Safety Science 131 (2020) 104908

Contents lists available at ScienceDirect

Safety Science

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

A novel cyber-risk assessment method for ship systems

Victor Bolbot[a,*], Gerasimos Theotokatos[a], Evangelos Boulougouris[a], Dracos Vassalos[a]

[a] Maritime Safety Research Centre, University of Strathclyde, UK

ARTICLE INFO

Keywords:
Cybersecurity
Safety
Autonomous inland waterway vessel
Navigation and propulsion systems

ABSTRACT

Recent advances in the maritime industry include research and development of new sophisticated ships with a number of smart functionalities and enhanced autonomy. The new functions and autonomy levels though come at the cost of increased connectivity. This results in increased ship vulnerability to cyber-attacks, which may lead to financial loss, environmental pollution, safety accidents. The aim of this study is to propose a novel method for cybersecurity risk assessment of ship systems. In this novel method, the Cyber-Preliminary Hazard Analysis method steps are enriched with new steps supporting the identification of cyber-attack scenarios and the risk assessment implementation. The proposed method is applied for the cyber-risk assessment and design enhancement of the navigation and propulsion systems of an inland waterways autonomous vessel. The results demonstrate that several critical scenarios can arise on the investigated autonomous vessel due to known vulnerabilities. These can be sufficiently controlled by introducing appropriate modifications to the systems design.

1. Introduction

1.1. Background

Cyber-Physical Systems (CPSs) represent a class of systems consisting of software and hardware components, which are used to control physical processes (Gunes et al., 2014). CPSs have been advancing in a number of application areas, including the maritime industry (DNV GL, 2015). CPSs are expected to increase the productivity and safety levels by removing, substituting and/or supporting the operator in the decision-making process, thus reducing the number of human errors leading to accidents. Typical examples of the existing marine CPSs include the Diesel-Electric Propulsion plant, the Safety Monitoring and Control System, the Dynamic Positioning System as well as the Heating, Ventilation & Air Conditioning systems (DNV GL, 2015). The number of the CPSs is expected to increase in autonomous ships, which are considered to be the ultimate marine CPS.

The maritime industry has demonstrated a strong interest in the development of the next generation ships such as smart ships or autonomous ships, employing CPSs. Examples of relevant projects include the autonomous Yara Birkenland ship design and construction (Yara, 2018), as well as the MUNIN (MUNIN, 2016), AAWA (AAWA, 2016), SISU and SVAN (Daffey, 2018) projects. The most recent initiative is the AUTOSHIP project (AUTOSHIP, 2019), which aims at converting a short sea going vessel (as a demonstrator) and an inland waterways vessel (as a demonstrator too) into autonomous vessels, thus pushing the available technology and autonomy levels further on larger size vessels.

The introduction of CPSs is accompanied by an increased complexity attributed to the heterogeneous character of the installed CPSs, the dependence on information exchanging with other systems, the additional new interactions with humans, the increased number of controllers running complex software and the increased interconnectivity required for implementing the desired CPSs' functionalities (Bolbot et al., 2019c). All these parameters, especially the latter, introduce new hazards, as cyber-attacks can exploit vulnerabilities in the communication links and directly affect the integrity or availability of the data and control systems, leading to accidents (Bolbot et al., 2019c; Eloranta and Whitehead, 2016).

A number of incidents have been reported with unauthorised people gaining access to various conventional ship control systems. In one case, the Electronic Chart Display Information System (ECDIS) was infected, resulting in a disruption of the ship operation with significant financial consequences (BIMCO, 2018a). In another attack, the ECDIS updates constituted a bridge for implementing the attack on a radar system allowing the attacker to manipulate the radar measurements displayed on screen (Wingrove, 2017). In another case, a malware was installed through a USB memory stick on a power management system, degrading its performance (BIMCO, 2018a). Satellite communication systems of another ship were also compromised by white hackers via a tracking system due to weak passwords (Doyle, 2017; Munro, 2017). Global Positioning System (GPS) spoofing attacks were reported in the

* Corresponding author.
E-mail address: victor.bolbot@strath.ac.uk (V. Bolbot).

https://doi.org/10.1016/j.ssci.2020.104908
Received 23 January 2020; Received in revised form 22 June 2020; Accepted 6 July 2020

Black sea during a military exercise, where the ships suddenly were "found" over 32 km inland (Newman, 2019). Even unknown outdated systems were found installed on ships, which constitute a potential entry point to the ship control systems (Rider, 2020). These incidents are indicative as there are numerous reported cases of cyber-attacks in shipping operations e.g. (BIMCO, 2018a; Bradbury, 2019; Marine Electronics and Communications, 2017; Santamarta, 2015; U.S. Coast Guard, 2019).

Important lessons can be learnt from these incidents, such as, which ships systems, how they can be compromised, and what might be the potential consequences. However, due to the novelty of this issue and underreporting, there are no reliable statistics with respect to the frequency of cyber-attacks (Tam and Jones, 2019). There exist some generic statistics available or questionnaire results, which can provide only indicative information (BIMCO, 2018b). In addition, some malware can remain dormant in a ship for prolonged time, which impedes the obtaining of accurate data (BIMCO, 2018a). Furthermore, the systems have constantly been evolving (Bolbot et al., 2019c), new vulnerabilities have been found and new attack types have been developed, which incommode the identification and prediction of potential attack scenarios based on the available accidents and incidents data.

