Ocean Engineering 152 (2018) 334–345

Contents lists available at ScienceDirect

Ocean Engineering

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

System-theoretic approach to safety of remotely-controlled merchant vessel

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

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

ARTICLE INFO

Keywords:
Unmanned vessels
Remote operation
STAMP
STPA
Safety of transportation

ABSTRACT

Unmanned merchant vessels' prototypes are expected to come into operation within a few years. This revolutionary shift in the shipping industry is feared to negatively impact the safety of maritime transportation. Therefore, in order to support future designers of remotely operated merchant vessels system, we applied System-Theoretic Process Analysis (STPA), identifying the most likely safety control structure of the analysed system and investigating it. The aim was to suggest potential ways of increasing the system's safety and to assess the effectiveness of such measures. Results indicate that the implementation of remotely-controlled merchant vessels and, in a wider sense, unmanned ships, and ensuring their safety shall consist of executing various controls on regulatory, organisational and technical plains. Potential effectiveness is evaluated and some recommendations are given on how to ensure the safety of such systems.

1. Introduction

As unmanned technologies' development gains momentum in various domains, it is postulated that similar can also be achieved in marine transportation. Herein, ships could be operated remotely from a shore control centre or even proceed autonomously. Supporters of such a shift argue that it would reduce shipping costs, environmental impact and threats to humans working for the industry (Porathe, 2016), while some more sceptical authors are of the opinion that the safety of maritime transportation can be negatively affected (Wróbel et al., 2017). It is therefore of utmost importance to ensure that such vessels at least do not reduce the level of safety (Burmeister et al., 2014b). Besides technical considerations and social controversies (Bitner et al., 2014), safety became the most important issue to resolve.

Numerous research projects' reports or scientific papers have recently been published in the field. Initially, only some basic ideas have been developed and refined (Iijima and Hayashi, 1991; Rødseth et al., 2013; Rødseth and Burmeister, 2012; Jalonen et al., 2017). Then, the concept was developed and some safety issues have been addressed, including those pertaining to unmanned ships' navigation (Johansen and Perez, 2016; Theunissen, 2014) and remote control (Man et al., 2015; Porathe et al., 2014; Wahlström et al., 2015). As safety of unmanned navigation remained in focus, there were attempts to utilise experience gained in other domains (Wahlström et al., 2015) in order to assess it. Finally, there were numerous attempts of identifying and quantifying hazards present in this field (Burmeister et al., 2014b; Heikkilä et al., 2017; Hogg and Ghosh, 2016; Kretschmann et al., 2015a, 2015b; Rødseth and Burmeister, 2015a; Rødseth and Tjora, 2014a; Wróbel et al., 2016; Jalonen et al., 2017). Security issues were considered as part of feasibility and safety analysis and were also addressed separately (Dobryakova et al., 2015). The conclusion of the above is that, in general, there is a potential within unmanned vessels' technology to improve safety of transportation (Kretschmann et al., 2015a), but more data is required and some issues still require addressing in order to reduce the uncertainties (Burmeister et al., 2014b; Wróbel et al., 2017).

Nevertheless, a reliability- and probability-based approach to safety analysis as applied in afore-mentioned research is neither exhaustive nor free of significant drawbacks. Such analyses can only be performed for systems, reliability structure of which is known. For remotely controlled vessels, their concepts of design are still being developed and the final structure of the system remains uncertain, therefore it is impractical to assess their safety in its reliability-based form (Leveson, 2011). Furthermore, a great deal of systems' understanding and safety improvements originates from knowledge gained during actual operations or even through accidents investigations (Mazaheri et al., 2015; Stoop and Dekker, 2012). Since no quantitative or qualitative data is available here, this approach cannot be applied.

Above considerations suggest that a different method of analysing the

* Corresponding author. Gdynia Maritime University, Faculty of Navigation, Department of Navigation, 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.oceaneng.2018.01.020
Received 26 May 2017; Received in revised form 29 September 2017; Accepted 4 January 2018
Available online 23 February 2018

safety of remotely-controlled ships shall be applied. System-Theoretic Process Analysis (STPA), a relatively new method of including safety in system's design has recently emerged (Leveson, 2011, 2002). Rooted in System-Theoretic Accident Model and Process (STAMP), it has been applied in some innovative domains (Owens et al., 2008) including maritime sector (Abrecht, 2016; Aps et al., 2015; Kwon, 2016). It is said to better encompass and help mitigate some hazards that are specific to modern, highly-automated and complex systems (Altabbakh et al., 2014; Bjerga et al., 2016). However, a safety analysis based on a systemic approach has not been applied to remotely-controlled shipping systems to date, a gap this paper is intended to bridge.

Therefore, we apply STPA to assess the safety of a remotely controlled, generic merchant vessel and provide future designers of such systems with advice pertaining to which of its parts are likely to fail and how. Furthermore, we suggest some measures to mitigate hazards and qualitatively assess their potential effectiveness by applying a mitigation potential analysis.

The paper consists of four Sections, the Introduction and Conclusions. Firstly, the description of anticipated unmanned ships' systems layout is given together with general assumptions and some considerations regarding its impact on safety. Secondly, the method of safety analysis is introduced, namely System-Theoretic Process Analysis (STPA). It is followed by Section 3 describing the results of the study which are then discussed in Section 4, together with brief assessment and communication of uncertainties. Last but not least, conclusions are drawn.

2. Remotely operated vessels' proof of concept

This Section introduces general considerations pertaining to unmanned ship and their safety.

The reduction of merchant ships' crews progressed for some time already with some of the vessels becoming technically and legally acceptable to be operated by crews of eight or even less. This was an effect of implementing new technologies, mainly in the engine department (Bertram, 2002). It is postulated that further progress in this field can lead to a complete elimination of the necessity to employ any crewmembers on board. Most operational requirements as specified in international conventions are in the form of functions to be performed with only few of the rules specifically requiring that those functions shall be performed by on-board crew members (AAWA, 2016; IMO, 2011).

It is anticipated that the overall design of such unmanned ships shall be significantly different to those operated nowadays in many aspects including hull design and propulsion arrangement (Grøtli et al., 2015). However, the greatest and the most important difference will be that all of her subsystems will be to a large extent controlled either remotely or in an autonomous mode. The ship would traverse an open sea in ballast or laden condition with no crew present on board. The system's basic functions will be performed automatically without involving human operators, who would be stationed in a so-called shore-based control centre and capable of remotely supervising the vessel or taking over its control using a dedicated satellite communication link. This would be possible whenever the ship encounters a situation that for any reason cannot be handled by the automated control system, or whenever deemed necessary. By that, the vessels are anticipated to follow an 'adjustable autonomy' scheme depending on the condition of the ship herself and the mission being executed. Particular levels of autonomy in the maritime industry have been published by Lloyd's Register of Shipping (LR, 2016) and are presented in Table 1 below.

Upon approaching the port of destination, a berthing (or 'conning') crew might be required to board the ship by launch boat or helicopter in order to bring her to the berth (Burmeister et al., 2014b), an arrangement similar to this of maritime pilots boarding ocean-going vessels nowadays. Since port manoeuvres are the most demanding part of passage (Ahmed and Hasegawa, 2013), coastal states might be unwilling to allow unmanned vessels to operate in their inland waters (Hooydonk, 2014; Rødseth and Burmeister, 2015a; Rødseth and Tjora, 2014a, 2014b; Van Den Boogaard et al., 2016) due to the uncertainty concerning their safety and security performance, at least in the initial phases of such vessels' implementation. Such a concept means that the system must be capable of operating in multiple autonomy modes ranging from AL-0 to AL-5 and switching between them without reducing system's overall safety performance.

Table 1
Ship autonomy levels, based on (LR, 2016).

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.

In this paper, we focus on the 'remote control' mode which corresponds to Autonomy Level 3. Here, an operator located on shore will have an overall command over a handful of vessels traversing different seas (Porathe et al., 2014). (S)he will oversee decision making, supervision and trouble-shooting, thus simultaneously performing tasks that today require many crewmembers' expertise. Decision support tools can be of some help in this. However, as soon as a situation develops in a particularly difficult direction, an assistance of full bridge team is said to be available in order to better deal with the problem (Kretschmann et al., 2015a). Still, such a team will be located in a shore based control centre some distance away from the vessel, which can potentially create further issues, just to mention communication link unreliability, flawed situation awareness and an inability to manually operate equipment (Ahvenjärvi, 2016; Porathe et al., 2014). The level of operator's involvement can be adjusted as required.

