaluate mitigation potential
Has proper mitigation potential been assigned?
Communicate results
Have all the hazards been addressed? Is the results presentation clear?
Consider protection against degradation
Have all the feasible protections been considered?

Fig. 2. Uncertainties' sources when using STPA.

Table 2
Uncertainty scale, inspired by Flage and Aven [68] with modification.

		Uncertainty magnitude		
		Significant (red)	Moderate (yellow)	Minor (green)
Category	Phenomena	Low level or no understanding	Medium level of understanding	High level of understanding
	Model	No basis for models or models give poor predictions	Some basis for models, level of simplifications adopted varies across the model; alternative hypotheses exist	Strong basis for the models, which give good predictions
	Assumptions	Poor justifications for the assumptions made, oversimplifying the analysed phenomena	Reasonable justifications for the assumptions made, although simplifying the analysed phenomena	Seen as reasonable
	Data	Not available or reliable	Data of varying quality is available	Much reliable data is available
	Consensus	Lack of consensus	Various views exist among experts	Broad agreement among experts

Since the hazard mitigation measures' effectiveness remains the most important of the systems' features for designers, operators and maritime administrations, we focus on this stage of safety analysis and develop a method of assessing uncertainties pertaining to it.

The view that system-theoretic methods can be augmented by other frameworks in order to analyse the uncertainties existent therein was presented in [69]. One of the first attempts to include an uncertainty analysis in STAMP was then given in [15] where the strength of knowledge supporting the analysis was postulated as the most important factor to be included. In order to expand this approach, we modified the 'degree of uncertainty' scale as described in [68] and further polemicised in [61]. The modification was carried out as a response to the on-going discussion in academia [70,71].

For each mitigation measure elaborated as per the framework given in Section 2.2.2, available information related to it has been assessed in five categories: understanding of phenomena, accuracy of the model, viability of assumptions made, availability of data, strength of consensus among experts. The framework is presented in Table 2. As seen, the assessment is qualitative in nature and was performed by the analysts themselves in the course of subjective assessment. The uncertainty in this case can be defined as an analysts' degree of belief that the elaboration of a particular mitigation measure is supported by sufficient data, assumptions etc., and that the mitigation measure in question is feasible to implement.

After a mitigation measure has been identified as potentially valuable in ensuring adequacy of particular control action, additional information about it was collected and reviewed from available literature particularly in the field of unmanned shipping, autonomous operations and maritime transportation. Especially, the following has been assessed:

- Phenomena – what is the level of understanding of the mitigation measure's functionalities? If it was successful in ensuring safety when applied in other domains, can the same be achieved in autonomous shipping?
- Model – is the model of a given mitigation measure's interactions with the system available? Are the consequences of implementing the particular mitigation measure in autonomous shipping well-comprehended?
- Assumptions – do assumptions supporting the implementation of a mitigation measure have a strong basis?
- Data – is the empirical data addressing application of a mitigation measure published in a variety of sources? Are the results conclusive?
- Consensus – do authors of scientific and professional publications agree on the feasibility of a given mitigation measure? Is it mentioned as a potential solution in a considerable number of sources?

Based on the answers to above questions, an uncertainty level in each of five categories has been assigned to all the mitigation measures. This could be significant, moderate or minor. Thus, a subjective level of analyst's confidence in the feasibility of particular mitigation measure is communicated.

Results of the above steps of autonomous merchant vessel's safety assessment are presented in Section3 and discussed in Section4.

3. Results

This Section presents the results of analysis: the safety control structure of the autonomous ship, list of hazards as well as uncertainties pertaining to the mitigation measures' elaboration.

3.1. Safety control structure of the autonomous ship

The autonomous vessel's high-level safety control structure is presented in Fig. 3. Herein, the most discernible component is a 'Virtual Captain' (VC), a computer controlling all on-board equipment and processes. Data is fed by environmental sensors (those measuring parameters of the environment, i.e. radar with Automatic Radar Plotting Aid, Automatic Identification System, infra-red cameras, echo-sounder, log, gyrocompass, Global Navigation Satellite System receivers etc.) as well as internal ones (i.e. rudder angle indicator, main engine status indicators, tank gauges, fire sensors) [34]. VC's main objective is to ensure that the vessel follows the prepared passage plan, reaches the port of destination within the assumed time and without causing any hazard to herself, other assets, humans or environment.

Based on the information received and the ship's control model, control algorithms formulate decisions, which are then executed by actuators in order to control shipborne processes. These actuators can include mechanisms of a diverse nature such as steering pumps, fuel system valves, fog horn and fire extinguishing system. Virtually all aspects of the ship's operation must be controlled for a prolonged time without any involvement of human operators except periodical conditions check. Those aspects involve 'Navigation' (meaning vessel's course and speed) and a large number of 'Auxiliary processes', the aim of which will be to ensure the vessels' optimum performance and safety. These are not addressed individually as their list and characteristics would depend on the actual system's design. Instead, they are only referred to in general.

Such an arrangement of the system would last until safety parameters exceed their limits. If that is the case, the VC would use the satellite communication link to call for the operator's assistance and switch the entire system to a lower level of autonomy, e.g. AL-3, see Table 1. Such limits shall be adjusted by human operators, which is to be done via communication link.

The VC might be capable of coordinating certain actions with other

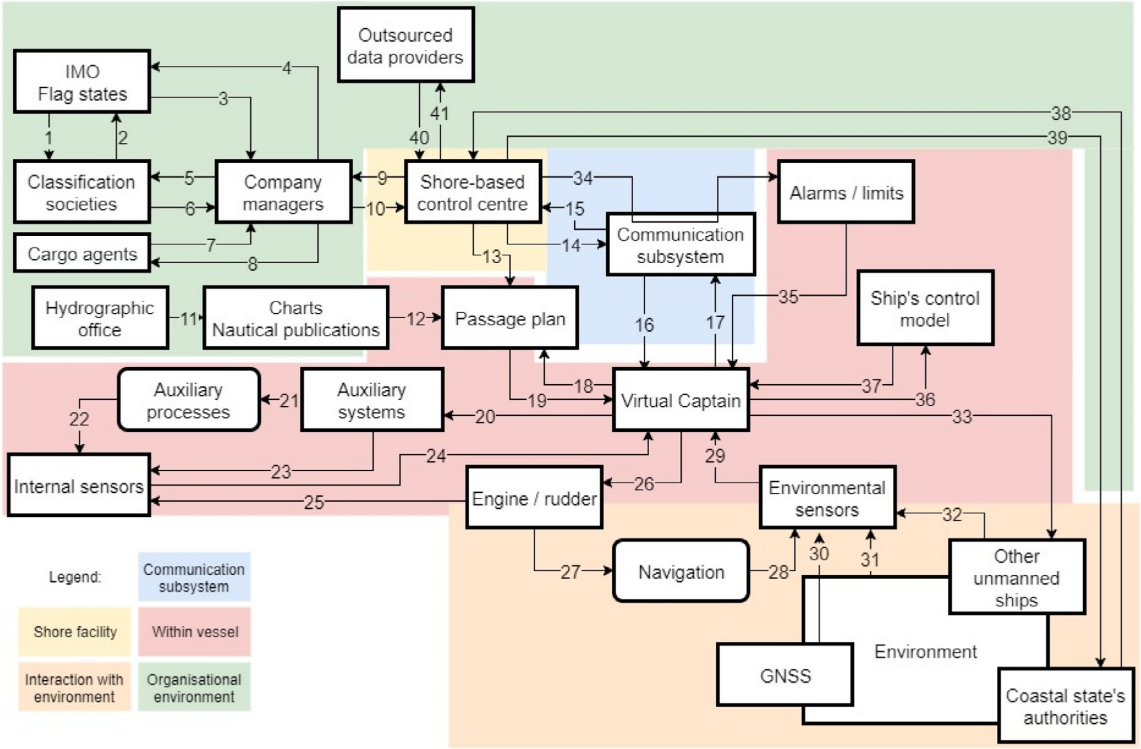


Fig. 3. Autonomous vessel's system safety control structure. (For interpretation of the references to colour in this figure, the reader is referred to the web version of this article.)

unmanned ships in the vicinity, but ways in which other third parties could influence vessel's behaviour should be limited for security reasons. For instance, coastal states' administrations ought to be capable of advising certain actions to be taken by the vessel, but the final decision should be the responsibility of the operators [31]. Similarly, the latter should have a convenient way of contacting the coastal states' authorities in order to perform administrative work or coordinate certain actions. Search and Rescue operations can serve as a good example of these.

Furthermore, the autonomous vessel will operate within a certain organisational and legal framework as shaped by today shipping industry's architecture. That will require following international regulations and rules for classification as well as cooperating with external organisations. The system's position within such a framework is yet to be clarified [28,29].

The 'system' of an autonomous ship can therefore be defined as below:

> *'all technical, organisational and human-based arrangements purposely designed or utilised in order to perform a safe navigation of a sea-going vessel operating autonomously'*

The defined system will consist of each component that has been either designed or can be intentionally used as its part. That would include not only the ship itself, but also the shore-based control centre (SBCC), software, hardware and liveware involved, operational procedures and legislation. In other words, everything on which system's designers can have certain degree of control.

The natural environment and ships other than unmanned will to a large extent remain outside of the system, thus will be generally referred to as the 'environment'. This will, unfortunately, also include illegal activities. These however remain out of this analysis' scope.

After the safety control structure as well as hazards' and constraints' list had been created, we performed the actual STPA. Each of the control actions was investigated in order to identify potential consequences and causes of it being inadequate. Then, we sought mitigation measures that might reduce the potential for such inadequacies. These measures were assigned the mitigation potential.