Considering the recent developments, it is expected that ships and especially autonomous ships will attract more attention from different hacker groups and the number of these incidents will increase. Therefore, there is a need to ensure that these attack scenarios are identified and properly addressed.

The ships can be viewed as complex industrial and transport systems, where Information Technology (IT) is strongly intertwined with Operational Technology (OT) (BIMCO, 2018a; International Maritime Organisation (IMO), 2017). It is important therefore to consider not only the financial but also the safety and environmental impact of successful cyber-attacks (BIMCO, 2018a; BV, 2018). However, different attack types can be applied to different components, might have different consequences and also different control barriers (Flaus, 2019). The classical hazard identification and analysis methods, properly modified, can support the identification of inadvertent attack scenarios and their control measures in systems (Flaus, 2019; Kriaa et al., 2015). Nevertheless, due to the scarcity of the available data mentioned previously, it is necessary to support the scenarios ranking process to allow for a cost-efficient designenhancement. In this respect, the likelihood and the attack scenarios will be affected by the specific attack group goal (Tam and Jones, 2019), which can be used to support the identification and ranking of these scenarios. As it is referred to the marine systems, it is also essential to ensure that these systems risk is in accordance with acceptable maritime criteria. As the whole context has constantly been evolving (Bolbot et al., 2019c), it is crucial to ensure that the method allows for the easy reassessment of scenarios when new vulnerabilities are identified or new systems are installed.

Summarising the above, it is important to: (a) consider in more detail the potential types and consequences of cyber-attacks on ship systems; (b) incorporate the different attack groups interests and activity levels; (c) facilitate and guide the ranking process; (d) be aligned with the existing processes in the maritime industry; (e) guide the system design enhancement.

1.2. Literature review

A number of standards are available for systems cybersecurity assessment and assurance, including ISO 27000 series standards (ISO/IEC, 2016), NIST SP 800 series standards (NIST, 2019), IEC 62433 series standards (IEC, 2018) and specific standards in automotive and aerospace industries (Flaus, 2019). As there is an increasing number of concerns with respect to the ship systems vulnerability to cyber-attacks in the maritime industry, a number of guidelines have been developed to address potential threats (ABS, 2018; BIMCO, 2018a; Boyes and Isbell, 2017; BV, 2018; ClassNK, 2019; DNV GL, 2016, 2019; IMO, 2016a, 2017; LR, 2019; Maritime affairs directorate of France, 2016; United States Coast Guard, 2015).

In addition, a number of previous research studies focused on the high-level cyber security assessment of the ship control systems and ship networks in autonomous ships. Jones et al. (2016) provided an overview of different attack scenarios for a typical cargo ship. Tam and Jones (2019) proposed a model-based approach for the risk assessment of cyber-threats named MaCRA (Maritime Cyber-Risk Assessment) by considering the technological systems vulnerabilities as well as the ease-of-exploiting and the potential hackers rewards. Using the same model-based approach, Tam and Jones (2018) implemented a risk assessment for a number of vessels including Yara Birkenland, Rolls Royce AAWA ocean-going reduced crew vessel and Mayflower autonomous ship. Kavallieratos et al. (2019) employed the STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service and Elevation of Privilege) method to assess risks in a generic autonomous vessel.

Other approaches used more detailed methods for cyber-security analysis. Omitola et al. (2018) analysed an unmanned surface vessel navigation system using the System-Theoretic Process Analysis for cyber-attacks (STPA-sec) targeting at modifying data that are provided as input to the vessel navigation system. Shang et al. (2019) combined attack trees with fuzzy ranking for assessing the likelihood of successful cyberattacks on ship propulsion/power generation systems. Guzman et al. (2019) suggested a new method, named uncontrolled flows of information and energy, which uses diagrammatic dependencies within CPSs for risk analysis of the collision avoidance function of an autonomous surface vessel. Svilicic et al. (2019a) proposed a risk assessment framework, which is based on a combination of questionnaires, vulnerability scanning and penetration testing results. Glomsrud and Xie (2019) suggested the use of the STPA with attack trees for the safety assessment of autonomous vessel. Kavallieratos et al. (2020) used STPA with security analysis in parallel for identification of safety and security requirements.

Nevertheless, the previously presented methods and standards do not seem to address properly the needs of cyber-risk assessment for maritime assets, as explained below. ISO 27000 (ISO/IEC, 2016) suggests a generic risk assessment framework, which might not be well adjusted to the industrial systems, such as ships, as the consequences are expressed in asset value and not in terms of safety, environmental and other consequences metrics. IEC 62443 (IEC, 2018) is a standard for industrial systems security, and the approach is not suitably "marinised". The NIST SP800-37 approach (NIST, 2019) focuses on the cyberattacks impact in terms of integrity, availability and confidentiality, which needs however an additional step to consider the potential safety, environmental and financial implications due to the loss of integrity, availability and confidentiality. The class societies rules for cyber-risk assessment are more suitable for ship systems; however they might either refer to other standards as IEC 62443 for carrying out the risk assessment process (LR, 2019), provide generic guidelines (ABS, 2018), assess consequences in terms of integrity, availability and confidentiality (BIMCO, 2018a; ClassNK, 2019; DNV GL, 2016) or lack in description of potential attacks types which will affect the consequences (BV, 2018).