Such an approach will require an extensive redesign of the ships in order to accommodate numerous sensors or prolonged maintenance-free periods (Rødseth and Burmeister, 2015b). The fact that a vessel is controlled remotely will affect virtually all aspects of her operation, including navigation, power generation, fuel management, cargo conditioning and fire safety. All those are mutually related (Krata et al., 2016; Krata and Szlapczynska, 2018; Krata and Wawrzynski, 2017) and thus a systemic approach is required to fully apprehend the effect of implementing a remote control into merchant vessels' operation on maritime safety.

3. Methods

The majority of risk assessment methods currently in use are based on the assumption that accidents are caused by particular safety-critical components not being able to serve their purpose (Salmon et al., 2012). This belief in reliability theory's significance contributed to safety

analysts and accident investigators refraining from analysing concealed causes of accidents (Leveson, 2011). Those may be of non-technical nature and belong to organisational or sociological domains (Willey, 2014). As such, they have often been neglected for the reason that it is difficult to quantify human behaviour and reliability of human operator (Montewka et al., 2017) or supervisor, for instance. Therefore in this Section, a different method of safety assessment is presented as given in (Leveson, 2011).

3.1. System-theoretic approach

A systemic insight has been proposed so as to address the safety issue on higher organisational levels including operational practices and management policies ensuring that hazards are controlled in each point of the system's structure (Kee et al., 2017; Leveson, 2011; Salmon et al., 2015). In this approach, referred to as System-Theoretic Accident Model and Process (STAMP), it is inadequate interactions between a system's components that lead to accidents. The nature of such interactions shall ensure that the system as a whole remains within safety limits (Kazaras et al., 2014). As a consequence of the above, violation of these 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). A system's states that could lead to safety constraint violation are inspected and ways of mitigating such violation sought. It is recommended to refrain from calculating probabilities of system transitioning to an unsafe state (Bjerga et al., 2016) due to a lack of empirical data, particularly in initial phases of system development.

A STAMP-based approach also takes into consideration one more aspect that can potentially prove vital when addressing the safety of a highly innovative system of a remotely-controlled ship. Nowadays, systems composed of thousands of technologically advanced components are run by relatively small crews, who are often physically separated from the system for cost-effectiveness or safety reasons, for instance. Such crews must have a perfect understanding (a mental model) and perception of the system's status and related automation. With the shift from a manual to remote control, people reportedly became less familiar with the systems under their supervision (Norman, 1989). Another important factor is that the majority of processes are conducted automatically, leaving humans with merely supervisory functions and requiring them to step in as soon as the automation cannot control the system any longer (Leveson, 2011). Utilising remote control may contribute to a limited perception of the actual state of the controlled process, boredom, loss of focus, skill degradation and loss of situational awareness (Porathe et al., 2014; Wahlström et al., 2015) in case any unusual event occurs. It is essential that operator's mental model of the process reflects its actual condition – such a case was relatively simple to achieve when operators controlled the machinery from local stations and could confirm systems' components' condition visually, aurally or even olfactory. With progressing separation of workers from physical components, the potential of mental model's accuracy degradation grew. The reasons for that could be various, just to mention possible inconsistencies between system's initial design and actual layout, improper management of change or inadequate/insufficient training.

Moreover, as a tendency to introduce more automation into systems progressed, another factor leading to an increased likelihood of unwelcome events surfaced: a human operator's mental model of the automation itself. In old-fashioned systems, confirmation of an actuator's operation was in many cases appearing almost instantly as a system's condition change could be observed locally. In remote control's case, this is much more complicated. Here, operators' decisions are enforced by actuators, and progress is monitored by sensors. This means, in short, that: firstly, the operator must make proper decision based on information fed and their own mental model of the system. Then, such decision must be 'translated' by software into actuators' command and thus relayed to the latter. Next, relevant actuators must enforce operator's decision in a proper way. Progress of such action must be monitored by sensors, and their readings transmitted to the operator who must check if they match his initial intentions. Basically, things can go wrong in each of these steps and proper measures shall be taken to prevent it from happening.

Herein, in a process of safety-guided design (Leveson, 2011), Safety-II paradigm can be invoked, focusing on making entire socio-technical systems capable of succeeding under expected and unexpected conditions alike (Hollnagel, 2014). In order to achieve this, safety is to be embedded in the design from the very beginning of system's existence, in which STAMP and related methods can assist (Altabbakh et al., 2014) as they are said to be more effective safety management tools than previously applied methods (Kazaras et al., 2014). In relation to unmanned merchant vessels as an emergent technology, such an approach creates the opportunity for both performing proactive safety assessment as well as assessing feasibility of system-theoretic approach in this aspect. The latter could be accomplished not sooner than some period after remotely-controlled vessels' implementation.

Therefore, we apply the System-Theoretic Process Analysis (STPA), a tool rooted in STAMP, with the intention to accumulate information about how the safety constraints can be violated and how to prevent such violations. In order to evaluate measures of increasing safety, we apply mitigation potential analysis as described in Section 2.3.

3.2. STPA

Although the STPA can be used at any stage of the system life cycle (Leveson, 2011), this study's goal is to apply it to a system which is still at a concept phase, namely a remotely controlled merchant ship. The aim of STPA-based safety analysis is to determine how the behavioural safety constraints, which are derived from system hazards, can be violated and how to prevent such violations. The ultimate goal is to identify scenarios leading to identified hazards and thus to losses so they can be either mitigated or controlled without involving unnecessary costs.

Firstly, an identification of the potential for inadequate control of the system that could lead to a hazardous state is conducted. Those can result from inadequate control or enforcement of the safety constraints, which in turn can occur because:

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.

Secondly, it is determined on how each potentially hazardous control action identified in first step could occur. This can consist of examination of the control loop in order to see what could cause it. Furthermore, control and mitigation measures can be suggested. For multiple controllers of the same component or safety constraint, identification of conflicts and potential coordination problems should be carried out. This step can be augmented by a consideration on how the designed controls could degrade over time and building in protection against it, including management of change procedures, performance audits or accident and incident analysis.

For instance, in the case of remotely-controlled merchant vessels, ensuring the reliable and precise communication between the ship and control centre will be one of the most vital functions of the system. Such interaction between two of the system's components is referred to as a 'control function' and can be inadequate in one or more ways as listed above. These ways are analysed further with respect to potential causes and consequences of such inadequacy.

It is postulated that most the cost-effective and efficient way of designing for safety in case of extremely complex systems is to carry out safety assessment in parallel with engineering the system itself (Leveson, 2011). In this model, design decisions are analysed by safety analysts and

feedback is given to improve the safety of the system in an iterative process.

However, it cannot be done here since it remains unclear whether the generic unmanned ship is in fact to be designed and come into operation in the foreseeable future. Therefore, this study focuses on an as accurate as possible assessment of ship's safety features basing on available information in hope to provide future system designers with reliable evaluation and suggestions pertaining to how the system should in fact be designed. In order to perform such analysis, the STPA was supported by a mitigation potential analysis.

3.3. Mitigation potential analysis

For the reason of the unavailability of data required for traditional safety assessment, a hazard mitigation potential has been chosen as a surrogate for a likelihood, an element of traditionally-understood risk (Dulac and Leveson, 2009). Reasons for its use include:

- The potential for eliminating or controlling the hazard in the design or operations has a direct and important impact on the likelihood of the hazard occurrence;
- Mitigatibility of the hazard can be determined before the system's architecture or design is selected.

Mitigation potential scale is used as listed below and presented in Fig. 1.

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.

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

Safety control structure is studied and ways of mitigating control functions' inadequacy are sought and assigned the mitigation potential value. For example, elimination of a necessity for communication link's existence could be assigned a higher value of mitigation potential than implementing algorithms to ensure a correctness of data transferred.

In our study, we assigned the mitigation potential to each of the potentially inadequate control functions' occurrence mitigating measures rather than to the hazards themselves. As a result, we quantified the potential of unsafe control function leading to the hazard instead of hazard leading to an accident. This was done because of a low detail level of our model.

3.4. Creating a safety control structure

In order to perform the STPA and mitigation potential analysis, a safety control structure was first developed as given in Fig. 2. This was achieved by reviewing the available literature pertaining to remotely-controlled vessels, see for instance (AAWA, 2016; Ahvenjärvi, 2016; Burmeister et al., 2014b; Kretschmann et al., 2015a; Man et al., 2015, 2014; Porathe, 2016; Rødseth and Brage, 2014; Rødseth and Burmeister, 2015a; Rødseth and Lee, 2015; Wróbel et al., 2016) and brainstorm-based workshop. The latter involved experts engaged in the design of an unmanned river-crossing ferry, whose knowledge was elicited. Similarly, a list of hazards and safety constraints was created in order to systematize knowledge regarding the safety of a remotely-controlled generic merchant vessel.