Results of the above are presented in Section 4 as well as in Appendices.

3.2. STPA

Based on the system's safety control structure presented in the former Section, a list of hazards and related safety constraints was compiled as given in Table 3.

As can be seen, an occurrence of certain hazards may propagate the emergence of others. Failure of propulsion, for instance (Hazard #2.2.) may lead to vessel's grounding (#2.1), then loss of structural integrity (#2.6.). Therefore, mitigation measures capable of protecting against multiple hazards simultaneously can be characterised by greatest effectiveness.

The hazards' list was then used as an aid in performing the actual STPA. In its course, a total of forty-eight control actions have been analysed with respect to their position within the system structure, potential scenarios leading to their inadequacy and consequences of such. Furthermore, potential ways of mitigating such inadequacies were elaborated and evaluated by the assignment of the mitigation potential. A total of 252 recommendations on mitigation measures' implementation have been elaborated, each of them pertaining to one of three classes: covering liveware, software or hardware. By 'liveware' we understand all organisational, legal and operational factors in which a human plays a major and direct part.

The catalogue of control actions together with the results of STPA is presented in Appendices.

3.3. Uncertainties

Unfortunately, the process of elaborating recommendations on mitigation measures' implementation is burdened with some uncertainties. These have been assessed in line with the method given in

Table 3
List of high-level system hazards and safety constraints. Partly based on [4,11,72]. Repetitive hazards have been crossed out and omitted in further steps.

#	Description of **hazard**
1	**Vessel's physical interaction with manned structures results in death or injury**
1.1	**Vessel violates minimum CPA with another ship**
1.2	**Vessel enters a No Go Area**
1.3	**Vessel improperly interacts with other man-made structures**
1.4	**Vessel is incapable of properly containing dangerous chemicals or energy**
1.5	**Vessel is boarded by unauthorised personnel or such commodities are placed on board**
1.6	**System does not provide assistance to person in distress**
2	**Vessel's inability to reach port of destination in expected time**
2.1	~~**Vessel enters a No Go Area**~~
2.2	**Propulsion/steering gear operational parameters cannot be maintained**
2.3	**Vessel is denied passage by coastal state's authorities**
2.4	**Vessel's navigational capabilities are impaired by weather conditions**
2.5	**Vessel does not meet stability criteria**
2.6	**Vessel's watertight integrity is not maintained (due to shear forces, bending moments or puncture)**
3	**Vessel's inability to deliver cargo in unchanged condition or in a condition that falls within industry standard**
3.1	**Vessel's cargo is not loaded/stowed properly**
3.2	**Vessel is unable to maintain proper cargo stowage conditions Vessel is unable to maintain proper cargo stowage conditions**
4	**Vessel's exposure to major damage or breakdown**
4.1	~~**Vessel enters a No Go Area**~~
4.2	~~**Vessel violates minimum CPA with another ship**~~
4.3	**Vessel does not meet fire safety precautions**
4.4	~~**Vessel's watertight integrity is not maintained**~~
4.5	**Vessel's power supply is not provided or insufficient**
4.6	**Both-way communication with the vessel cannot be established**
5	**Vessel's inability to prevent environmental pollution**
5.1	**Vessel is unable to maintain integrity of tanks containing oils or oily mixtures**
5.2	**Vessel is unable to maintain proper fuel combustion parameters**
5.3	~~**Vessel is incapable of properly containing dangerous chemicals or energy**~~
6	**Vessel's interaction with third-party assets causes reduction of their value or operational abilities**
6.1	~~**Vessel violates minimum CPA with another ship, runs into element of infrastructure or damages other man-made objects**~~
6.2	**Vessel contributes to delay of other ships' traffic**
6.3	**System does not meet international, classificatory or national regulations**
6.4	**System's communication subsystem unintentionally interferes with other assets**
6.5	**System's interaction with other assets (including unmanned vessels) leads to the emergence of any of above**

Section 2.2.4 and are presented within the Appendices where small symbols are placed as a reference to Table 2. Therein, a level of uncertainty in each of five categories is expressed for every mitigation measure. Grey shading within the symbols indicates that for each of five rows (corresponding to the uncertainty categories: Phenomena, Model, Assumptions, Data, Consensus in this order top to bottom), uncertainty has been assessed as either Significant, Moderate or Minor (in this order, left to right), see Table 4.

These uncertainties have been summarised in Fig. 4, where a traffic light symbolism is utilised to describe uncertainties related to the mitigation measures belonging to one of three classes (liveware, software or hardware) and five major portions of the system: organisational environment, shore facility, communication, vessel and her direct environment (horizontal axis, also indicated by background colour in Fig. 3). Therein, red represents the number of instances in which significant uncertainty has been assigned to the process of elaborating given the mitigation measure. The latter pertains to the relevant portion of the system and the mitigation measures' class. Similarly, green represents minor uncertainties whereas yellow denotes their moderate level.

In Figs. 5–7, the breakdown of uncertainties' magnitudes for each of the three classes are depicted in more detail, taking into account the categories of uncertainty (phenomena, model, assumptions, data and consensus).

3.4. Case study

The application of the presented method is demonstrated through case studies. Two selected control actions, out of 48 that exist in the proposed model of autonomous ship safety, are analysed here.

3.4.1. Analysis of control action #31 Environment probing

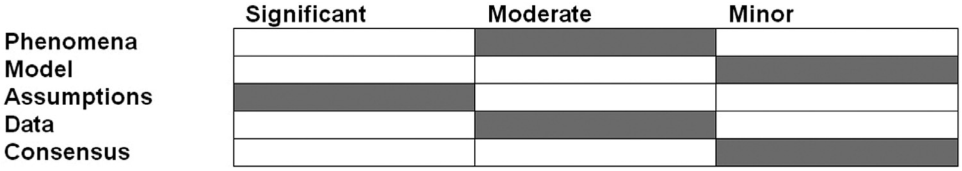
#31: *Environment probing* consists of gathering environmental data by autonomous vessel's sensors in order for the VC to create a situational awareness [73]. Those sensors can include GNSS receiver, radar, echosounder, log, infra-red camera, anemometer etc. The importance of this control action is based on the consequences of its inadequacy: should sensors fail to gather the data pertaining to weather and other ships' traffic, the VC would become 'blind' and will not be capable of performing the navigation process safely and efficiently. This might cause improper decisions to be made and sent to the propulsion subsystem. It has been assessed that this could lead to the emergence of as many as thirteen different hazards as defined in Table 3.

Such inadequacy (failure to observe environmental conditions) can be caused by a variety of factors that have been identified. Those include sensors' failures, installed sensors' inability to measure a required feature, unsuitable sensors being installed or their sub-optimal performance. To counteract the above, the following mitigation measures have been elaborated:

1. implementation of redundancy or development of highly-reliable sensors,
2. use of sensors capable of measuring multiple features simultaneously (just as GNSS receiver can provide data pertaining to its position, speed and course over ground),
3. development and implementation of highly sensitive sensors with reduced sampling time.

All the above pertain to hardware solutions and interaction of the system with the environment. They are also intended to reduce the likelihood of the relevant control action's inadequacy occurrence; therefore, they were assigned a mitigation potential value of '3', as given in Section 2.2.3. As for protection against control degradation, the development of improved sensors can be named along with implementation of leading indicators detecting the worsening

Table 4
Illustration of symbols used as an uncertainty level indication within Appendices.



	Significant	Moderate	Minor
Phenomena		■	
Model			■
Assumptions	■		
Data		■	
Consensus			■

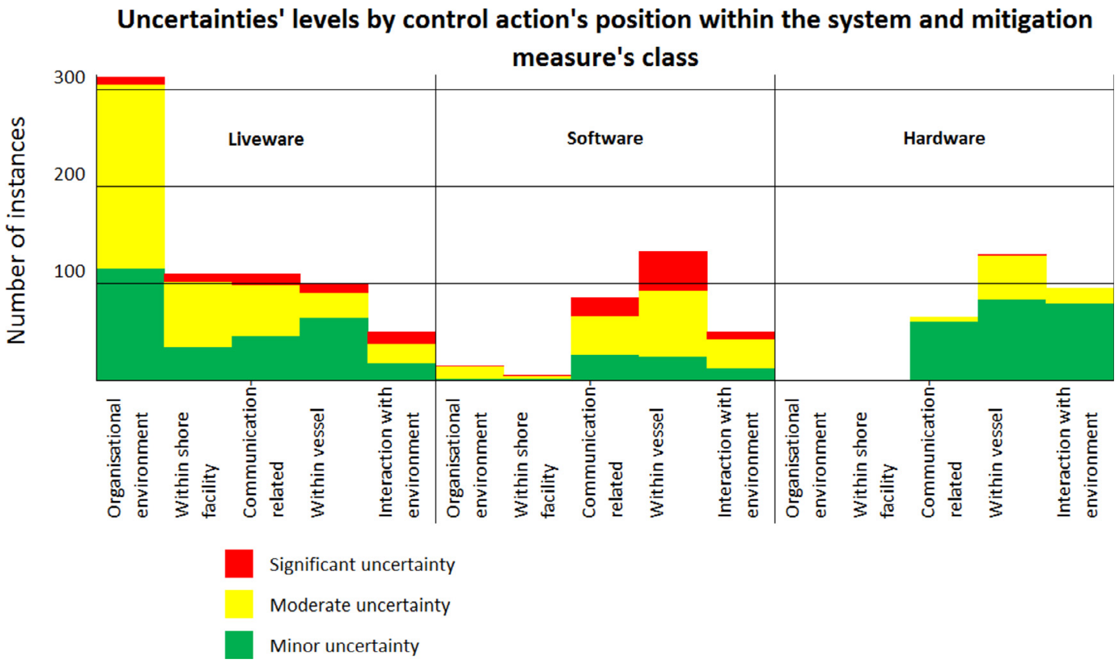


Fig. 4. A high-level breakdown of the uncertainties by class of mitigation measure and control action's position within the system.