In many of the previous research studies, such as Jones et al. (2016); Tam and Jones (2019) and Tam and Jones (2018), the risk assessment was implemented considering a high level system architecture, which does not support the system cybersecurity enhancement. The risk assessment using STRIDE, as in other studies (Kavallieratos et al., 2019), can be used to identify a number of potential attack scenarios but it did not address the safety-related consequences. The use of other approaches involving STPA (Omitola et al., 2018) and Attack Trees (Shang et al., 2019) or both (Glomsrud and Xie, 2019) can be rather labour intensive. It is deduced from previous STPA applications that this method may result in an overwhelming number of hazardous scenarios (Bolbot et al., 2020; Bolbot et al., 2019b; Bolbot et al., 2018). In

the authors view, such a detailed method would be beneficial to be applied after a less labour-intensive approach is used. Other approaches, as presented by Svilicic et al. (2019a), are applied in conjunction with ships systems penetration testing. This supports the risk assessment process but cannot be implemented prior to the actual system testing. Therefore, the generation of the relevant system requirements cannot be supported.

In addition, none of the previous studies conducted a risk assessment of an inland waterways autonomous vessel. Inland waterways autonomous vessels operate in a different environment in comparison to the short sea or ocean going vessels, with different systems requirements and size, and they can attract the interest from different hackers groups. For instance, it is much easier to embark an autonomous inland ship in comparison with ships that sail in open seas or in short shipping routes, but of course piracy incidents frequency will also depend on the operating area. Ships operation in canals imposes specific boundaries on the ship design, affecting the amount of transferred cargo and consequently the loss value. Additionally, autonomous inland waterways ships will use different communication protocols such as 4G, whereas ocean going ships might use satellite communication with shore. Therefore, the scenarios that can arise due to cyber-attacks and their likelihood can be different in an autonomous inland ship than in other types of ships.

In this respect, the aim of this study is to develop a novel method for conducting the risk assessment for cyber-attacks for ship systems including autonomous ships, which addresses the limitations of previous methods/approaches. The developed novel method is subsequently employed to conduct the cyber-attacks risk assessment for the navigation and propulsion systems of an inland waterways autonomous vessel. The novelty of the present research includes: (a) a novel method development for ships cyber risk assessment; (b) identification of potential vulnerabilities, attack vectors and control barriers for ships systems required to facilitate the method application; (c) identification of attack scenarios arising in the propulsion and navigation systems of the investigated inland autonomous ship, and; (e) identification of the safety/cyber security control measures/barriers for this ship.

The remaining of this article is organised as follows. The developed method for cyber-attacks risk assessment is presented in Section 2. A description of the investigated case study of the inland waterways vessel is provided in Section 3. The derived results along with their discussion are provided in Section 4. Finally, the main findings are summarised and suggestions for future research are provided in Section 5.

2. Proposed method for the cyber risk assessment in ships

2.1. Method rationale, overview and method novelty

The Cyber Preliminary Hazard Analysis (CPHA) is selected as the basis for the development of the novel method proposed in this study. This method is rather similar with classical HazId (Hazard Identification), which is widely used in maritime industry, so it can be easily understood and used by the safety engineers in its original form or a modified form. Furthermore, a similar approach based on CPHA has been adopted by Bureau Veritas (BV) according to their rules (BV, 2018). In addition, this approach seems to be more aligned with the IEC 62433 standard guidelines for cyber risk assessment of industrial systems, as HazId results are suggested to be used as input to the cyber risk assessment.

The developed method, named CYber-Risk Assessment for Marine Systems (CYRA-MS), consists of four phases (A to D) and follows in total ten steps, as illustrated in the flowchart depicted in Fig. 1. The method initiates with the identification of the system components and the mapping of the relevant connections/interactions (Step 1) as it is important first to sufficiently understand the investigated system. The proper understanding of component functions and interactions will support the identification of attack consequences. Subsequently, a specific attack group is selected for the analysis (Step 2), as different attack groups will focus on different attack scenarios. In parallel, based on the literature review and an existing vulnerabilities database, the existing vulnerabilities for the system components are identified (Step 3). The vulnerabilities are used to identify the potential attacks on various system components. Based on the specific attack group goal and vulnerabilities, the potential attacks types (Step 4) on the system components along with the potential consequences (Step 5) of each attack type are identified. In Step 6, an estimation for the success likelihood of each specific attack scenario is provided based on the following parameters: attack group goals, activity level, technological level, connectivity level, required resources for exploiting vulnerabilities and available control barriers. The different consequences are ranked in terms of their severity in Step 7. In Step 8, the control measures for each hazardous scenarios are identified/proposed. The scenarios risk is reassessed based on the new control measures in Step 9. In Step 10, the different safety requirements and suggestions for the system design are summarised based on previous steps. All these 10 Steps are elaborated in detail in the following sections.