By ‘generic’, we mean a ship that is designed and operated for transporting cargo between ports. To be more specific, such an unmanned vessel is expected to traverse oceans in an autonomous mode (AL-5), and enter ports as done nowadays, which is with full complement of crew on board (AL-0 or AL-1) (Burmeister et al., 2014a). We focused

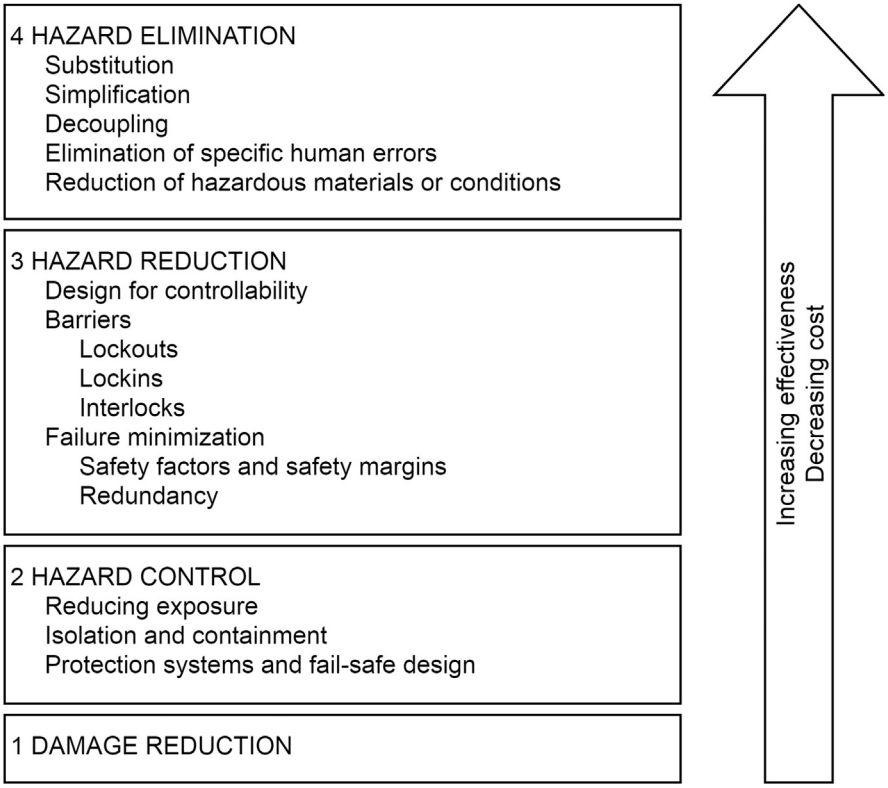

Fig. 1. Effectiveness of hazard mitigation approaches, based on (Leveson, 2011).

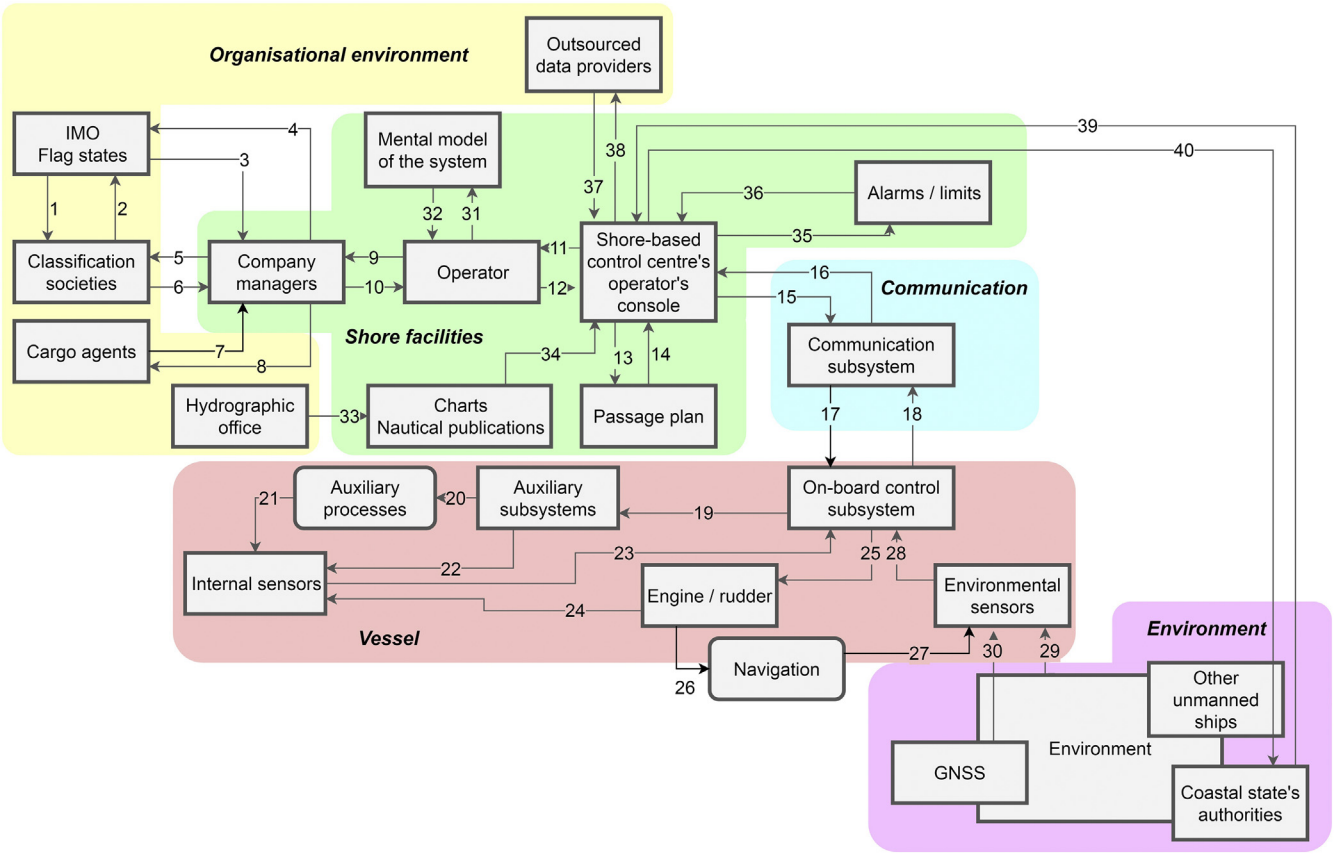

Fig. 2. System's safety control structure.

on what is in between: the navigation in high traffic density areas or otherwise demanding or non-standard conditions. Such conditions shall be defined in order to provide the system with a procedure of safe and smooth transition from AL-5 (autonomy) to AL-3 (remote control), a call for operator's assistance in other words. Nevertheless, such 'generic' ship is defined as not having any special requirements pertaining to cargo stowage. Bulk carriers, general cargo or container vessels can serve as a good example. Although they can be technologically advanced, their cargo conditioning equipment and technology as well as safety features are far simpler than those of tankers or passenger vessels for instance.

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

Results of the above are presented in Section 3 as well as in Appendices.

4. Results

This Section presents the list of hazards and safety constraints as well as high-level safety control structure and its description.

4.1. Safety control structure

The remotely-controlled vessel's system-level decisions are made by an operator on shore. Data fed by various sensors is used to provide the operator with an artificial situation awareness. The sensors can be either environmental or internal. While the former will pertain to the navigational situation around the vessel and will include global navigation satellite systems (GNSS) receivers, radars, cameras, echosounders etc. (Burmeister et al., 2014b; Kretschmann et al., 2015a), the latter will monitor the vessel's interior, just to mention its stability condition or machinery status (Krata and Wawrzynski, 2017; Wawrzyński and Krata, 2016a, 2016b). The issue of disagreement between particular sensors' indications could be resolved by data fusion algorithms (Filipowicz and Neumann, 2008), which would require at least some of the sensors to be doubled or tripled. The data should be as accurate as possible to allow an operator to make proper decisions in ample time and keep all the parameters within the limits. Such decisions will be executed by actuators to control ship's movements as well as other processes. Ballast water management, cargo conditioning and fire safety monitoring can be listed here, but virtually all parameters of the vessel's performance should be controllable to a certain degree. Such a degree will depend on the vessel's technical condition, her mission status or the complexity of navigation situation.

Ensuring proper functioning of those auxiliary systems will be required to provide the vessel's main function: carriage of commodities between ports, to which the propulsion is vital. Here, the use of azimuthal thrusters or similar devices can be nominated as candidates for providing the vessel with propulsion as these appliances can both create thrust and direct it in a desired way. Another advantage of using them instead of traditional shaft propeller and rudder is the potential for providing the redundancy when two or more devices are installed. Nevertheless, since this issue is yet to be resolved by actual designers of the vessel, in our analysis we keep using expressions of 'engine' or 'rudder' to describe the propulsion and steering subsystem in general. No matter the actual design, these appliances will be used to control what is here referred to as 'Navigation', meaning vessel's course and speed.