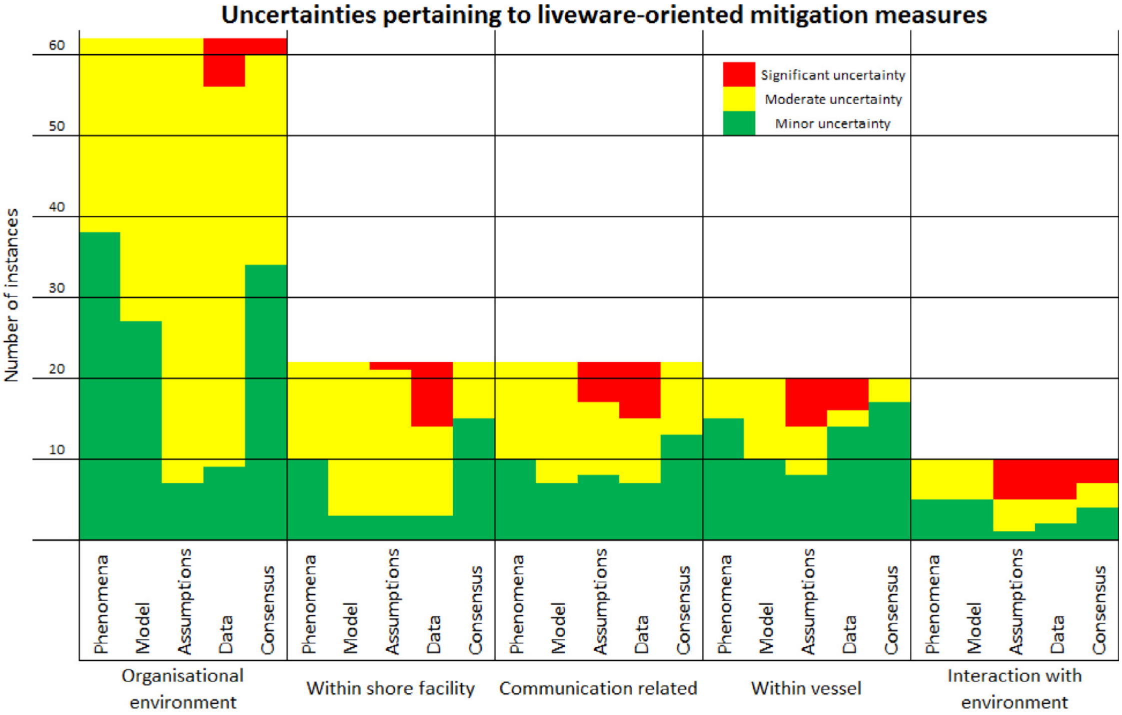


Fig. 5. A detailed breakdown of uncertainties by categories for autonomous vessels’ liveware solutions.

performance of a particular sensor and prompting for its immediate replacement [53,74] (which would only be possible once the vessel calls at a port of convenience [75]).

Thence, uncertainties pertaining to the mitigation measures’ elaboration have been qualitatively and subjectively assessed based on literature review, sometimes pertaining to other domains than autonomous shipping, for which more experience has been gained in recent years and more information is available. Factors as listed within Table 5 have been taken into consideration while assessing the uncertainty.

3.4.2. *Analysis of control action #21 Regulation*

#21: *Regulation (of auxiliary processes)* incorporates control imposed upon phenomena not immediately related to the ship's movements. Those can include a variety of processes ranging from exhibition of navigational lights through the operation of AMV's ballast system. Such diversity issues to be regulated by numerous types of equipment can lead to the emergence of many hazards, but also calls for multiple solutions and different measures of their mitigation. These vary from design-based and procedural to hardware.

Table 6 contains factors taken into consideration when evaluating

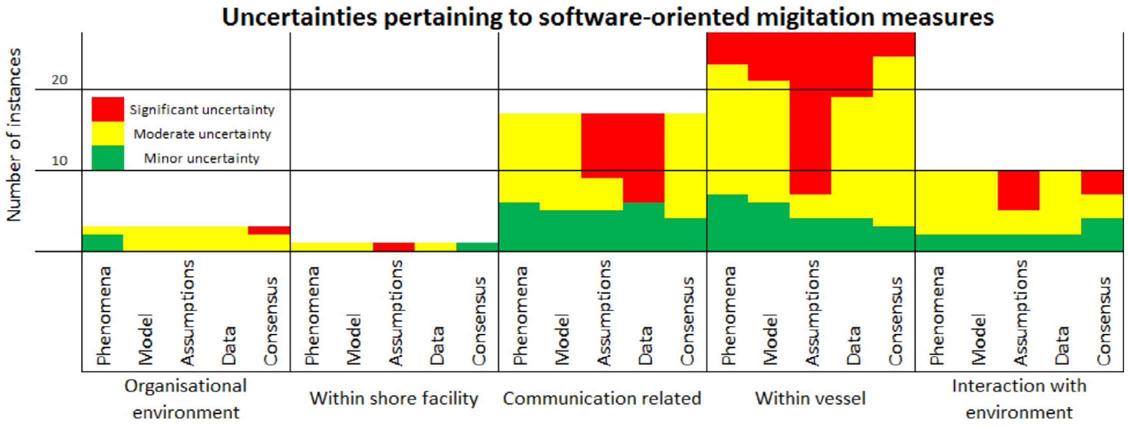


Fig. 6. A detailed breakdown of uncertainties by categories for autonomous vessels' software solutions.

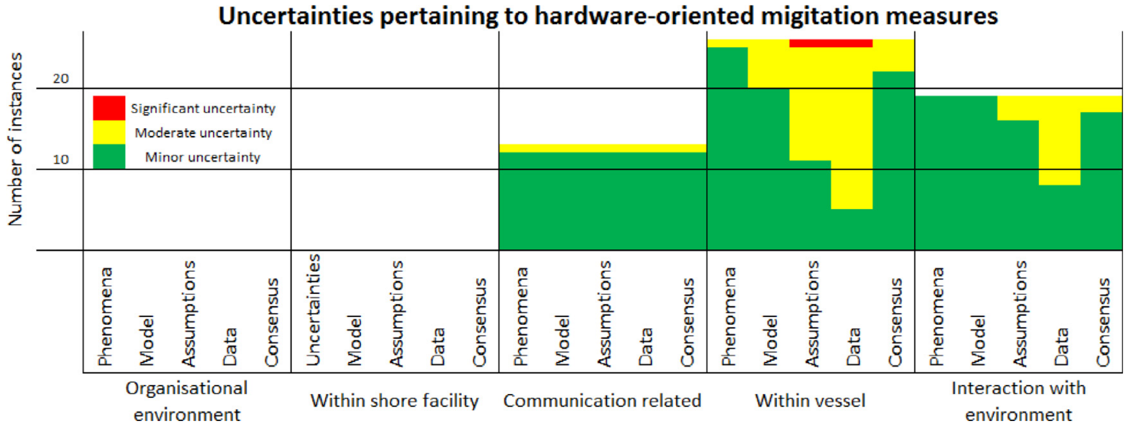


Fig. 7. A detailed breakdown of uncertainties by categories for autonomous vessels' hardware solutions.

the level of uncertainties pertaining to particular hazard mitigation measures. The rationale behind the latter can be summarised as follows:

- Rigorous maintenance regime: since equipment is to operate in a prolonged maintenance-free mode, upkeep must be performed strictly as required to satisfy operational needs.
- Redundant equipment: certain system's functions can be performed by secondary (spare) machinery should the primary one suffer from malfunction.
- Resilience-based design: the system shall retain ability to perform its basic (life-sustaining) operations in all circumstances for a period of time required for intervention, this can be achieved through resilience engineering.
- Procedures on consumables' management: as various resources (fresh water, lubricants, oils etc.) can be required for machinery to operate, these must be available and procedures aiming in their supply shall be implemented.
- Capacity surpluses: since it may turn out that system meets previously unrecognised and demanding operational parameters, equipment shall be capable of flexibly adapting to such, for instance by operating with above-nominal capacity.
- Extensive testing: all machinery shall be thoroughly tested so as to demonstrate its fitness and interoperability with the rest of the system.
- Implementation of leading performance indicators: potentially dangerous conditions could be detected before they actually occur by implementation of leading indicators, measuring latent anomalies in given subsystem's performance.

Herein, all mitigation measures except 'resilience-based design' are intended for the reduction of a potential hazard's likelihood of occurrence.

Results of the performed analysis are presented mostly in Appendices for each control action as given in Fig. 3 and discussed throughout Section 4.2.

4. Discussion

Results obtained within the autonomous vessel's system preliminary safety assessment are discussed in Section 4.1. Thence, Section 4.2 elaborates on uncertainties pertaining to the former and the potential ways of addressing them.

4.1. Safety assessment results

Tables as given in Appendices shall be considered as one of the first steps in assisting designers of future autonomous ocean-going vessels in incorporating safety into the system's design. Since the concepts of the system are still in the relatively early development phases as this paper is written, results of the study must inevitably be very general. Nevertheless, virtually all control loops and actions can and shall be addressed on a higher detail level as the system's development progresses and more information is available. By reviewing the results of the study, few features can be highlighted.