The novelty of the CYRA-MS method compared to the CPHA include: (a) the consideration of attack group goals in the analysis; (b) the incorporation of different attack types; (c) estimating the likelihood of the successful attacks considering the attack group goals, activity level, technological level, connectivity level, required resources and available control barriers; (d) expanding the Formal Safety Assessment (FSA) consequences table to allow ranking of scenarios in financial, safety and environmental terms.

2.2. Phase A – Preparation for analysis (Steps 1–3)

The prerequisite for the CYRA-MS is the identification of: (a) the control system elements; (b) the control elements functions and functionalities; (c) the control system elements interfaces (sensors and actuators) with the physical word; (d) the controlled processes; (e) the interfaces among the control systems; (f) the data flow in the system, and; (g) the potential entry points into the system (physical and logical access points) (IEC, 2018). This is implemented in Step 1 (Fig. 1), by analysing the available system information and developing the system physical and logical mapping (Flaus, 2019). An example of what this information includes is provided in the results for the case study presented in Section 4.1 in Fig. 3 and Table 11.

As the attackers do not have neither the same motives nor the same resources when attacking a ship network (Tam and Jones, 2019), the attack scenarios assessed in Steps 4 to 7 (Fig. 1) for each attack group will vary. In this respect, the potential attack groups (or threat groups) are selected in Step 2 (Fig. 1). Using previous research studies (BIMCO, 2018a; Boyes and Isbell, 2017; BV, 2018; Flaus, 2019; IEC, 2011a; Tam and Jones, 2019), the attack groups were identified and presented in Table 1. The technological level of each attack group according to the Bureau Veritas (BV) guidelines is also presented in Table 1.

The known vulnerabilities, the potential entry points and attack types are identified in Step 3 (Fig. 1) by using the information provided in the following resources: (a) previous research publications e.g. (Flaus, 2019; Kavallieratos et al., 2019; Omitola et al., 2018; Tam and Jones, 2018); (b) the available maritime standards (BIMCO, 2018a; Boyes and Isbell, 2017; DNV GL, 2016; IMO, 2016a; Maritime affairs directorate of France, 2016); (c) relevant generic standards (IEC, 2011a), and; (d) the Cybersecurity and Infrastructure Security Agency (CISA) database (CISA, 2019a). A generic list of the vulnerabilities, the potential entry points and the attack types for the various system components, which are identified based on the existing literature and reported cyber-attack cases, is provided in Table B.1 in Appendix B. Whilst this list is provided in Table B.1, it is highly recommended to keep updating this list due the evolving nature of this area, as it is expected that new vulnerabilities and attack types will be discovered,

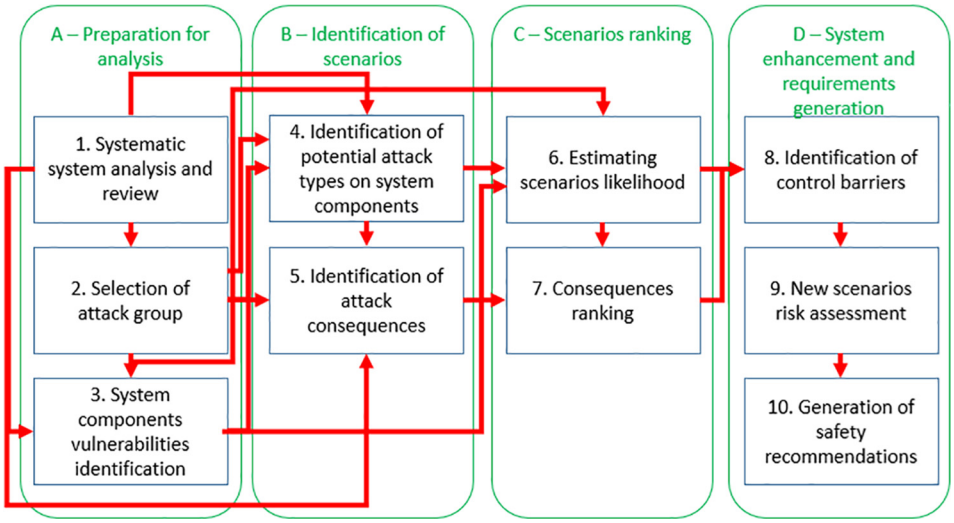

Fig. 1. CYRA-MS method flowchart.

Table 1
Identified attack groups.

a/a	Attack group	Goal	Technological level (TL)
1	Generic hackers	Spreading their malware around the web network to get ransom	1
2	Amateur hackers	Improving and training their hackings skills	2
3	Ethical hackers	Finding vulnerabilities in system with the goal to improve the system	2
4	Former malicious employees	Taking revenge from the ship operating company	3
5	Malicious external providers	Stealing the machinery/condition based data	3
6	Activists (Hacktivists)	Delay or cancel the introduction of autonomous vessels or of specific vessels	3
7	Criminal hackers	Stealing the ship, her cargo, components or seeking for a monetary reward	4
8	Competitors	Stealing valuable data or sabotaging and damaging the ship	4
9	Terrorists	Damaging the ship and/or causing fatalities	4
10	Criminals	Transferring illegal cargo or people	4
11	States	Damaging or taking control over the ship Developing non access/zero GPS zones	5

Table 2
Ship accident types (IMO, 2008).