Some shipboard processes shall be controlled automatically by the on-board control subsystem, but an overriding authority should be with the operator. One of the reasons behind such arrangement is that a fail-safe mechanism shall be provided in case the operator's decisions

cannot be relayed to the vessel and she shall proceed on her own for some time (Hogg and Ghosh, 2016).

An operator's primary objective will be to ensure that the vessel is following the pre-planned route in a safe and efficient manner. It shall be at the operator's discretion to amend the passage plan if required for the purpose of collision avoidance or any other. Similarly, in order to achieve it, the operator shall be in possession of up-to-date model of the environment (charts, nautical publications); mental model of the ship and all of its controllers are also of a great importance. Additional data, for example regarding expected traffic or weather conditions could be obtained from external sources in order to extend the operator's perception of the situation around the vessel under control. At least in the initial phases of system implementation, the experience of seafarers in handling demanding situations will need to be exploited together with their ability of maintaining situation awareness (Ahvenjärvi, 2016; Bertram, 2002). Seafarers, particularly Master Mariners or Chief Engineers, with additional training in remote control appear to be suitable candidates for the position of shore-based operators (Hogg and Ghosh, 2016).

The operator's role will therefore be similar to that of today's vessels crews, except for the fact that (s)he will need to achieve it from some distance by use of remote controllers. In order for these to act properly, a secure and reliable communication link needs to be provided and some fail-safe mechanism developed for the occasion that communication is not available for some reason. The only feasible ways of transmitting the necessary data worldwide today is satellite communication. However, at certain areas, other protocols can be used, for example VHF radio-communication or mobile wireless telecommunication (Höyhtyä et al., 2017). Furthermore, should neither of these be available, high-frequency (HF) communication can be nominated as a backup since it can provide a global coverage. No matter which of communication technologies is used, its reliability will be vital to provide integrity of the system. This includes protections against cyberterrorism (Rødseth and Lee, 2015).

Further components of the system include various actors that can have an influence on remotely-controlled vessels' safety performance on higher hierarchy levels. These include: the International Maritime Organisation and flag state administrations, classification societies and companies managing the ships and control centres. Such actors will issue certain procedures, guidelines and regulations governing the ways in which not only the ships themselves but also the entire systems shall be designed, constructed and operated. Vessels' management companies shall be responsible for coordinating operators' actions by issuing operational procedures, organising training and management of on-board subsystems' maintenance.

The low-detail structure of the anticipated system focusing on safety control structure is depicted in Fig. 2.

The 'system' of a remotely-controlled ship can therefore be defined as: '*all technical, organisational and human-based arrangements purposely designed or utilized in order to perform a safe navigation of a sea-going vessel controlled remotely*'.

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, software, hardware and liveware involved, operational procedures and legislation. In other words, everything on which the system's designers can have a 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 threats to security such as cyberterrorism. Those, in general, remain out of this analysis' scope even though illegal activities can affect virtually each of the system's components.

The relationships between the components of this defined system as well as the system and the environment are referred to as control functions. Ensuring their proper functioning prevents safety constraints' violations (safety controls). In order to determine ways in which control functions can potentially be dangerous and quantify a potential of preventing them from becoming such, we performed STPA followed by mitigation potential analysis.

As can be seen in Fig. 2, the elaborated structure consists of a rather limited number of components and relationships between them. This is due to the fact that the present (fall 2017) stage of technology development does not allow for more detailed analysis. Nevertheless, most if not all of the control functions could be broken into higher level of details where more components are included. However, without knowing the exact design of a remotely-controlled vessel's system, such an approach cannot be supported. The depicted safety control structure is the reasonable compromise between speculation on future systems' layout and views presented in available literature. Some consequences of this approach are given in Section 4.2.

4.2. Hazards' and constraints' list

Based on the developed system's safety control structure we compiled a list of hazards and related safety constraints, as given in Table 2. As can be seen, the occurrence of certain hazards may propagate into the emergence of others. Therefore, mitigation measures capable of protecting against multiple hazards simultaneously can be characterized by greatest effectiveness.

4.2.1. Interactions' analysis

Upon elaborating the safety control structure and hazards' list, we then proceeded to analyse each of the control functions in accordance with STPA principles. This was done with regard to their:

- position within the system;
- potential hazards resulting from it being inadequate;
- consequences of such inadequacy in each of four potential cases (not provided, unsafe provided, incorrect timing, incorrect duration);
- potential causes of inadequacy;
- feasible mitigation measures and their potential;
- potential protections against degradation in time.

The above factors were elaborated and compiled in a form of tables, an example of which is presented in Table 3. The full catalogue of control functions is given in Appendices.

The analysis of this function proceeded as follows. Its position within the system was first reviewed to determine control loops affecting it and being affected, see Fig. 2. Thence, hazards resulting from its potential inadequacy were identified. Since shore-ship communication is one of the most essential to remotely-controlled vessel's safety, failure to provide it can directly lead to the emergence of any of hazards as listed in Table 2 as virtually all on-board activities are controlled through it. Potential causes as well as consequences of the communication link's failure were then refined with respect to the four types of inadequacy as given in Section 2.2. Ways of ensuring that the communication link remains safe, reliable and efficient were then sought together with measures of degradation control.

By refining potential causes of inadequacy and recommendations on mitigation measures, we aimed at providing future system designers and operators with suggestions on how certain issues can be resolved in order to embed safety in the design of remotely-controlled merchant vessels' system. The obtained results are discussed within Section 4.

5. Discussion

Results of the analysis performed are discussed within Section 4.1, while uncertainties are addressed in Section 4.2.

5.1. Discussion of study's results

In total, forty-six control functions have been analysed, affecting twenty-four high-level components of the system. A catalogue of the

Table 2
List of high-level system hazards and safety constraints. Partly based on (Allianz, 2015; Kretschmann et al., 2015b). Repetitive hazards have been crossed out and omitted in further steps.

#	Description of **hazard**/*constraint*
1	**Vessel's physical interaction with manned structures results in death or injury**
1.1	**Vessel collides with another ship** *Vessel shall not violate minimum CPA with another ships*
1.2	**Vessel runs into element of infrastructure (i.e. bridge)** *Ship shall not enter No Go Area*
1.3	**Vessel damages other man-made objects (i.e. fishing gear)** *Ship shall maintain safe distance from any objects*
1.4	**Vessel is incapable of properly containing dangerous chemicals or energy** *Vessel shall not release any dangerous substance or excessive energy to the environment*
1a	**Vessel's inability to provide assistance to humans in distress**
1a.1	**System does not detect a distress situation** *System shall be capable of detecting distress situations*
1a.2	**System deliberately ignores distress situation** *Ship shall provide assistance to any person in distress*
1a.3	**System is forced to abandon rescue operation or its attempt** *Ship shall be capable of providing assistance to any person in distress in any conditions*
2	**Vessel's inability to reach port of destination in expected time**
2.1	**Vessel runs aground** *Ship shall not enter No Go Area*
2.2	**Vessel suffers from propulsion/steering failure** *Control over engine and rudder must be provided at all times when at sea*
2.3	**Vessel is denied passage due to security concerns** *System's security and cybersecurity shall be maintained at all times*
2.4	**Vessel encounters severe weather conditions limiting her navigational capabilities** *Efficient weather routing shall be employed*
2.5	**Vessel suffers from loss of stability** *Ship shall maintain stability at all times*
2.6	**Vessel suffers from flooding** *Ship's hull condition, incl. shear forces and bending moments, shall be observed*
3	**Vessel's inability to deliver cargo in unchanged condition or in a condition that falls within industry standard**
3.1	**Vessel loses her cargo at sea** *All necessary resources shall be dedicated to ensure proper stowage of cargo on board*
3.2	**Vessel is unable to maintain proper cargo stowage conditions** *Cargo stowage condition shall be monitored and controlled at all times*
4	**Vessel's exposure to major damage or breakdown**
4.1	~~**Vessel runs aground**~~
4.2	~~**Vessel collides with another ship, runs into element of infrastructure or damages other man-made objects**~~
4.3	**Vessel suffers from fire or explosion** *Ship must maintain fire safety precautions at all times*
4.4	**Vessel suffers from loss of structural integrity** *Ship's hull condition, incl. shear forces and bending moments, shall be observed*
4.5	**Vessel suffers from loss of power supply** *Power supply must be provided at all times*
5	**Vessel's inability to prevent environmental pollution**
5.1	**Vessel is unable to maintain integrity of tanks containing oils or oily mixtures** *Oil tanks' levels shall be monitored and controlled at all times*
5.2	**Vessel is unable to maintain proper fuel combustion parameters** *Engines' working parameters shall be monitored and controlled at all times*
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 collides with another ship, runs into element of infrastructure or damages other man-made objects**~~
6.2	**Vessel contributes to delay of other ships' traffic** *Vessel's route shall be optimized so as to avoid any negative interactions*
6.3	**Vessel violates international or coastal state's regulations** *Coastal state's and international regulations shall be observed at all times*
6.4	**System's communication subsystem unintentionally interferes with other assets** *Ship shall not negatively impact others' operational capabilities*

control functions and results of their analysis are given in Appendices, where each of the functions is addressed separately, however in full accordance with its position within the entire structure (numbers refer to those depicted in Fig. 2).