4.1.1. Overview

For the reasons mentioned in the Introduction, instead of applying the methods of quantitative safety analysis, the system-theoretic, qualitative method has been used. Herein, safety was not actually evaluated since no specific statements describing the expected safety

Table 5
Detailed refinement of uncertainty levels in mitigation measure's elaboration – control action #31. See Refs. [76–86].

Mitigation measure	Uncertainty category	Description	Result (uncertainty level)
Redundancy and improved reliability	Phenomena	Well-recognized as a way of ensuring particular subsystem's reliability [44,75,76]	Minor
	Model	Consequences of applying it into autonomous shipping are rather well-comprehended: it will increase investment costs [76,77] but will also help providing necessary data, possibly by use of data fusion algorithms [78]	Minor
	Assumptions	Redundancy is a well-explored subject, assumptions only refer to data fusion design [33], which is also well-known	Minor
	Data	Some data is only available for other domains (e.g. Dynamic Positioning) [79], but data pertaining to use of different, redundant and advanced sensors is lacking	Moderate
	Consensus	Experts agree that this is necessary and profitable [2,10,75,80,81]	Minor
Wide-range sensors	Phenomena	Many specimens are available on the market, working principles are known [2]	Minor
	Model	Wide-range sensors will provide additional data, overlapping with others [33,81–83]	Minor
	Assumptions	Innovative industry of autonomous shipping shall use highly-advanced sensors once developed [82,84]	Minor
	Data	Although sensors are in fact available, little data is available on their long-time operation in varying conditions [33]	Moderate
	Consensus	Some experts argue that it is more beneficial to use greater number of simpler sensors [74]	Moderate
Highly-sensitive sensors	Phenomena	Numerous specimens are available on the market, working principles of which are known [2]	Minor
	Model	Highly-sensitive sensors can provide data of a required accuracy [10,85]	Minor
	Assumptions	Most of sensors used nowadays can provide sufficient data for vessels' operations [10]	Minor
	Data	Sensors are constantly being improved, but data regarding their long-time performance varies in quality [2]	Moderate
	Consensus	Experts agree that highly-advanced sensors shall be used [82]	Minor

performance of the system in question have been sought. Rather than that, the study consisted of seeking solutions by the implementation of which the safety can be ensured. This was done by reviewing a complex network of mutual interactions among the system's components. The advantage of such an approach over previously used ones lies in the possibility to perform the study in relation to subject, of which there is insufficient or no quantitative data, as is the case of AMV. Applying reliability-based methods to achieve it would mean the necessity to analyse a reliability structure of the system, which cannot be determined at this point. Nevertheless, the results of the study are in general consistent with those performed before - in their parts concerning potential hazards and solutions.

4.1.2. Human error

Firstly, a relatively high number of potential causes for control actions' inadequacy can be attributed to human error. Although it is understandable that human operators might have little control over a vessel operating in an autonomous mode, hazards can still result from human interactions with other system's components [22], see for example control actions #1-10c and 34 in Appendices. Those can be associated with the design process [56] (#14a,16,20,21), software development (#26,32,33), data interpretation (#9,40), limits' settings [46,108] (#34) or even illegal activities [6,109]. Humans' impact on the system's safety, although not evident from the safety assessment's results, will exist as humans will maintain an influence on its performance, one way or another [3]. Therefore, a relatively high number of mitigation measures are focused on liveware (see Fig. 4) and range from procedures on legislation implementation through operational trainings.

4.1.3. Technical considerations

Secondly, technical considerations will have a great importance to the safety of autonomous vessels. These pertain to both software and hardware, which must be reliable and efficient. Consider collision avoidance and assume that the applicable rules are not amended (some scholars raise concern that the implementation of autonomous vessels may require such amendments, see for example [29]). In order to prevent two ships from colliding, a set of conditions must be met. Two vessels shall not violate the minimum Closest Point of Approach (CPA), meaning that the distance between them shall at no circumstances be less than a certain value [110]. This limit can vary depending on circumstances, just to name a few: vessels' relative speed, area of navigation or weather conditions, [111–117]. The existence of a risk of collision must be determined by constantly calculating and monitoring the CPA and other proximity indicators that help to determine the situational awareness, e.g. the relative location of the target ship with respect to the own one, the rate of change for relative speed and course of the other ship.

In order to achieve successful collision avoidance, the other vessel's presence must first be detected (#31) and its elements of movement must be calculated. This requires sensors to be reliable and data processing algorithms to be accurate (#37), accounting for the good seamanship practice. If more than one sensor is involved, data fusion issues apply. Assuming that the CPA and other indicators are calculated correctly and are below the minimum acceptable threshold (#35), certain action (#26) shall be taken by one of the vessels so as to reduce the risk of collision, as prescribed by COLREG, [118,119]. Therefore, the 'own' vessel shall analyse the data and determine if she is the 'give-way'. This will depend on many factors, just to name the relative bearing and speed or both ships' navigational status. Action required to avoid collision (e.g. heading or speed alteration) must be calculated together with its feasibility [120] (avoiding collision with one vessel might lead to colliding with another one or grounding). The decision must be made and executed by the actuation of either the rudder angle or the main engine's revolutions. The effectiveness of the action taken shall be monitored [121,122]. On top of that, it might turn out that the object detected by radar was not in fact the vessel but a floating container for instance, and collision avoidance rules did not even apply for the situation.

This rather simple example highlights the importance of applying a holistic approach to an autonomous vessels' system's design. Here, all of its components must 'cooperate': humans set proper thresholds for proximity indicators (#34), sensors detect the object, algorithms process the data and create decisions, which are then executed by actuators. These interactions are sometimes extremely complex and must not be addressed on a linear basis [8,22].

4.1.4. Reliability and maintenance

Further on technical considerations, ensuring the sufficient reliability of equipment, including sensors as well as any other devices (#14a-17,20-22), can be a major issue. Nowadays, the crew on board a ship can perform maintenance and repairs, also as a contingency. This will not be possible for unmanned vessels, which must be adequately designed so as to survive any potentially hazardous mechanical breakdown or software malfunction [30]. These two issues include system's inability to establish both-way communication between SBCC and the vessel. For such circumstances, a fail-to-safe mechanism shall be built-in to the system in order to prevent failure propagation [5,11] and allow for damage control with the assistance of other assets, salvage companies for instance. Efforts in damage control are reflected in

Table 6
Detailed refinement of uncertainty levels in mitigation measure's elaboration – control action #21. [87–107].

Mitigation measure	Uncertainty category	Description	Result (uncertainty level)
Rigorous maintenance regime	Phenomena	Maintenance procedures are well-known, however not for such complex systems with prolonged maintenance-free periods [5,44,86,87]	Moderate
	Model	Model of applying maintenance procedures can be established but will depend on data on equipment reliability, which might not be solid [22,30]	Moderate
	Assumptions	It is assumed that decent procedures or algorithms can be elaborated [88], but this requires experience-based data	Significant
	Data	Data pertaining to maintenance needs of particular equipment are available, but assumes constant supervision of qualified personnel [88]	Moderate
	Consensus	It is agreed that rigorous maintenance regime must be implemented [88]	Minor
Redundant equipment	Phenomena	Well-recognized as a way of ensuring particular subsystem's reliability [44,75,76]	Minor
	Model	Consequences of applying it into autonomous shipping are rather well-comprehended: it will increase investment costs [76,77] but will also help providing necessary data, possibly by use of data fusion algorithms [78]	Minor
	Assumptions	Redundancy is a well-explored subject, assumptions only refer to data fusion design [33], which is also well-known	Minor
	Data	Some data is only available for other domains (e.g. Dynamic Positioning) [79]	Minor
	Consensus	Experts agree that this is necessary and profitable [2,10,75,80,81]	Minor
Resilience-based design	Phenomena	Resilience engineering is a relatively novel approach [89] and thus not widely applied [90]	Moderate
	Model	Models are lacking and those available usually pertain to domains other than shipping [89,91,92]	Moderate
	Assumptions	Great number of assumptions must be made, relating to system's actual structure [22]	Significant
	Data	Data on application of resilience engineering in shipping is lacking, some attempts have been made in other domains [92]	Significant
	Consensus	Experts in autonomous shipping refer to concepts similar to resilience claiming that it must be built-in [30,86,93]	Minor
Procedures on consumables' management	Phenomena	Such procedures have been successfully implemented in many shipping companies [94]	Minor
	Model	Model is relatively simple and well-developed [94,95]	Minor
	Assumptions	These procedures would be based on existing ones so assumptions only pertaining to different model of operations need to be made [31,44,53]	Minor
	Data	Data related to procedures on consumables' management can be sensitive but is rather simple to calculate [95]	Minor
	Consensus	Experts agree that this is necessary and profitable [96]	Minor
Capacity surpluses by design	Phenomena	Phenomena of including necessary surpluses by design is well recognized [97]	Minor
	Model	Design surpluses are successfully applied to many modern systems	Minor

(continued on next page)

Table 6 (*continued*)

		[98]	
	Assumptions	Relative novelty of unmanned shipping technology implies that expected levels of certain parameters remain unknown, therefore the surpluses are also burdened with uncertainties [93]	Significant
	Data	Data can be possible to obtain in relation to 'manned' shipping but its applicability to AMVs can be questioned	Moderate
	Consensus	Issue has been raised in few papers [97,98] but exact application to unmanned shipping has not been addressed	Moderate
Extensive testing	Phenomena	Testing is being performed for a variety of machinery and processes and is well-understood [45,99–102]	Minor
	Model	Testing's influence on safety is clear [45,99–102]	Minor
	Assumptions	Exact scope of tests to be carried out is yet to be determined as it will vary from 'manned' shipping [55]	Moderate
	Data	Data is in favour of the statement that tests' results help improve safety performance [99–102]	Minor
	Consensus	It is widely agreed that commissioning tests are essential to safety [27,55,86]	Minor
Implementation of leading performance indicators	Phenomena	Key Performance Indicators (KPIs) are relatively novel and not widely applied means of assessing safety, although based on promising foundations [103]	Moderate
	Model	KPIs might be well-suited for identifying breakdowns and failures but have sparsely been applied in shipping to date [91,104]	Moderate
	Assumptions	Assumptions are fragile as actual studies on KPIs in unmanned shipping are yet to be carried out [105]	Significant
	Data	KPIs can more easily be applied to systems for which quantitative data is available or at least its actual layout is known [52,106]	Significant
	Consensus	Not many mentions suggesting application of KPIs with relation to AMV could be found [88]	Moderate

recently published requirements for passenger ships' safe return to port, see for example [123]. These can be a starting point for the elaboration of future rules of classification for unmanned ships' resilience engineering.