Collision [A-1]
Grounding [A-2]
Contact [A-3]
Fire or explosion [A-4]
Hull failure/failure of watertight doors/ports etc. not caused by [A-1 – A-4], [A-5]
Machinery damage/damage to ship equipment [A-6]
Capsizing, listing or foundering not caused by [A-1 – A-6], [A-7]
Crew injury or death [A-8]

which may result in new attack scenarios.

2.3. Phase B – Identifying the attack scenarios (Steps 4–5)

Based on the goals of each attack group (from Step 2) as well as the system components vulnerabilities and attack vectors (from Step 3), the potential attack scenarios are identified in Step 4 (Fig. 1). The identification of the potential attack scenarios can be implemented with the assistance of Table B.1 which connects the system components with the potential attack types.

The system components functionalities (Step 1) and the attack group goal (Step 2) are used to derive the potential consequences of the attack scenarios in Step 5 analysis (Fig. 1). The potential consequences can be categorised in the following three different types: (a) safety consequences leading to violation of the safety requirements; (b) environmental consequences leading to environmental pollution, and; (c) financial consequences. The identification of potential safety and financial inadvertent effects is enhanced through the review of accidents lists for ships according to IMO list of incidents accidents (IMO, 2008), which are provided in Table 2. The potential environmental consequences according to MARPOL (IMO, 2016b) can be of two major types: air pollution or sea pollution. The financial consequences include: (a) loss or damage of ships systems; (b) loss or damage to ship cargo, and; (c) disruptions in ship operation and associated logistic chain leading to financial loss; and (d) potential legislation effects leading to financial losses. Steps 4 and 5 are not completely independent as the attack group goal affects both the targeted inadvertent scenario and the employed attack scenario.

2.4. Phase C – Scenarios ranking (Steps 6–7)

In Steps 6 and 7, the scenarios are ranked according to their expected likelihood and severity. However, as the cybersecurity issues are relatively new in the maritime industry, to the best of authors' knowledge, there are no reliable statistics for different attack scenarios. For this reason, a new methodological approach is suggested below.

The likelihood of each scenario (combination of attack and consequences) is affected by: (a) the level of exposure of each system (EL) to attacks due to the connectivity level (CL1) and the complexity level (CL2) (BV, 2018); (b) the interest of the specific attack group in an attack scenario (IL), (Tam and Jones, 2019); (c) the attacker technological level (TL) (BV, 2018); (d) each attack group activity level (AL) (EBIOS, 2019); (e) the ease of exploitation (EE) (Tam and Jones, 2019) and; (f) the vulnerability level due to the absence/presence as well as the effectiveness of mitigating and preventative barriers for each scenario (VL).

Therefore, the frequency (F) of the successful attack (events per ship-year) can be estimated according to the following equation:

Table 3
Ranking for successful attack scenarios (FI) and attack group activity level (AL).

Ranking (FI and AL)	Frequency	Definition of attack frequency	F (per ship-year)	F (per ship-hour)
7	Frequent	Likely to occur once per month on one ship	10	$1.14 \cdot 10^{-3}$
5	Reasonably probable	Likely to occur once per year in a fleet of 10 ships, i.e. likely to occur a few times during the ship's life	10^{-1}	$1.14 \cdot 10^{-5}$
3	Remote	Likely to occur once per year in a fleet of 1,000 ships, i.e. likely to occur in the total life of several similar ships	10^{-3}	$1.14 \cdot 10^{-7}$
1	Extremely remote	Likely to occur once in the lifetime (20 years) of a world fleet of 5,000 ships.	10^{-5}	$1.14 \cdot 10^{-9}$

Table 4
Determination of exposure level (EL) (BV, 2018).

Exposure level		Connectivity level (CL1)				
		1	2	3	4	5
Complexity level (CL2)	1	1	1	1	1	1
	2	2	2	2	2	2
	3	3	3	4	4	5

$$F = 10^{FI-6} = 10^{AL-6}10^{EL-5}10^{(IL-5)/2}10^{(TL-5)/2}10^{EE-5}10^{VL-6} \quad (1)$$

The consecutive terms in the right hand side part of Eq. (1) denote, respectively: the number of the attack attempts frequency (10^{AL-6})[attack per ship-year] ($AL \in \{1-7\}$), the probability of the attack success due to the system exposure (10^{EL-5}) [-] ($EL \in \{1-5\}$, the probability of the attack group interest in a specific scenario ($10^{(IL-5)/2}$) [-] ($IL \in \{1-5\}$), the probability of the attack success due to the attack group technological level ($10^{(TL-5)/2}$) [-] ($TL \in \{1-5\}$), the amount of resources required for a successful attack (10^{EE-5}) [-] ($EE \in \{1-5\}$), and the probability of the attack success due to the presence of protective barriers (10^{VL-6}) [-] ($VL \in \{1-6\}$). Practically, Eq. (1) considers that if a cyber-attack attempt is implemented (depicted by AL), its success will be dependent on all the other parameters values (EL, IL, TL, EE, VL).