5.1.1. Control functions' inadequacy

Most of the controls could be inadequate in multiple ways as given in Section 2.2. As a result, it can be deduced that not only shall they be provided, but also every effort should be taken in order to ensure that they are provided correctly, in proper time and in a proper sequence in relation to other. This can be achieved by implementing suitable algorithms or procedures, disabling certain functions of the system unless certain conditions are met. On the other hand, it might prove beneficial to allow operators to override such restrictions in order to utilise their experience in unexpected conditions, for instance.

5.1.2. Hazards emerging

Many of the control functions' potential inadequacies may result in the emergence of virtually any of the hazards (#1–6b,9–12,35-40 for instance). This may be attributed to three factors:

- relatively low detail level of the analysis, where only very general statements could be made in relation to the system's structure and thus it was recommended to consider somewhat worse consequences of particular control function's failure,
- fact that most of the control functions whose inadequacy would result in emergence of 'any hazard' refer to high level of system's hierarchy, such as management or legal aspects,
- complexity of the system and nature of mutual interactions between its components may lead to multidirectional failure propagation due to operators' and managers' inability to counteract it (Wróbel et al., 2016).

The above indicate a need for further research in the domain of unmanned shipping, to which however more empirical data may be required.

5.1.3. Causal categories

Each potential cause as given in Appendices tables can be assigned to one of three causal categories: human (resulting from human error), operational (unsuitable procedures, algorithms, legal acts) or technical (hardware malfunctions). Results of such categorization and breakdown of inadequacy causes against control function's position within the system are depicted in Fig. 3.

Initially, we expected to blame the environmental conditions for at least some of inadequacies, but none of potential causes could be assigned to such a category. This can be attributed to the fact that, with the system theory applied, the environmental conditions by themselves do not create a hazard. Instead, it is the system's inability to measure or counteract them that do.

The most prominent results reveal that the majority of safety constraint violations within the vessel can potentially be attributed to technical issues (see control functions #19 through 25 in Appendices) which emphasizes the importance of ensuring sufficient reliability of vessel's technical equipment. Furthermore, a relatively high number of potential causes for control functions' inadequacy pertains to the interaction between shore-based facilities and legal or organisational environment (#1–8). However, mistakes made at levels of hierarchy so far removed from daily routine, for instance international conventions' legislation process, can in many cases be corrected by a good seamanship (Knudsen, 2009). Similarly, a low number of potential causes can be attributed to human factor while the very concept of a remotely-controlled vessel implies that humans' actions will have a great

Table 3
Example of control function analysis.

Control function number:	**17**	Communication subsystem → On-board control subsystem
Control function name:	*Decisions' relay*	
Textual description:	Decisions made by operator are relayed to the vessel via communication link	
Rationale:	Operator's decisions must be transmitted to the actuators on board via communication link	
Hazards resulting:	All hazards	

Potential for inadequacy:	***Control function is not provided***	***Unsafe control function is provided***	***Control function is provided in wrong time***	***Control function is provided for too short or too long***
Consequences:	Operator's decisions are not relayed to the vessel	Operator's decisions are relayed to the vessel incorrectly	Operator's decisions are relayed to the vessel with delay	Incomplete data set is relayed to the vessel, some decisions may be missing
Potential causes:	Data is transmitted to a wrong vessel Satellite is offline Vessel's antennae set malfunction Vessel navigates outside satellite communication system coverage	Control function #15 inadequate Dataset is distorted	Data buffers at any stage of transmission are overflown Subsystems' clocks are not coordinated	Control function #15 inadequate Communication link malfunction
Feasible mitigation measures and potential	Fail-to-safe mechanism 1 Implementation of AL-5 4 Redundancy of antennas 3 Use of multiple satellite link providers 3 Redundancy of ways of communication 3 Vessel identification within dataset 2	Data validation algorithms 2	System time transmission 3 Data transmission management procedures/algorithms 2	Transfer repetition algorithms 2
Protection against control degradation	Performance tests of communication link	Performance tests of communication link		

impact on the system's safety (#10c-12,35–38) (Man et al., 2015, 2014; Porathe et al., 2014; Stokey et al., 1999). However, methods of evaluating the significance of particular control functions' inadequacy for the safety of systems in question are lacking and should be elaborated by academia to help distinguish which parts of the system are the most vulnerable.

5.1.4. Mitigation potential

By reviewing the results of mitigation potential analysis, one may notice an overrepresentation of mitigation measures aiming in '*Reduction of the likelihood that the hazard will occur*' or '*Reduction of the likelihood that the hazard results in an accident*' (see Fig. 4). Other values were relatively rarely used as they consisted of complete hazard elimination or reduction of damage should the hazard/accident occur. This can be attributed to the fact that little can be done to completely eliminate the likelihood of certain hazards at this stage of technology's development as well as the level of detail in which the system is analysed. This is particularly apparent when discussing the mitigation potential of various procedures – they themselves were to large extent assigned value '3': '*Reduction of the likelihood that the hazard will occur*' (#1,4,10c,33 and 35), but it must be kept in mind that the procedures' existence does not mitigate the hazard by itself. It is humans writing or following them that do so.

5.1.5. Remote control issues

As mentioned before, should the hazard occur on board and lead to an accident, the operator located some hundreds miles away may find himself in a position in which (s)he has very little or no means of affecting the way in which such a situation develops. Causes for that can be sought in a trait of remote control itself, where operators are unable to make the necessary manual adjustments. As argued in (Wróbel et al., 2017), this can have massive consequences for unmanned vessels, where at some point failures can propagate rapidly (Wróbel et al., 2016). Such propagation could be interrupted onboard manned vessels operated nowadays, in which case a crew would step in and fight the emergency.

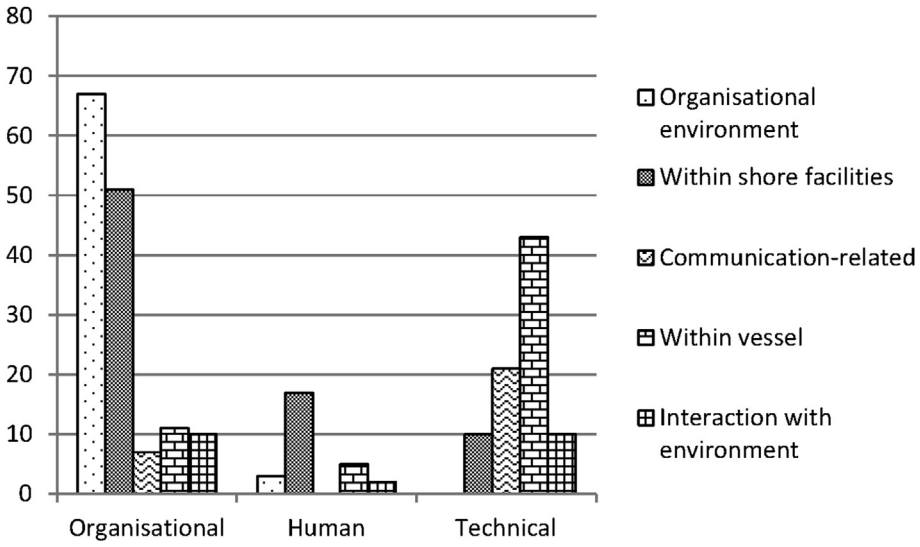

Fig. 3. Breakdown of potential causes of control functions' inadequacy.

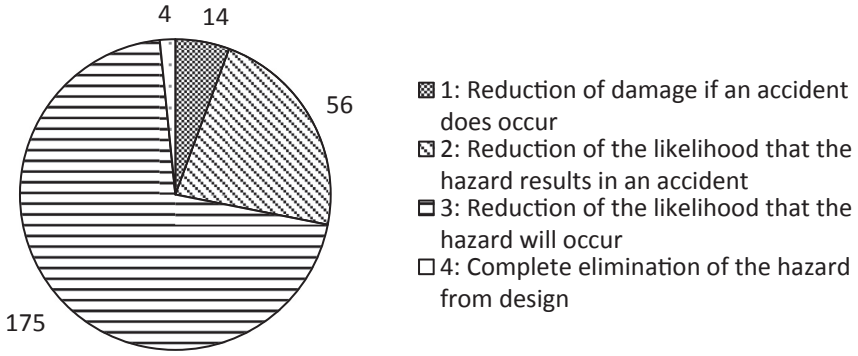

Fig. 4. Breakdown of mitigation potential assigned to mitigation measures.

