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

A R T I C L E I N F O

Keywords:
Unmanned vessels
Remote operation
STAMP
STPA
Safety of transportation

A B S T R A C T

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

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.

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.

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.

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