The assumptions behind the Eq. (1) along with their justification are provided below in bullet points:

- The base of 10 has been used in similar way with Level Of Protection Analysis (LOPA) approach (British Standards Institution (BSI), 2004) and to allow the estimation of raking according to FSA.
- The probabilities of the attack group interest and technological level lie in the range from 0.01 to 1. This assumption can be viewed as aligned with the ANSSI 2013 approach (Flaus, 2019), where the attacker technological level is divided by 2.
- For estimating the system exposure level, ease of exploitation and vulnerability level, it is assumed that their probability values are in the range between 0.0001 and 1. In this respect, the considered assumption for the exposure level is aligned with the relevant procedures in the ANSSI 2013 approach (Flaus, 2019).
- For the vulnerability level, the underlying assumption is that each protective barrier can mitigate the 90% of relevant hazardous conditions. This is a rather conservative assumption with regard to the effectiveness of the mitigation barriers (British Standards Institution (BSI), 2004). This assumption can be overcome if appropriate evidence for the barrier effectiveness is provided. For instance, higher effectiveness can be assigned to protective barriers not based on digital technologies (Cormier and Ng, 2020).

The Frequency Index (FI) is calculated according to the following equation, which was derived by summing the exponents of Eq. (1), rounding up the calculated value (to avoid non-integer values) and considering that the FI minimum value is equal to 1:

$$FI = \max\left[\text{round}\left(\text{AL} + (\text{EL} - 5) + \frac{IL-5}{2} + \frac{TL-5}{2} + (\text{EE} - 5) + (\text{VL} - 6)\right), 1\right] \quad (2)$$

The activity level (AL) corresponds to the number of an attack attempts by a specific group. It is proposed to determine the AL by using a ranking developed based on Formal Safety Assessment (FSA) Frequency Index (IMO, 2018), since the proposed method is developed for marine systems applications. The categorisation and the respective frequency ranges considered in this study are provided in Table 3. For determining the level of exposure for each system, the method proposed in (BV, 2018) is employed. Thus, each system exposure level is estimated based

Table 5
Connectivity level ranking (CL1) (BV, 2018).

Connectivity Level	Description	Ranking (CL)
Level 1	Isolated system with no connectivity	1
Level 2	The system is connected to another system through secure (encrypted) communication and the communication is one-way from the considered system to another system.	2
Level 3	Applicable to a system with Connectivity Level 2, which employs wireless connection. The system is one-way interconnected to another system using unencrypted communication protocols. The communication is both ways between the systems using secure communication protocols.	3
Level 4	The system is connected to another system using distant link but using secure communication protocols and private network. The system is connected to another system using public network but employing protective device between the two systems.	4
Level 5	The system is exposed to public network e.g. external supplier can access the system network.	5

Table 6
Complexity level (CL2) ranking (BV, 2018).

Complexity Level	Definition	Ranking
Level 1	Systems with workstations and light servers; restoration of these systems is easily applied	1
Level 2	Systems with host authentication servers, database servers, supervision or programming workstations	2
Level 3	Unmanned systems, swarm connections, or systems dependent on high density of system exchange	3

on the system complexity and connectivity levels as illustrated in Tables 4–6. The attacker interest level is determined by adopting and enhancing the relevant ranking of MaCRA approach (Tam and Jones, 2019) as in Table 7. Each attacker technological level is provided in Table 1 by using BV guidelines (BV, 2018). The ease of exploitation is ranked according to Table 7. The ranking for the mitigation effectiveness or preventative barriers (it is alternatively referred as the vulnerability level) is implemented according to Table 7 based on our previous research work in (Bolbot et al., 2019a).

For estimating the vulnerability level ranking, the following barriers types are considered: (a) the presence of redundant components or communication lines implementing the same functionality with the one under attack; (b) the available safety or system reconfiguration functions; (c) the presence of humans operators constantly monitoring the system or potential rectification actions; (d) the presence of antivirus software on the considered components; (e) the presence of additional firewalls; (f) the incorporation of intrusion detection systems; (g) the use of enhanced security software architecture on the considered system components, and; (h) the level of access granted to the personnel to specific systems/functions. A detailed list of control barriers is provided in Table B.1.

The frequency and the severity of each attack scenario are ranked using the FSA ranking tables as proposed by (IMO, 2018), and presented in Tables 3 and 8. The severity ranking is implemented based on the consequences, where the most severe consequence among different types is selected for the risk estimation. The financial cost from the ship operation disruption is estimated based on the equivalence of a human life loss (Net cost of averting a fatality value from FSA), which is taken as $3m for 1998 according to (IMO, 2018) whilst considering the average inflation rate from 1998 to 2020 (2.29%). The consequences to the air pollution are derived according to the provided guidelines for cyber risk assessment by BV (2018). For harmonising the proposed methodology results with the pertinent IMO FSA guidelines, the attack risk is evaluated using the risk matrix presented in Table 9. In this risk matrix, higher severity but lower frequency accidents are given higher priority in comparison to lower severity but higher frequency accidents.