Therefore, it might prove best to focus on reducing the likelihood of control becoming inadequate.

As can be seen in the mitigation potential analysis, some of the worst results pertain to ensuring both way communication between the shore-based control centre and the vessel (#15 through 18). If such a link is broken, information cannot be transmitted from vessel to operator and, in turn, his/her decisions cannot be relayed to the vessel, which becomes uncontrollable.

The issue of the operator's actual influence on the vessel's performance and potential consequences of inability to provide secure and efficient communication between them raises yet another concern. It will be necessary to compose a contingency plan aiming in failing to safe in case the communication link ceases operation. Automatic shutdown of propulsion and commencement of drifting might seem to be a tempting idea, but a possibility that such failure will occur in a frequented waters or where the currents are strong must not be neglected. If so, it might be better to embed a fail-safe mechanism consisting of autonomous steering into safer waters (control functions #17 & 18). In that case, the necessity of having efficient autonomous control algorithms as a backup makes remote control impractical. Perhaps the fact that the communication link between operator and the vessel is so vital and vulnerable will actually make AL-5 safer than AL-3, contrary to logic or at least intuition. They both argue that a human operator should be a backup for machine, not the other way around. Hence, AL-3 and AL-5 can both be considered as a backup for the other. Which of these will prove easier to implement and operate, will depend on actual operational circumstances and their design and are likely to be the subject of more detailed study once more data is available.

Nevertheless, an ultimate contingency planning on regaining control over a dead ship shall be elaborated, which might require dispatching a salvors' team to embark the vessel no matter its position, even in the middle of the ocean, before she sinks or becomes impossible to trace. Calculation of potential costs of such operation might successfully divert shipping company decision makers' attention to resilience engineering.

5.1.6. Hazards' mitigation

Mitigation of many hazards can be achieved by introducing the redundancy to some safety-critical subsystems or devices (#16–20 and 25). Although such an approach is said to be non-optimal (Leveson, 2011), it proved successful when ensuring the safety of complex systems, although sometimes at the expense of cost-effectiveness and higher initial investments. Since the redundancy is often named as the first-choice-solution, it is also mentioned as a measure of ensuring numerous control functions' adequacy. Despite any other effort taken to ensure the adequacy of control function, it may prove useful as a final line of defence against thrusters' failure, for instance.

Apart from the design of the vessel, its control algorithms and other technical issues, operational procedures and training shall also be in focus. Insufficient training of operators or incorrect information within a manual can lead to many of the listed control functions becoming inadequate (#10a,10c,13,25 for instance). On the other hand, if the procedures are easy to understand and properly encompass the situation, they might work as a good measure of mitigation. The same can be attributed to the training: a well-trained and experienced operator having adequate control over the vessel can find the best solution to the situation encountered. His/her attitude can prevent both omission and

commission errors from happening.

5.1.7. Protection against controls degradation

As for the protection against control degradation, the proper attitude of decision makers and operators (#5a,9,12,13,32), procedures on the maintenance of equipment (#25) and accident/incident investigations (#3,6a,10a,12,31) can be listed as feasible. Most of them are also included as a primary means of mitigating the control functions' inadequacy. To this point, we can argue that skill degradation and over-reliance on the automation can cause a system's overall degradation and shall be fought against with full commitment of all personnel involved in any level of system's hierarchy (Foreman et al., 2015).

5.2. Uncertainties

Although system-theoretic methods are believed to provide more insightful models of analysed systems' behaviour or accidents than previously used ones, they are not free from uncertainties. In the remotely operated merchant vessel's case, these will mainly originate from the assumption that the analysed model of the system is a sound representation of a real one (which is still in a concept phase and is liable to change). Therefore, they will propagate from system's safety control structure formulation into further steps of the analysis.

There are two major approaches to dealing with the uncertainties: reduction by improved modelling and better information (Bjerga et al., 2016). Normally in STPA, the uncertainties are reduced by a better modelling of the system, which is impossible since this study is merely one of first steps in the iterative process of a safety-driven design. The only remaining approach to uncertainties' treatment is therefore their better communication. Since the very aim of safety assessment is to inform decision-makers and managers on potential hazards related to certain operations (Flage and Aven, 2009), such as unmanned navigation, it is also essential to consider the possibility of error (Goerlandt and Reniers, 2016) and make the future users of the study aware of potential drawbacks of the analysis. Having data on the strength of analysts' statements, the final users could make better-informed decisions (Bjerga et al., 2016).

Therefore, a method of classifying uncertainties as suggested in (Flage and Aven, 2009) can be applied. It is argued that the uncertainty can be minor, moderate or significant. Particular values are assigned by the analysts based on guidelines as given in Table 4.

When conducting hazard analysis, particularly of a system to be built in future, it is also essential to address the so-called black swans: scenarios that for some reason have not been analysed. These are divided into three groups:

a) Unknown unknowns: events that were completely unknown to the scientific environment;
b) Unknown knowns: events that were not on the list of known events from the perspective of those who carried out a safety analysis, but were better acknowledged by others (Aven, 2015);
c) Known unknowns: events, existence of which was expected by analysts, but no further data pertaining to them could be elaborated (Flage and Aven, 2015).

With respect to the above taxonomy, potential causes of uncertainty pertaining to the study are listed in Table 5 together with significance category.

As can be seen in Table 5, larger uncertainties pertain to earlier phases of model creation and hazard analysis. As the assessment proceeds, consecutive stages can be assigned a lesser likelihood of black swans' existence. Such a situation generates the phenomenon that at some stage, little more can be said about the system, unless certain issues are resolved on earlier stages. In the remotely-controlled vessel's case, this will require carrying out an actual design of the system and then the iterative process of (1) assessing its safety, (2) creating recommendations for design improvement, (3) implementing them if feasible, (4) assessing the safety of upgraded model, and so on, as mentioned in Section 2.2.

Table 4
Uncertainty categories, based on (Flage and Aven, 2009).

Category	Description
Significant	One or more of the following is met: *The phenomena involved are not well understood, models are non-existent or known/believed to give poor predictions;* *The assumptions made represent strong simplifications;* *Data are not available, or are unreliable;* *There is lack of agreement/consensus among experts.*
Minor	All of the following conditions are met: *The phenomena involved are well understood, the models used are known to give predictions with the required accuracy;* *The assumptions made are seen as very reasonable;* *Much reliable data are available;* *There is broad agreement among experts.*
Moderate	Conditions between those characterising significant and minor uncertainty, for instance: *The phenomena involved are well understood, but the models used are considered simple/crude;* *Some reliable data are available.*

Table 5
Black swans present in remotely operated vessel's STPA.

Black swan	Items	Category
Unknown unknowns	Incomplete list of hazards	Moderate
	Incomplete list of potential causes of function's inadequacy	Moderate
Unknown knowns	Improper model of safety control structure	Significant
	Incomplete list of control functions	Moderate
Known unknowns	Incomplete list of mitigation measures	Moderate
	Improper mitigation potential values assigned	Moderate
	Unknown effectiveness of mitigation measures	Moderate
	Incomplete list of degradation protection measures	Moderate

Another dimension of uncertainty can be observed within some of the items as listed in Table 5. To this point, it cannot be elaborated which of the control functions has the greatest impact on the system's overall safety performance. The likelihood and consequences of each of the control functions becoming inadequate can be different and depends on various factors, just to name their position within the system or human element's impact on it. Similarly, mitigation measures actual rather than potential effectiveness should be analysed. Even having the same mitigation potential assigned, some can still be more feasible than others. In order to address these issues, more empirical data is required or a new method of compiling the existing one.

Summing up, we are in the position that at the current level of remotely-controlled merchant vessel technology's development and volume of publicly available information pertaining to its future shape, the performed qualitative analysis cannot be further enhanced at this point. For instance, as remotely-controlled vessels' performance will depend on its software's integrity, this must be first developed to proceed with the safety assessment any further. The fact that control algorithms will be contained in virtually any of system's components as depicted in Fig. 2. gives decent impression of how much work needs to be done.

Since STAMP and STPA are *per se* reported to be efficient tools for hazard identification and assessment (Altabbakh et al., 2014; Bjerga et al., 2016; Leveson, 2011), vast majority of the uncertainties will result from data unavailability (due to technology being innovative). This novelty also does not permit uncertainties' to be reduced through better modelling of the system in question, thus only can they be evaluated and communicated. Nevertheless, such communication can indicate areas in which the further research shall be conducted in order to collect more data and reduce the uncertainties themselves. It also helps assess the validity of the study.