4.1.5. Hazards

Recent research reveals that some accident causal categories can have a greater impact on potentially reducing the safety of autonomous vessels than others, [11,124]. For instance, software or hardware malfunctions can be more vital to safety than errors occurring within resource management. This can be attributed to the fact that wrongdoings made at lower levels of organisation hierarchy can be more difficult to timely identify and correct (especially in autonomous operations). In this context, errors occurring within legal or organisational framework can have an impact on the occurrence of technical malfunctions, but not necessarily result in an immediate danger to the system. On the other hand, in daily operations, software or hardware malfunctions can propagate on few other components, but the results of such propagation can be both immediate and devastating.

Moreover, one can notice that for numerous control actions, their inadequacy can lead to the emergence of a large number of hazards (#1-7c,9-10c,14a-17,34-41). This can be attributed to the relatively low detail level of the analysis and the complexity of the system in question where, under conditions of autonomous operation, failures can propagate rapidly.

Analysing the control actions' catalogue did not help identify any new hazard to be added to the list as given within Table 3. This may be due to the fact that the analysis has been performed in a very low level of detail and that the initial list has been refined in cooperation with experts in the field who have included all the system-level hazards they have ever encountered. Possibly, the list of hazards could be extended once more information about the system layout is available and its specific processes can be analysed more thoroughly.

4.1.6. Systemic approach summary

The innovativeness of the AMVs' system and confusion regarding its actual, future layout force the safety analysis to be based primarily on a literature review. Unlike conventional shipping, there are very few experts who can be elicited in order to gain their impressions regarding autonomous shipping. And even if this can be achieved, such persons are in majority involved in ongoing commercial projects on system development and thus can be biased or unable to share their expertise. Moreover, most of the safety analyses performed to dates were based on a probabilistic paradigm. The study herein is based on a different approach, a systemic one, although built on the foundations of previous ones as most of the content is inspired by the results of a 'probabilistic' literature review. Therefore, results are to a large extent consistent with those achieved previously.

However, an application of systemic approach helped view the system holistically, systematise the mutual relationships between its components of a different nature and elaborate some solutions on preventing or otherwise handling the potential inadequacies of these interactions. To date, research focused on mitigation measures was rather scarce or limited [30,37,125,126] with authors generally focusing on hazard identification [5–7] rather than on seeking diversified solutions to thereby-defined problems. In this context, the control actions' descriptions as given in Appendices can be viewed as a compilation of recommendations on the implementation of safety-critical solutions for specified problems.

Nevertheless, some uncertainties exist herein and must be discussed.

4.2. Uncertainties

Within the framework introduced in Section 2.2.4., no resultant uncertainty is calculated based on the magnitudes of uncertainty within a particular category. Instead, the degree of belief is communicated in such a way that future system developers and decision-makers can easily recognise aspects requiring more attention in order to reduce the uncertainties. For instance, a more detailed inspection of the control actions' catalogue (Appendices) and uncertainty analysis results (Figs. 5–7) leads to the conclusion that software covering operations within the vessel or communication require further study. The

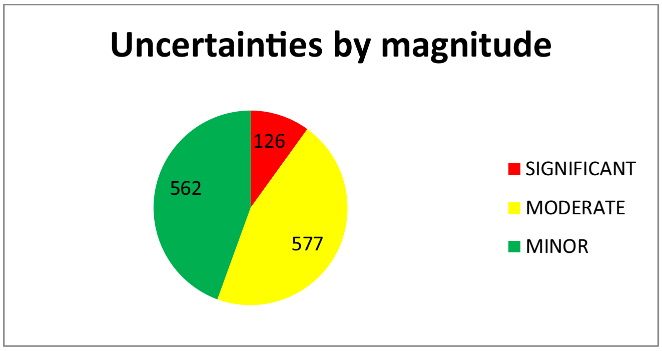


Fig. 8. Global breakdown of uncertainties by magnitude.

percentage of 'significant uncertainty' within this group is notable, see Fig. 6. This may be attributed to the fact that the other two groups of mitigation measures (liveware and hardware) to be implemented for autonomous vessels are predominantly similar to those existing in present systems and are thus well-explored in academia and industry. Although the future design of unmanned vessel is expected to differ from this of manned one in many aspects [30], certain solutions applied in the latter will most likely be implemented. This reduces the uncertainties pertaining to hardware and organisational issues, but not the software which is to account for fully autonomous operations. However, as argued in [46], different kinds of malfunctions and errors can affect virtually every aspect of an unmanned vehicle's design and operation and shall therefore be counteracted.

Moreover, a relatively big number of 'significant uncertainty' can be observed in two uncertainty categories, related to empirical data and assumptions, see Fig. 6. This can result from the fact that virtually no data pertaining to unmanned merchant vessels' operational performance is available to date as they are still in the concept phase of technology development and none has entered into operation. Similarly, assumptions for the entire study were based on the information available from literature, experts' elicitation and Authors' previous experience with shipping in its 'manned' form. Whether these assumptions can be projected on autonomous shipping is a question of what shape the latter will actually take. This in turn will be the result of a long design process, further improvements and can vary for prototypes implemented by different companies.

Nevertheless, the total number of 'significant uncertainties' assigned is rather small in compare to 'moderate' and 'minor' ones, as can be seen in Fig. 8. One potential reason for it can be that while the general concept of AMVs' design and operation is quite well understood, its details remain unknown. The question remains open whether the data or models describing existing systems can be used to assess a similar yet highly innovative one, as is the case of an autonomous vessel. Such information as well as user experience and tacit knowledge in the form of experts' views should be used with caution as not all aspects of different systems' operation and design can be sufficiently similar to justify its use.

Total number of uncertainty levels assigned to the mitigation measures' elaboration process as depicted in Fig. 8 can also result from how the levels of uncertainty are defined in Table 2.

Uncertainty analysis as applied is not free from shortcomings. Firstly, a subjectivity of judgments pertaining to the magnitude of uncertainty is not eliminated. For instance, it can be difficult for an analyst to distinguish between 'high' and 'medium' level of phenomena's understanding [71]. In such circumstances, though, cautionary, or precautionary principles could apply. On the other hand, the very foundation of the presented method lies within describing the extent to which an analyst is convinced that his/her judgments are correct, instead of calculating that from a hard evidence. Similar effects can be noticed in many of the qualitative methods of safety assessment [127].

Secondly, the method does not ascertain that all potential hazard scenarios have been addressed. Instead, only these mitigation measures that have been elaborated could be further refined into statements pertaining to the uncertainties. The potential for black swans is thus not eliminated [67]. Although system-theoretic approach is said to better model systems' safety performance than previously used methods [21], it still does not guarantee the completeness nor accuracy of the analysis [128] (see also Fig. 2). Uncertainty assessment can therefore be incomplete because its input as elicited from experts can be incomplete. Herein, since no quantitative analysis can be performed for now, only a more detailed experts' elicitation could be beneficial to resolve black swans issues pertaining to hazards threatening the safe and efficient operations of autonomous ships. Moreover, experts might assist in evaluating the actual feasibility of the mitigation measures.

5. Conclusions

In the course of system-theoretic analysis of an AMVs' safety, a list of hazards, hazardous scenarios and solutions pertaining to ensuring such vessel's safety has been compiled. The aim was to apply the system theory to improve the safety performance of these vessels, which are scheduled for implementation into the global shipping industry within the foreseeable future. By formulating the said hazard mitigation measures, we accomplished the very goal of our research.

Nevertheless, any system shall be constantly analysed throughout its design and operation. Therefore, the given analysis shall be considered merely as one of the first steps in this process. Further analysis shall be conducted as soon as more information regarding the unmanned merchant vessels is available. The actual design of the system and empirical data on its safety performance can be of the highest importance while expert elicitation methods might prove beneficial in addressing uncertainties.

The opportunity of analysing a system that is in an early phase of development was also used to refine the method of assessing some of the uncertainties present in system-theoretic approach.

The magnitudes of uncertainty were assigned as supported by background knowledge available at the present stage of AMVs' technology development. As it progresses, more information would become available to analysts, and uncertainties could be re-evaluated. The purpose of the presented uncertainty analysis method is to communicate which parts of the future system require further, more detailed study with respect to the reduction of the uncertainties and improvement of safety. Communicating the magnitude of uncertainties pertaining to particular aspects of system's operation can attract future system developers' attention to the need of collecting additional data or the improvement of some models.