2.5. Phase D – System enhancement and requirements generation (Steps 8–10)

Based on the previous step results (Steps 1–7), it assessed whether the risk for each investigated scenario is within the acceptable region. For the investigated scenarios with not acceptable risk, the appropriate preventive and mitigating control barriers are identified and proposed in Step 8. The scenarios risk can be reduced by (ISO/IEC, 2016): (a) avoiding risk, e.g. changing the operational area; (b) removing the risk source, e.g. reducing the connectivity level; (c) influencing the likelihood, e.g. adding control barriers; (d) mitigating the consequences, e.g. enhancing the response and recovery after attack, and; (e) sharing risk through insurance.

Subsequently, the scenarios risk is reassessed considering the modified system architecture that includes the proposed control barriers. If the risk is acceptable, the process terminates. Otherwise, new barriers or architecture/functions are proposed. Based on this analysis results, it is reviewed whether different control barriers are repeated several times. Based on the frequency of appearance of different control barriers, the relevant safety recommendations at this ship design stage are derived.

3. Case study description

The proposed methodology was applied to estimate the cyber risk of a fully autonomous version of the Pallet Shuttle Barge (PSB) (Blue Lines Logistics, 2015) operating in inland waterways in the unmanned mode. This vessel is the one of the two use-cases of the AUTOSHIP project (AUTOSHIP, 2019). The main ship particulars are provided in Table 10. It must be noted that this study considers a theoretical use case of a fully autonomous PSB and not the actual demontrator of the AUTOSHIP project. Moreover, this study focuses on this vessel navigation and propulsion systems, as they are considered the most vulnerable to cyber-attacks (BIMCO, 2018b). The systems and equipment as well as their relevant interconnections and interactions, which are used for the vessel navigation and the propulsion in the autonomous mode, are provided in the schematic shown in Fig. 2. This schematic was developed based on the information reported in (Boyes and Isbell, 2017; Höyhtyä et al., 2017; Maritime affairs directorate of France, 2016; Schmidt et al., 2015; Stefani, 2013) and available drawings for similar ships. Further information is provided in Section 4.1.

4. Results and discussion

4.1. Phase A – Preparation for analysis (Steps 1–3)

The results of the developed methodology (Step 1) include the investigated autonomous ship systems control elements, their functionalities, their interactions with other control elements, the potential entry points for cyber-attacks and the relevant network zones identification. The derived results from Step 1 are presented in Fig. 3 and

Table 7
Attack group interest, Ease of exploitation, Vulnerability level ranking.

	Interest Level definition	Ease of Exploitation definition	Vulnerability level definition	Ranking IL/EE/VL
Level 1	Small to no value for the attack group/Small to no alignment with the attacker goal	Extraordinary resources are required to launch the attack/Very high attack cost	Extremely remote barriers unavailability/Five or more control barriers	1
Level 2	Small value to the attack group/Small alignment with the attacker goal	Significant resources are required to launch the attack/High attack cost	Remote barriers unavailability/Four control barriers	2
Level 3	Average value to the attack group/Moderate alignment with the attacker goal	Moderate resources are required to launch the attack/Mediocre attack cost	Rare barriers unavailability/Three control barriers	3
Level 4	Valuable to the attack group/High alignment with the attacker goal	Limited resources are required to launch the attack/Small attack cost	Adequate barriers availability/Two control barriers	4
Level 5	Extremely valuable/Very high to complete alignment with the attacker goal	Insignificant resources are required to launch the attack/Very small attack cost	Some barriers availability/One or no control barrier	5
Level 6	- (No ranking provided for this level)	- (No ranking provided for this level)	No barriers provided	6 (only for VL)

Table 8
Ranking for severity of consequences based (IMO, 2018).

		Safety	Environmental		Financial		
Ranking (SI)	Severity	Effects on human Safety	Oil spillage definition	Air pollution	Effects on ship	Effect from ship operation disruption/court costs/reputation loss/insurance costs/fines	S Equivalent fatalities
4	Catastrophic	Multiple fatalities	Oil spill size between < 100–1000 tonnes	Major air pollution with long-term environmental consequences	Total loss	50,000,000 $	10
3	Severe	Single fatality or multiple severe injuries	Oil spill size between < 10–100 tonnes	Air pollution resulting in air evacuation	Severe damage	5,000,000 $	10^{-0}
2	Significant	Multiple or sever injuries	Oil spill size between < 1–10 tonnes	Limited environmental impact due to air pollution involving reporting to authorities	Non-severe ship damage	500,000 $	10^{-1}
1	Minor	Single or minor injuries	Oil spill size < 1 tonne	Limited to no air pollution	Local equipment damage	50,000 $	10^{-2}

Table 9
The risk matrix (IMO, 2018).