6. Conclusions

The preliminary safety control structure and hazards' list has been created for the system whose purpose will be to ensure remotely-controlled merchant vessel's navigation and cargo transportation without negatively affecting the overall level of maritime safety. The structure has then been analysed in accordance with System-Theoretic Process Analysis framework. Scenarios in which particular control functions can become ineffective or inadequate have been identified. Furthermore, potential mitigation measures have been examined and evaluated with some recommendations given. The purpose of the research was to provide further designers of similar systems with these recommendations. By achieving that, we fulfilled the very aim of our study.

Results indicate that the implementation of remotely-controlled merchant vessels and, in a wider sense, unmanned ships, and ensuring their safety shall consist of executing various controls on regulatory, organisational and technical plains. They must all be in place and their effectiveness must be secured. Furthermore, the potential degradation of this fragile structure over time must be constantly counteracted, in which training and proper attitude of the decision-makers can be vital.

Uncertainties discussed pertain mainly to insufficient data on how the vessels in question will in fact be operated. Providing such information can propel further, more detailed safety assessments, and vice versa. The hereby paper is just one of the first steps in this long, iterative process. The development of technology shall be an unending process, and the same should apply to the safety assessment.

In addition to that, the safety of merchant vessels having potential of being operated in an autonomous mode shall be investigated. Further attention shall be directed at minimalizing uncertainties.

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). Second author appreciates also the financial contributions from Polish Ministry of Science and Higher Education, grant number DS/442/2017, duration 2017-2019. The views expressed remain solely those of the authors.

We are grateful to Mr. Risto Tuominen and Mr. Risto Tiusanen for their valuable advice on the model of safety control structure. Mr. Owen Jones helped us improve the language of the paper.

Appendix A. Supplementary data

Supplementary data related to this article can be found at https://doi.org/10.1016/j.oceaneng.2018.01.020.

References

AAWA, 2016. Remote and Autonomous Ships the Next Steps. London.
Abrecht, B., 2016. Systems Theoretic Process Analysis (STPA) of an Offshore Supply Vessel Dynamic Positioning System. Massachusetts Institute of Technology.
Ahmed, Y.A., Hasegawa, K., 2013. Automatic ship berthing using artificial neural network trained by consistent teaching data using nonlinear programming method. Eng. Appl. Artif. Intell. 1–18. https://doi.org/10.1016/j.engappai.2013.08.009.
Ahvenjärvi, S., 2016. The human element and autonomous ships. TransNav Int. J. Mar. Navig. Saf. Sea Transp 10, 517–521. https://doi.org/10.12716/1001.10.03.18.
Allianz, 2015. Safety and Shipping Review 2015. Munich.
Altabbakh, H., AlKazimi, M.A., Murray, S., Grantham, K., 2014. STAMP - holistic system safety approach or just another risk model? J. Loss Prev. Process. Ind. 32, 109–119. https://doi.org/10.1016/j.jlp.2014.07.010.
Aps, R., Fetissov, M., Goerlandt, F., Helferich, J., Kopti, M., Kujala, P., 2015. Towards STAMP based dynamic safety management of eco-socio- technical maritime transport system. Procedia Eng 128, 64–73. https://doi.org/10.1016/j.proeng.2015.11.505.
Aven, T., 2015. Implications of black swans to the foundations and practice of risk assessment and management. Reliab. Eng. Syst. Saf. 134, 83–91. https://doi.org/10.1016/j.ress.2014.10.004.
Bertram, V., 2002. Technologies for Low-crew/No-crew Ships (Forum Captain Computer. Brest).
Bitner, M., Starościk, R., Szczerba, P., 2014. Czy Robot Zabierze Ci Pracę? Sektorowa Analiza Komputeryzacji I Robotyzacji Europejskich Rynków Pracy. Warszawa.
Bjerga, T., Aven, T., Zio, E., 2016. Uncertainty treatment in risk analysis of complex systems: the cases of STAMP and FRAM. Reliab. Eng. Syst. Saf. 156, 203–209. https://doi.org/10.1016/j.ress.2016.08.004.
Burmeister, H.-C., Bruhn, W., Rødseth, Ø.J., Porathe, T., 2014a. Autonomous Unmanned Merchant Vessel and its Contribution towards the e-Navigation Implementation: the MUNIN Perspective1. Int. J. e-Navigation Marit. Econ 1, 1–13. https://doi.org/10.1016/j.enavi.2014.12.002.
Burmeister, H.-C., Bruhn, W.C., Rødseth, Ø.J., Porathe, T., 2014b. Can unmanned ships improve navigational safety?. In: Proceedings of the Transport Research Arena. Paris.
Dobryakova, L., Lemieszewski, Ł., Ochin, E., 2015. The vulnerability of unmanned vehicles to terrorist attacks such as GNSS-spoofing. In: Marine Traffic Engineering and International Symposium Information on Ships. Kołobrzeg, pp. 100–111.
Dulac, N., Leveson, N.G., 2009. Incorporating safety in early system architecture trade studies. J. Spacecraft Rockets 46, 430–437.
Filipowicz, W., Neumann, T., 2008. Problem of detecting objects and of covering an area. Sci. J. Marit. Univ. Szczecin 13, 10–14.
Flage, R., Aven, T., 2015. Emerging risk – conceptual definition and a relation to black swan type of events. Reliab. Eng. Syst. Saf. 144, 61–67. https://doi.org/10.1016/j.ress.2015.07.008.
Flage, R., Aven, T., 2009. Expressing and communicating uncertainty in relation to quantitative risk analysis. Reliab. Risk Anal. Theory Appl. 2, 9–18.
Foreman, V.L., Favaró, F.M., Saleh, J.H., Johnson, C.W., 2015. Software in military aviation and drone mishaps: analysis and recommendations for the investigation process. Reliab. Eng. Syst. Saf. 137, 101–111. https://doi.org/10.1016/j.ress.2015.01.006.
Goerlandt, F., Reniers, G., 2016. On the assessment of uncertainty in risk diagrams. Saf. Sci. 84, 67–77. https://doi.org/10.1016/j.ssci.2015.12.001.
Grøtli, E.I., Reinen, T.A., Grythe, K., Transeth, A.A., Vagia, M., Bjerkeng, M.C., Rundtop, P., Svendsen, E., Rødseth, Ø.J., Eidnes, G., 2015. Design, development and validation of marine autonomous systems and operations. In: Beslutningsstøtte Og Alarmsystemer.
Heikkilä, E., Tuominen, R., Tiusanen, R., Montewka, J., Kujala, P., 2017. Safety qualification process for an autonomous ship prototype - a goal-based safety case approach. In: Marine Navigation. CRC Press, Gdynia, pp. 365–370. https://doi.org/10.1201/9781315099132-63.
Hogg, T., Ghosh, S., 2016. Autonomous merchant vessels: examination of factors that impact the effective implementation of unmanned ships. Aust. J. Marit. Ocean Aff 8, 206–222. https://doi.org/10.1080/18366503.2016.1229244.
Hollnagel, E., 2014. Is safety a subject for science? Saf. Sci. 67, 21–24. https://doi.org/10.1016/j.ssci.2013.07.025.
Hooydonk, E. Van, 2014. The law of unmanned merchant shipping – an exploration. J. Int. Marit. Law 20, 403–423.
Höyhtyä, M., Ojanperä, T., Mäkelä, J., Ruponen, S., Järvensivu, P., 2017. Integrated 5G satellite-terrestrial systems: use cases for road safety and autonomous ships. In: 23rd Ka and Broadband Communications Conference. Trieste.
Iijima, Y., Hayashi, S., 1991. Study towards a 21st-century intelligent ship. J. Navig. 44, 184–193. https://doi.org/10.1017/S0373463300009929.
IMO, 2011. Principles of Minimum Safe Manning. London.
Jalonen, R., Tuominen, R., Wahlström, M., 2017. Safety of Unmanned Ships - Safe Shipping with Autonomous and Remote Controlled Ships. Espoo. Available at: https://aaltodoc.aalto.fi/handle/123456789/28061?show=full. (Accessed 23 January 2018).
Johansen, T.A., Perez, T., 2016. Unmanned aerial surveillance system for hazard collision avoidance in autonomous shipping. In: International Conference on Unmanned Aircraft Systems (ICUAS). IEEE, Arlington, VA, pp. 1056–1065. https://doi.org/10.1109/ICUAS.2016.7502542.
Kazaras, K., Kontogiannis, T., Kirytopoulos, K., 2014. Proactive assessment of breaches of safety constraints and causal organizational breakdowns in complex systems: a joint STAMP-VSM framework for safety assessment. Saf. Sci. 62, 233–247. https://doi.org/10.1016/j.ssci.2013.08.013.
Kee, D., Jun, G.T., Waterson, P., Haslam, R., 2017. A systemic analysis of South Korea Sewol ferry accident - striking a balance between learning and accountability. Appl. Ergon. 59, 504–516. https://doi.org/10.1016/j.apergo.2016.07.014.
Knudsen, F., 2009. Paperwork at the service of safety? Workers' reluctance against written procedures exemplified by the concept of "seamanship. Saf. Sci. 47, 295–303. https://doi.org/10.1016/j.ssci.2008.04.004.
Krata, P., Montewka, J., Hinz, T., 2016. Towards the Assessment of Critical Area in a Collision Encounter Accounting for. Pr. Nauk. Politech. Warsz, pp. 1–10. XX.
Krata, P., Szlapczynska, J., 2018. Ship weather routing optimization with dynamic constraints based on reliable synchronous roll prediction. Ocean Eng. 150, 124–137. Available at: https://www.sciencedirect.com/science/article/pii/S0029801817307874.
Krata, P., Wawrzynski, W., 2017. Prediction of ship resonant rolling - related dangerous zones with regard to the equivalent metacentric height governing natural frequency of roll. TransNav Int. J. Mar. Navig. Saf. Sea Transport. 11 (4), 607–614. Available at: http://www.transnav.eu/Article_Prediction_of_Ship_Resonant_Rolling_Krata,44,764.html. (Accessed 23 January 2018).
Kretschmann, L., Mcdowell, H., Rødseth, Ø.J., Fuller, B.S., Noble, H., Horahan, J., 2015a. Maritime Unmanned Navigation through Intelligence in Networks - Quantitative Assessment.