The results of our study indicate that the developers of future AMVs might wish to concentrate their effort on software development and validation as this part of the system appears to be hampered by the most significant uncertainties pertaining to its safety performance.

One of the yet-to-be resolved issues with safety analysis and resulting uncertainties assessment is their potential incompleteness. Furthermore, the usefulness of the hereby elaborated safety recommendations and uncertainties-related data should be evaluated as soon as the system in question is in fact designed and more empirical data becomes available. Within these aspects lies the potential for further study.

Acknowledgements

The authors appreciate the financial contributions from Finnish Funding Agency for Technology Innovation (TEKES), since this research was co-funded by the Advanced Autonomous Waterborne Application Initiative (AAWA) project (project number 5166/31/2014; duration 01.01.2015–30.06.2017). The views expressed remain solely those of the authors. Additionally, the second author appreciates the financial contributions from the Polish Ministry of Science and Higher Education, grant number DS/442/2017, duration 2017–2019.

We are grateful to Mr. Risto Tuominen and Mr. Risto Tiusanen as well as other experts for their valuable advice on the model of safety control structure and a high-level hazards' list. Mr. Owen Jones assisted us in the necessary English proofreading.

We also wish to express our gratitude to three anonymous reviewers whose valuable comments allowed us to improve the initial version of the manuscript.

Supplementary material

Supplementary material associated with this article can be found, in the online version, at http://dx.doi.org/10.1016/j.ress.2018.05.019.

References

[1] Jokioinen E. Remote and autonomous ships-the next steps. London: AAWA; 2016.
[2] Kretschmann L, Mcdowell H, Rødseth ØJ, Fuller BS, Noble H, Horahan J. Maritime unmanned navigation through intelligence in networks – quantitative assessment. 2015.
[3] Porathe T. A navigating navigator onboard or a monitoring operator ashore? Towards safe, effective, and sustainable maritime transportation: findings from five recent EU projects. Transp Res Procedia 2016;14:233–42. http://dx.doi.org/10.1016/j.trpro.2016.05.060.
[4] Kretschmann L, Rødseth ØJ, Tjora Å, Fuller BS, Noble H, Horahan J. Maritime unmanned navigation through intelligence in networks – qualitative assessment. Hamburg: 2015.
[5] Rødseth ØJ, Burmeister H-C. Risk assessment for an unmanned merchant ship. TransNav Int J Mar Navig Saf Sea Transp 2015;9:357–64. http://dx.doi.org/10.12716/1001.09.03.08.
[6] Hogg T, Ghosh S. Autonomous merchant vessels: examination of factors that impact the effective implementation of unmanned ships. Aust J Marit Ocean Aff 2016;8:206–22. http://dx.doi.org/10.1080/18366503.2016.1229244.
[7] MacKinnon SN, Man Y, Lundh M, Porathe T. Command and control of unmanned vessels: keeping shore based operators in-the-loop. Proceedings of the ATENA conferences system, NAV 2015 eighteenth international conference on ships and shipping research. 2015.
[8] Wróbel K, Krata P, Montewka J, Hinz T. Towards the development of a risk model for unmanned vessels design and operations. TransNav Int J Mar Navig Saf Sea Transp 2016;10:267–74. http://dx.doi.org/10.12716/1001.10.02.09.
[9] Krata P, Szłapczyńska J. Weather hazard avoidance in modeling safety of motor-driven ship for multicriteria weather routing. TransNav 2012;6:71–8.
[10] Burmeister H-C, Bruhn WC, Rødseth ØJ, Porathe T. Can unmanned ships improve navigational safety? Proceedings of the transport research arena. Paris; 2014.
[11] Wróbel K, Montewka J, Kujala P. Towards the assessment of potential impact of unmanned vessels on maritime transportation safety. Reliab Eng Syst Saf 2017;165:155–69. http://dx.doi.org/10.1016/j.ress.2017.03.029.
[12] Kongsberg. YARA and KONGSBERG enter into partnership to build world's first autonomous and zero emissions ship 2017. https://www.km.kongsberg.com/ks/web/nokbg0238.nsf/AllWeb/98A8C576AEFC85AFC125811A0037F6C4?OpenDocument (accessed May 25, 2017).
[13] Heikkilä E, Tuominen R, Tiusanen R, Montewka J, Kujala P. Safety qualification process for an autonomous ship prototype – a goal-based safety case approach. In: Weintrit A, editor. Proceedings of the twelfth international conference marine navigation and safety of sea transportation, TransNav. CRC Press; 2017. p. 365–70.
[14] Endrina N, Rasero JC, Konovessis D. Risk analysis for RoPax vessels: a case of study for the strait of gibraltar. Ocean Eng 2018;151:141–51. http://dx.doi.org/10.1016/J.OCEANENG.2018.01.038.
[15] Bjerga T, Aven T, Zio E. Uncertainty treatment in risk analysis of complex systems: the cases of STAMP and FRAM. Reliab Eng Syst Saf 2016;156:203–9. http://dx.doi.org/10.1016/j.ress.2016.08.004.
[16] Papanikolaou A, editor. Risk-based ship design Berlin, HeidelbergBerlin Heidelberg: Springer; 2009. http://dx.doi.org/10.1007/978-3-540-89042-3.
[17] Montewka J, Goerlandt F, Innes-Jones G, Owen D, Hifi Y, Puisa R. Enhancing human performance in ship operations by modifying global design factors at the design stage. Reliab Eng Syst Saf 2017;159:283–300. http://dx.doi.org/10.1016/j.ress.2016.11.009.
[18] 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. http://dx.doi.org/10.1016/j.marpolbul.2016.03.071.
[19] United States Coast Guard. Ports and waterways safety assessment (PAWSA) 2005.
[20] Trbojevic VM, Carr BJ. Risk based methodology for safety improvements in ports. J Hazard Mater 2000;71:467–80. http://dx.doi.org/10.1016/S0304-3894(99)00094-1.
[21] Altabbakh H, AlKazimi MA, Murray S, Grantham K. STAMP – holistic system safety approach or just another risk model? J Loss Prev Process Ind 2014;32:109–19. http://dx.doi.org/10.1016/j.jlp.2014.07.010.
[22] Leveson NG. Engineering a safer world – Systems thinking applied to safety. Cambridge, MA: MIT Press; 2011.
[23] Aps R, Fetissov M, Goerlandt F, Kopti M, Kujala P. STAMP-Mar based safety management of maritime navigation in the Gulf of Finland (Baltic Sea). Proceedings of the European navigation conference 2016. http://dx.doi.org/10.1109/EURONAV.2016.7530538.
[24] Valdez Banda OA, Goerlandt F. A STAMP-based approach for designing maritime safety management systems. Saf Sci 2018;109:109–29. http://dx.doi.org/10.1016/j.ssci.2018.05.003.
[25] Abdulkhaleq A, Lammering D, Wagner S, Röder J, Balbierer N, Ramsauer L, et al. A systematic approach based on STPA for developing a dependable architecture for fully automated driving vehicles. Proceedings of the forth European STAMP workshop 179. Elsevier Ltd; 2016. p. 41–51. http://dx.doi.org/10.1016/j.proeng.2017.03.094.
[26] Abrecht B. Systems theoretic process analysis (STPA) of an offshore supply vessel dynamic positioning system. PhD thesis. Lexington, MA: 2016.
[27] Salmon PM, Cornelissen M, Trotter M. Systems-based accident analysis methods: a comparison of Accimap, HFACS, and STAMP. Saf Sci 2012;50:1158–70. http://dx.doi.org/10.1016/j.ssci.2011.11.009.
[28] Ortiz de Rozas JM. The production of unmanned vessels and its legal implications in the maritime industry. University of Oslo; 2014.
[29] Van Hooydonk E. The law of unmanned merchant shipping – an exploration. J Int Marit Law 2014;20:403–23.
[30] Rødseth ØJ, Burmeister H-C. New ship designs for autonomous vessels. Trondheim: 2015.
[31] Burmeister H-C, Bruhn W, Rødseth ØJ, Porathe T. Autonomous unmanned merchant vessel and its contribution towards the e-navigation implementation: the MUNIN perspective. Int J E-Navigation Marit Econ 2014;1:1–13. http://dx.doi.org/10.1016/j.enavi.2014.12.002.
[32] Porathe T, Prison J, Man Y. Situation awareness in remote control centres for unmanned ships. Proceedings of the human factors in ship design and operation. London; 2014.
[33] Rødseth ØJ, Tjora Å. A System Architecture for an Unmanned Ship. Proceedings of the thirteenth international conference on computer and IT applications in the maritime industries (COMPIT 2014). 2014. p. 291–302.
[34] Bruhn WC, Burmeister H-C, Long MT, Moræus JA. Conducting look-out on an unmanned vessel: Introduction to the advanced sensor module for MUNIN's autonomous dry bulk carrier. Integr. Ship's Inf. Syst. 2014.
[35] Ahmed YA, Hasegawa K. Automatic ship berthing using artificial neural network trained by consistent teaching data using nonlinear programming method. Eng Appl Artif Intell 2013:1–18. doi:10.1016/j.engappai.2013.08.009.
[36] Patriarca R, Bergström J. Modelling complexity in everyday operations: functional resonance in maritime mooring at quay. Cogn Technol Work 2017:1–19. doi:10.1007/s10111-017-0426-2.
[37] Van Den Boogaard M, Feys A, Overbeek M, Le Poole J, Hekkenberg R. Control concepts for navigation of autonomous ships in ports. Proceedings of the tenth symposium high-performance marine vehicles. 2016.
[38] Rødseth ØJ, Lee K. Secure communication for e-navigation and remote control of unmanned ships. In: Volker B, editor. Proceedings of the fourteenth conference on computer and IT applications in the maritime industries. 2015. p. 44–56.
[39] Wärtsilä. Wärtsilä successfully tests remote control ship operating capability. https://www.wartsila.com/media/news/01-09-2017-wartsila-successfully-tests-remote-control-ship-operating-capability; 2017 (accessed October 19, 2017).
[40] Höyhtyä M, Ojanperä T, Mäkelä J, Ruponen S, Järvensivu P. Integrated 5G satellite-terrestrial systems: use cases for road safety and autonomous ships. Proceedings of the twenty-third Ka and broadband communications conference. 2017.
[41] Bitner M, Starościk R, Szczerba P. Czy robot zabierze ci pracę? Sektorowa analiza komputeryzacji i robotyzacji europejskich rynków pracy. Warszawa: 2014.
[42] Lee TK. Liability of autonomous ship: The scandinavian perspective. University of Oslo; 2016.
[43] LR. Cyber-enabled ships ShipRight procedure – autonomous ships. Southampton: 2016.
[44] Rødseth ØJ, Nordahl H. Definitions for autonomous merchant ships. 2017.
[45] Blanke M, Henriques M, Bang J. A pre-analysis on autonomous ships. Kongens Lyngby: 2017.
[46] Stokey R, Austin T, von Alt C, Purcell M, Goldsborough R, Forrester N, et al. AUV bloopers or why murphy must have been an optimist: a practical look at achieving mission level reliability in an autonomous underwater vehicle. Proceedings of the eleventh international symposium on unmanned untethered submersible technology (UUST '99). 1999. p. 32–40.
[47] Kalra N, Paddock SM. Driving to safety: How many miles of driving would it take to demonstrate autonomous vehicle reliability? Transp Res Part A Policy Pract 2016;94:182–93. http://dx.doi.org/10.1016/j.tra.2016.09.010.
[48] Kazaras K, Kontogiannis T, Kirytopoulos K. Proactive assessment of breaches of safety constraints and causal organizational breakdowns in complex systems: a joint STAMP-VSM framework for safety assessment. Saf Sci 2014;62:233–47. http://dx.doi.org/10.1016/j.ssci.2013.08.013.
[49] Asare P, Lach J, Stankovic JA. FSTPA-I: a formal approach to hazard identification via system theoretic process analysis. Proceedings of the ACM/IEEE forth international conference on cyber-physical systems 2013. http://dx.doi.org/10.1109/ICCPS.2013.6604009.
[50] Kwon Y. System theoretic safety analysis of the Sewol-Ho ferry accident in South Korea. Massachusetts Institute of Technology; 2016.
[51] Reason J. The contribution of latent human failures to the breakdown of complex systems. Philos Trans R Soc London B Biol Sci 1990;327:475–84.
[52] Verma AK, Ajit S, Karanki DR. Reliability and safety engineering. London: Springer-Verlag; 2010.

[53] Dokas IM, Feehan J, Imran S. EWaSAP: an early warning sign identification approach based on a systemic hazard analysis. Saf Sci 2013;58:11–26. http://dx.doi.org/10.1016/j.ssci.2013.03.013.

[54] Burmeister HC, Bruhn WC, Walther L. Interaction of harsh weather operation and collision avoidance in autonomous navigation. TransNav Int J Mar Navig Saf Sea Transp 2015;9:31–40. http://dx.doi.org/10.12716/1001.09.01.04.

[55] Lee S-M, Kwon K-Y, Joh J. A fuzzy logic for autonomous navigation of marine vehicle satisfying COLREG guidelines. Int J Control Autom Syst 2004;2:171–81.

[56] Ahvenjärvi S. The human element and autonomous ships. TransNav Int J Mar Navig Saf Sea Transp 2016;10:517–21. http://dx.doi.org/10.12716/1001.10.03.18.

[57] 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 Manuf 2015;3:2674–81. http://dx.doi.org/10.1016/j.promfg.2015.07.635.

[58] Kongsberg Maritime. Autonomous ship project, key facts about YARA Birkeland. https://www.km.kongsberg.com/ks/web/nokbg0240.nsf/AllWeb/4B8113B707A50A4FC125811D00407045?OpenDocument; 2017 (accessed October 30, 2017).

[59] Lockwood F, Kent T, Paul J, Shenoi A, Westgarth R, O'dell M, et al. Global marine technology trends 2030: autonomous systems. 2017.

[60] Kaplan S, Garrick BJ. On the quantitative definition of risk. Risk Anal 1981;1:11–27. http://dx.doi.org/10.1111/j.1539-6924.1981.tb01350.x.

[61] Goerlandt F, Reniers G. On the assessment of uncertainty in risk diagrams. Saf Sci 2016;84:67–77. http://dx.doi.org/10.1016/j.ssci.2015.12.001.

[62] Goerlandt F, Khakzad N, Reniers G. Validity and validation of safety-related quantitative risk analysis: a review. Saf Sci 2016. http://dx.doi.org/10.1016/j.ssci.2016.08.023.

[63] Goerlandt F, Kujala P. On the reliability and validity of ship–ship collision risk analysis in light of different perspectives on risk. Saf Sci 2014;62:348–65.

[64] Aven T, Heide B. Reliability and validity of risk analysis. Reliab Eng Syst Saf 2009;94:1862–8. http://dx.doi.org/10.1016/j.ress.2009.06.003.

[65] Rao KD, Kushwaha HS, Verma AK, Srividya A. Quantification of epistemic and aleatory uncertainties in level-1 probabilistic safety assessment studies. Reliab Eng Syst Saf 2007;92:947–56. http://dx.doi.org/10.1016/j.ress.2006.07.002.

[66] Montewka J, Goerlandt F, Kujala P. On a systematic perspective on risk for formal safety assessment (FSA). Reliab Eng Syst Saf 2014;127:77–85. http://dx.doi.org/10.1016/j.ress.2014.03.009.

[67] Flage R, Aven T. Emerging risk – conceptual definition and a relation to black swan type of events. Reliab Eng Syst Saf 2015;144:61–7. http://dx.doi.org/10.1016/j.ress.2015.07.008.

[68] Flage R, Aven T. Expressing and communicating uncertainty in relation to quantitative risk analysis. Reliab Risk Anal Theory Appl 2009;2:9–18.

[69] Pruyt E. Dealing with uncertainties? Combining system dynamics with multiple criteria decision analysis or with exploratory modelling. Policy Anal 2007:1–22.

[70] Flage R, Aven T. Comments to the article by Goerlandt & Reniers titled "On the assessment of uncertainty in risk diagrams" [Safety Sci. 84 (2016) 67–77]. Saf Sci 2017;98:9–11. http://dx.doi.org/10.1016/j.ssci.2017.04.007.

[71] Goerlandt F. Evidence assessment schemes for semi-quantitative risk analyses: a response to Roger Flage and Terje Aven (Letter to the editor). Saf Sci 2017;98:12–6. http://dx.doi.org/10.1016/j.ssci.2017.04.008.

[72] Allianz. Safety and shipping review 2015. Munich: 2015.

[73] Rødseth ØJ, Tjora Å, Baltzersen P. Maritime unmanned navigation through intelligence in networks – architecture specification. Trondheim: 2013.

[74] Pasman HJ, Rogers WJ, Mannan MS. Risk assessment: what is it worth? Shall we just do away with it, or can it do a better job? Saf Sci 2017;99:140–55. http://dx.doi.org/10.1016/j.ssci.2017.01.011.

[75] Bertram Volker. Technologies for low-crew/no-crew ships. Forum Captain Computer IV. Brest: ENSIETA; 2002.

[76] Wild G, Murray J, Baxter G. Exploring Civil Drone Accidents and Incidents to Help Prevent Potential Air Disasters. Aerospace 2016;3(3):22. http://dx.doi.org/10.3390/aerospace3030022.

[77] Fiondella L, Lin Y, Pham H, Chang P, Li C. A confidence-based approach to reliability design considering correlated failures. Reliab Eng Syst Saf 2017;165:102–14. http://dx.doi.org/10.1016/j.ress.2017.03.025.

[78] Fagnant DJ, Kockelman K. Preparing a nation for autonomous vehicles: opportunities, barries and policy recommendations for capitalizing on self-driven vehicles. Transp Res Part A 2013:1–20.

[79] Eriksson R, Friebe A. Challenges for autonomous sailing robots. Proceedings of the machine vision and image processing conference IEEE; 2007. p. 67–73. http://dx.doi.org/10.1109/IMVIP.2007.46.

[80] Rokseth B, Utne IB, Vinnem JE. Deriving verification objectives and scenarios for maritime systems using the systems-theoretic process analysis. Reliab Eng Syst Saf 2018;169:18–31. http://dx.doi.org/10.1016/j.ress.2017.07.015.

[81] Özgüner Ü, Stiller C, Redmill K. Systems for safety and autonomous behavior in cars: the DARPA grand challenge experience. Proc IEEE 2007;95:397–412. http://dx.doi.org/10.1109/JPROC.2006.888394.

[82] Luettel T, Himmelsbach M, Wuensche H-J. Autonomous ground vehicles—concepts and a path to the future. Proc IEEE 2012;100:1831–9. http://dx.doi.org/10.1109/JPROC.2012.2189803.

[83] Campbell S, Naeem W, Irwin GW. A review on improving the autonomy of unmanned surface vehicles through intelligent collision avoidance manoeuvres. Annu Rev Control 2012;36:267–83. http://dx.doi.org/10.1016/j.arcontrol.2012.09.008.