Kretschmann, L., Rødseth, Ø.J., Tjora, Å., Fuller, B.S., Noble, H., Horahan, J., 2015b. Maritime Unmanned Navigation through Intelligence in Networks - Qualitative Assessment.
Kwon, Y., 2016. System Theoretic Safety Analysis of the Sewol-ho Ferry Accident in South Korea. Massachusetts Institute of Technology.
Leveson, N.G., 2011. Engineering a Safer World - Systems Thinking Applied to Safety. MIT Press, Cambridge, MA.
Leveson, N.G., 2002. System Safety Engineering: Back to the Future. Massachusetts Institute of Technology.
LR, 2016. Cyber-enabled Ships ShipRight Procedure – Autonomous Ships. Southampton.
Man, Y., Lundh, M., Porathe, T., 2014. 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 7, 231.
Man, Y., Lundh, M., Porathe, T., Mackinnon, S., 2015. From desk to field - human factor issues in remote monitoring and controlling of autonomous unmanned vessels. Procedia Manuf 3, 2674–2681. https://doi.org/10.1016/j.promfg.2015.07.635.
Mazaheri, A., Montewka, J., Nisula, J., Kujala, P., 2015. Usability of accident and incident reports for evidence-based risk modeling - a case study on ship grounding reports. Saf. Sci. 76, 202–214. https://doi.org/10.1016/j.ssci.2015.02.019.
Montewka, J., Goerlandt, F., Innes-Jones, G., Owen, D., Hifi, Y., Puisa, R., 2017. Enhancing human performance in ship operations by modifying global design factors at the design stage. Reliab. Eng. Syst. Saf. 159, 283–300. https://doi.org/10.1016/j.ress.2016.11.009.
Norman, D.A., 1989. The "Problem" of Automation: Inappropriate Feedback and Interaction, Not "Overautomation." San Diego.
Owens, B.D., Herring, M.S., Dulac, N., Leveson, N.G., Ingham, M.D., Weiss, K.A., 2008. Application of a Safety-driven Design Methodology to an Outer Planet Exploration Mission.
Porathe, T., 2016. 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 14, 233–242. https://doi.org/10.1016/j.trpro.2016.05.060.
Porathe, T., Prison, J., Man, Y., 2014. Situation awareness in remote control centres for unmanned ships. In: Human Factors in Ship Design & Operation. London, pp. 1–9.
Rødseth, H., Brage, M., 2014. Maintenance management for unmanned shipping. In: Volker, B. (Ed.), 13 Th Conference on Computer and IT Applications in the Maritime Industries COMPIT'14. Redworth, pp. 277–290.
Rødseth, Ø.J., Burmeister, H.-C., 2015a. Risk assessment for an unmanned merchant ship. TransNav. Int. J. Mar. Navig. Saf. Sea Transp 9, 357–364. https://doi.org/10.12716/1001.09.03.08.
Rødseth, Ø.J., Burmeister, H.-C., 2015b. New Ship Designs for Autonomous Vessels.
Rødseth, Ø.J., Burmeister, H.-C., 2012. Developments toward the Unmanned Ship.
Rødseth, Ø.J., Lee, K., 2015. Secure communication for e-navigation and remote control of unmanned ships. In: Volker, B. (Ed.), Proceedings of the 14th Conference on Computer and IT Applications in the Maritime Industries-compit. Ulrichshusen, pp. 44–56.
Rødseth, Ø.J., Tjora, Å., 2014a. A system architecture for an unmanned ship. In: 13th International Conference on Computer and IT Applications in the Maritime Industries (COMPIT 2014). Redworth, pp. 291–302.
Rødseth, Ø.J., Tjora, Å., 2014b. A risk based approach to the design of unmanned ship control systems. In: Ehlers, S., Asbjørnslett, B.E., Rødseth, Ø.J., Berg, T.E. (Eds.), Proceeding of the Conference on Maritime-port Technology. Taylor & Francis Group, Trondheim, pp. 153–162.
Rødseth, Ø.J., Tjora, Å., Baltzersen, P., 2013. Maritime Unmanned Navigation through Intelligence in Networks - Architecture Specification.
Salmon, P.M., Cornelissen, M., Trotter, M., 2012. Systems-based accident analysis methods: a comparison of Accimap, HFACS, and STAMP. Saf. Sci. 50, 1158–1170. https://doi.org/10.1016/j.ssci.2011.11.009.
Salmon, P.M., Walker, G.H., Stanton, N.A., 2015. Pilot error versus sociotechnical systems failure: a distributed situation awareness analysis of Air France 447. Theor. Issues Ergon. Sci. 64–79. https://doi.org/10.1080/1463922X.2015.1106618.
Stokey, R., Austin, T., von Alt, C., Purcell, M., Goldsborough, R., Forrester, N., Allen, B., 1999. AUV bloopers or why murphy must have been an optimist: a practical look at achieving mission level reliability in an autonomous underwater vehicle. In: 11th Int. Symp. Unmanned, Untethered, Submers. Technol. (UUST '99), pp. 32–40.
Stoop, J., Dekker, S., 2012. Are safety investigations pro-active? Saf. Sci. 50, 1422–1430. https://doi.org/10.1016/j.ssci.2011.03.004.
Theunissen, E., 2014. Navigation of unmanned vessels – history, enablers, challenges and potential solutions. In: 12th International Naval Engineering Conference and Exhibition. Amsterdam.
Van Den Boogaard, M., Feys, A., Overbeek, M., Le Poole, J., Hekkenberg, R., 2016. Control concepts for navigation of autonomous ships in ports. In: 10th Symposium on High-performance Marine Vehicles. Cortona.
Wahlström, M., Hakulinen, J., Karvonen, H., Lindborg, I., 2015. Human factors challenges in unmanned ship operations – insights from other domains. In: 6th International Conference on Applied Human Factors and Ergonomics. Elsevier B.V., pp. 1038–1045. https://doi.org/10.1016/j.promfg.2015.07.167
Wawrzyński, W., Krata, P., 2016a. Method for ship's rolling period prediction with regard to non-linearity of GZ curve. J. Theor. Appl. Mech. 54, 1329–1343.
Wawrzyński, W., Krata, P., 2016b. On ship roll resonance frequency. Ocean Eng. 126, 92–114. Available at: http://www.sciencedirect.com.libproxy.aalto.fi/science/article/pii/S0029801816303602. (Accessed 10 April 2017).
Willey, R.J., 2014. Consider the role of safety layers in the bhopal disaster. Chem. Eng. Prog. 110, 22–27.
Wróbel, K., Krata, P., Montewka, J., Hinz, T., 2016. Towards the development of a risk model for unmanned vessels design and operations. TransNav Int. J. Mar. Navig. Saf. Sea Transp 10, 267–274. https://doi.org/10.12716/1001.10.02.09.
Wróbel, K., Montewka, J., Kujala, P., 2017. Towards the assessment of potential impact of unmanned vessels on maritime transportation safety. Reliab. Eng. Syst. Saf. 165, 155–169. https://doi.org/10.1016/j.ress.2017.03.029.