[84] Łebkowski A. The Concept of Autonomous Coastal Transport. In: Weintrit A, Neumann T, editors. Proceedings of the twelfth international conference marine navigation and safety of sea transportation, TransNav 2017. p. 351–7. http://dx.doi.org/10.1201/9781315099132-61.

[85] Perera LP, Carvalho JP, Guedes Soares C. Autonomous guidance and navigation based on the COLREGs rules and regulations of collision avoidance. In: Guedes Soares C, Parunov J, editors. Proceedings of the international workshop "advanced ship design for pollution prevention". Taylor & Francis Group; 2009. p. 205–16.

[86] Ludvigsen M, Sørensen AJ. Towards integrated autonomous underwater operations for ocean mapping and monitoring. Annu Rev Control 2016;42:145–57. http://dx.doi.org/10.1016/j.arcontrol.2016.09.013.

[87] Man Y, Lundh M, Porathe T. Seeking harmony in shore-based unmanned ship handling-from the perspective of human factors, what is the difference we need to focus on from being onboard to onshore? Adv Hum Asp Transp Part I 2014;7:231.

[88] Ahmadi A. Aircraft scheduled maintenance programme development decision support methodologies and tools. Lulea University of Technology; 2010.

[89] Rødseth H, Brage M. Maintenance Management for Unmanned Shipping. In: Volker B, editor. Proceedings of the thirteenth conference on computer and IT applications in the maritime industries COMPIT '14. 2014. p. 277–90.

[90] Righi AW, Saurin TA, Wachs P. A systematic literature review of resilience engineering: Research areas and a research agenda proposal. Reliab Eng Syst Saf 2015;141:142–52. http://dx.doi.org/10.1016/j.ress.2015.03.007.

[91] Patriarca R, Bergström J, Di Gravio G, Costantino F. Resilience engineering: current status of the research and future challenges. Saf Sci 2018;102:79–100. http://dx.doi.org/10.1016/j.ssci.2017.10.005.

[92] Schröder-Hinrichs J-U, Praetorius G, Graziano A, Kataria A, Baldauf M. Introducing the concept of resilience into maritime safety. Proceedings of the sixth resilience engineering symposium. Resilience Engineers Association; 2015. p. 1–7.

[93] Sadeghzadeh I, Zhang Y. A review on fault-tolerant control for unmanned aerial vehicles (UAVs). St. Louis, MO: American Institute of Aeronautics and Astronautics; 2011. p. 1–12. http://dx.doi.org/10.2514/6.2011-1472. Infotech@aerosp. 2011.

[94] Jalonen R, Tuominen R, Wahlström M. Safety of unmanned ships. Helsinki: 2017.

[95] Bialystocki N, Konovessis D. On the estimation of ship's fuel consumption and speed curve: a statistical approach. J Ocean Eng Sci 2016;1:157–66. http://dx.doi.org/10.1016/j.joes.2016.02.001.

[96] Krata P, Szłapczyńska J. Ship weather routing optimization with dynamic constraints based on reliable synchronous roll prediction. Ocean Eng 2018;150:124–37. http://dx.doi.org/10.1016/j.oceaneng.2017.12.049.

[97] Trodden DG, Murphy AJ, Pazouki K, Sargeant J. Fuel usage data analysis for efficient shipping operations. Ocean Eng 2015;110:75–84. http://dx.doi.org/10.1016/j.oceaneng.2015.09.028.

[98] Frąckowiak W. Struktury niezawodnościowe systemów napędowych statków z uwzględnieniem funkcji operatorskich. Zesz Nauk Akad Morskiej W Gdyni 2012;76:14–23.

[99] Doerry N. Designing electrical power systems for survivability and quality of service. Nav Eng J 2007;119:25–34. http://dx.doi.org/10.1111/j.0028-1425.2007.00017.x.

[100] Robertson LS. Reducing Death on the Road: The effects of minimum safety standards, publicised crash tests, seat belts and alcohol. Am J Public Health 1996;86:31–5.

[101] Tyrell D, Jacobsen K, Martinez E, Perlman AB. A train-to-train impact test of crash energy management passenger rail equipment: structural results. Proceedings of the international mechanical engineering congress and exposition. American Society of Mechanical Engineers; 2006.

[102] Johnson M, Shrewsbury B, Bertrand S, Calvert D, Wu T, Duran D, et al. Team IHMC's lessons learned from the DARPA robotics challenge trials. J F Robot 2017;32:241–61. http://dx.doi.org/10.1002/rob.21674.

[103] Saunders J, Parent D, Ames E. NHTSA oblique crash test results: vehicle performance and occupant injury risk assessment in vehicles with small overlap countermeasures. Proceedings of the twenty-forth enhanced safety of vehicles. 2015.

[104] Valdez Banda OA, Hänninen M, Lappalainen J, Kujala P, Goerlandt F. A method for extracting key performance indicators from maritime safety management norms. WMU J Marit Aff 2016;15:237–65. http://dx.doi.org/10.1007/s13437-015-0095-z.

[105] Fälth J, Ljungqvist M. Identification of leading objective indicators of safety in shipping. Lund: 2013.

[106] Schmidt M, Fentzahn E, Atlason GF, Rødseth H. Maritime unmanned navigation through intelligence in networks – autonomous engine room. Warnemünde: 2015.

[107] Thieme CA, Utne IB. Safety performance monitoring of autonomous marine systems. Reliab Eng Syst Saf 2017;159:264–75. http://dx.doi.org/10.1016/j.ress.2016.11.024.

[108] Karvonen H, Aaltonen I, Wahlström M, Salo L, Savioja P, Norros L. Hidden roles of the train driver: a challenge for metro automation. Interact Comput 2011;23:289–98. http://dx.doi.org/10.1016/j.intcom.2011.04.008.

[109] Czaplewski K, Goward D. Global navigation satellite systems – Perspectives on development and threats to system operation. TransNav, Int J Marine Nav Safety Sea Transp 2016;10(2):183–92. http://dx.doi.org/10.12716/1001.10.02.01.

[110] Szłapczyński R, Szłapczyńska J. Review of ship safety domains: Models and applications. Ocean Eng 2017;145:277–89. http://dx.doi.org/10.1016/j.oceaneng.2017.09.020.

[111] Krata P, Montewka J. Assessment of a critical area for a give-way ship in a collision encounter. Arch Transp 2015;34:51–60.

[112] Zhang J, Yan X, Chen X, Sang L, Zhang D. A novel approach for assistance with anti-collision decision making based on the international regulations for preventing collisions at sea. Proc Inst Mech Eng Part M J Eng Marit Environ 2012;226:250–9. http://dx.doi.org/10.1177/1475090211434869.

[113] Hilgert H, Baldauf M. A common risk model for the assessment of encounter situations on board ships. Dtsch Hydrogr Zeitschrift 1997;49:531–42. http://dx.doi.

org/10.1007/BF02764347.

[114] Colley BA, Curtis RG, Stockel CT. Manoeuvring times, domains and arenas. J Navig 1983;36:324–8. http://dx.doi.org/10.1017/S0373463300025030.

[115] Curtis R. A ship collision model for overtaking. J Oper Res Soc 1986;37:397–406.

[116] Krata P, Montewka J, Hinz T. Towards the assessment of critical area in a collision encounter accounting for stability conditions of a ship. Pr Nauk Politech Warsz Transp 2016:169–178.

[117] Łukaszewicz A. Określanie odległości krytycznej podjęcia manewru ostatniej chwili zgodnie z przepisami konwencji COLREG. Międzynarodowa Konf. Nauk. Transp. XXI wieku, Stare Jabłonki: Politechnika Warszawska; 2007, p. 389–96.

[118] IMO. COLREG: convention on the international regulations for preventing collisions at sea. International Maritime Organization; 1972.

[119] Naeem W, Irwin GW, Yang A. COLREGs-based collision avoidance strategies for unmanned surface vehicles. Mechatronics 2012;22:669–78. http://dx.doi.org/10.1016/j.mechatronics.2011.09.012.

[120] Koszelew J, Wołejsza P. Determination of the last moment manoeuvre for collision avoidance using standards for ships manoeuvrability. Annu Navig 2017;24:301–13. http://dx.doi.org/10.1515/aon-2017-0022.

[121] Cockroft AN, Lameijer JNF. A guide to the collision avoidance rules. 6th ed. Oxford: Elsevier; 2004.

[122] Goerlandt F, Montewka J, Kuzmin V, Kujala P. A risk-informed ship collision alert system: framework and application. Saf Sci 2015;77:182–204. http://dx.doi.org/10.1016/j.ssci.2015.03.015.

[123] DNV-GL. Guidance for safe return to port projects. Class guideline DNVGL-CC-0004. 2016.

[124] Chen S, Wall A, Davies P, Yang Z, Wang J, Chou Y. A human and organisational factors (HOFs) analysis method for marine casualties using HFACS-maritime accidents (HFACS-MA). Saf Sci 2013;60:105–14. http://dx.doi.org/10.1016/j.ssci.2013.06.009.

[125] Theunissen E. Navigation of unmanned vessels – history, enablers, challenges and potential solutions. Proceedings of the twelfth international naval engineering conference and exhibition. 2014.

[126] Rødseth ØJ, Burmeister H-C. Developments toward the unmanned ship 2012.

[127] Rae A, Alexander R. Forecasts or fortune-telling: when are expert judgements of safety risk valid? Saf Sci 2017. http://dx.doi.org/10.1016/j.ssci.2017.02.018.

[128] Song Y. Applying system-theoretic accident model and processes (STAMP) to hazard analysis. McMaster University; 2012.