Risk Index (RI)					
FI	Frequency	Severity (SI)			
		1 Minor	2 Significant	3 Severe	4 Catastrophic
7	Frequent	(H) 8	(H) 9	(H) 10	(H) 11
6		(M) 7	(H) 8	(H) 9	(H) 10
5	Reasonably probable	(M) 6	(M) 7	(H) 8	(H) 9
4		(M) 5	(M) 6	(M) 7	(H) 8
3	Remote	(L) 4	(M) 5	(M) 6	(M) 7
2		(L) 3	(L) 4	(M) 5	(M) 6
1	Extremely remote	(L) 2	(L) 3	(L) 4	(M) 5
High (H) = Intolerable Risk		Medium (M) = Tolerable Risk		Low (L) = Negligible Risk	

Table 10
Investigated ship particulars.

Length	50 m
Breadth	6.6 m
Maximum Draught	2.2 m
Air draught	5.6 m
Maximum cargo load	300 tonnes
Maximum speed	8.1 knots
Installed engines power	300 HP
Propulsion type	Diesel-mechanical with azimuth propulsion aft and bow thruster

Table 11. As it can be observed in Fig. 3, the investigated autonomous PSB has four major network zones. Zone 1 depicts the shore control centre, Zone 2 depicts the high level controllers, whereas Zone 3 and Zone 4 depict the engine automation and navigation systems.

Typically terrorist groups mainly target a ship accident occurrence (Tam and Jones, 2019). Thus, the focus of the present case study will shift towards identifying attacks and scenarios, which may be of interest by terrorists (Step 2).

The vulnerabilities list, potential entry points and attack types (step 3) have been provided in Appendix B.

4.2. Phase B & C – Identifying and ranking the attack scenarios (Steps 4–7)

In total 52 different attack scenarios were identified in Steps 4 and 5 by focusing on each system component. An example is provided in Table 11. The calculated risk index of these scenarios are shown in Fig. 4. The components functionality, potential vulnerabilities and goal of the attacker group were considered for determining the attack consequences. However, as mentioned in Section 2.2, the identified scenarios need to be updated based on the new identified vulnerabilities to remain up-to-date.

For the investigated vessel RI calculation the following assumptions were considered:

- The Activity Level (AL) of the terrorists was selected as reasonably probable (5). According to EBIOS (EBIOS, 2019), it could be ranked as low, however it is expected that the autonomous vessel will attract greater attention than the usual means of transport.
- The Technological Level (TL) was set to 4, following the guidelines provided in (BV, 2018).
- The interest level (IL) for scenarios with major safety consequences was set to 5, as terrorists are expected to cause as much damage in terms of human lives as possible. Less significant safety consequences correspond to lower IL values.
- For the Ease of Exploitation (EE) ranking, the systems with direct access to public network (Shore Control Centre, Connectivity Manager, Ship Control Station, VHF, AIS, GPS) were considered the easiest ones to be exploited. The systems in zones 2 and 4 were considered the more difficult systems to be attacked. The systems in zone 3 were considered the least accessible systems, as they hold a lower position in the control system architecture (Flaus, 2019).
- Since the ship systems are connected to the public network (4G and internet through shore control centre) (CL1 = 5) and it is a system with high complexity level (CL2 = 3), the components Exposure Level (EL) was set to 5.
- Initially, no protective measures were considered, therefore the Vulnerability Level (VL) was set to 5.

Out of the 52 identified scenarios, 4 were categorised as critical, 41 were found to be in a tolerable region and only 7 of them were initially characterised as of negligible importance. After the incorporation of the available and new safety/cyber security/security barriers, criticalscenarios were not found, 14 scenarios were considered as tolerable and the rest (38) scenarios were classified as negligible. The identified scenarios by the CYRA-MS with RI greater or equal with 8 are provided in Table 12. These scenarios are related to the access to the ship control station and the shore control station, as they may result in major consequences. Other top critical scenarios were related either to the GPS signal related attacks, as it is a scenario that can be easily exploited, or a malware installation on the collision avoidance system and the situation awareness system, as it is a scenario with potential major consequences.

4.3. Phase D – System enhancement and requirements generation (Steps 8–10)

The enhanced system logical structure is also presented in Fig. 3. For the system cyber risk reduction, it was considered that the vessel communication is implemented via a secure network with the shore control centre, whilst all the communications with the public network at the shore control centre and in other zones are cut, setting the EL to 4. In addition, it was considered that firewalls/redundant communication lines applying different technologies are installed between the different network zones. A safety system and intrusion detection systems monitoring for system safety and suspicious controllers behaviour in zone 2 are proposed as a means for the verification of the ship systems control actions. It is also proposed that these monitoring systems implement functions redundant to some of the functions of autonomous

Table 11
Investigated PSB selected components functionalities description.

Component	Functionalities	Data sent	Data received
Shore control centre	Monitoring of physical processes Navigation control Control over the ship in emergency/manoeuvring operating modes Implementation of software updates	Control information for navigation Selected route Ship operating mode Control status of equipment (on/off) New software	Equipment health status Equipment status (on/off, loads, position) Images from cameras Vessel position VHF data Traffic in the area Radar, ECDIS information

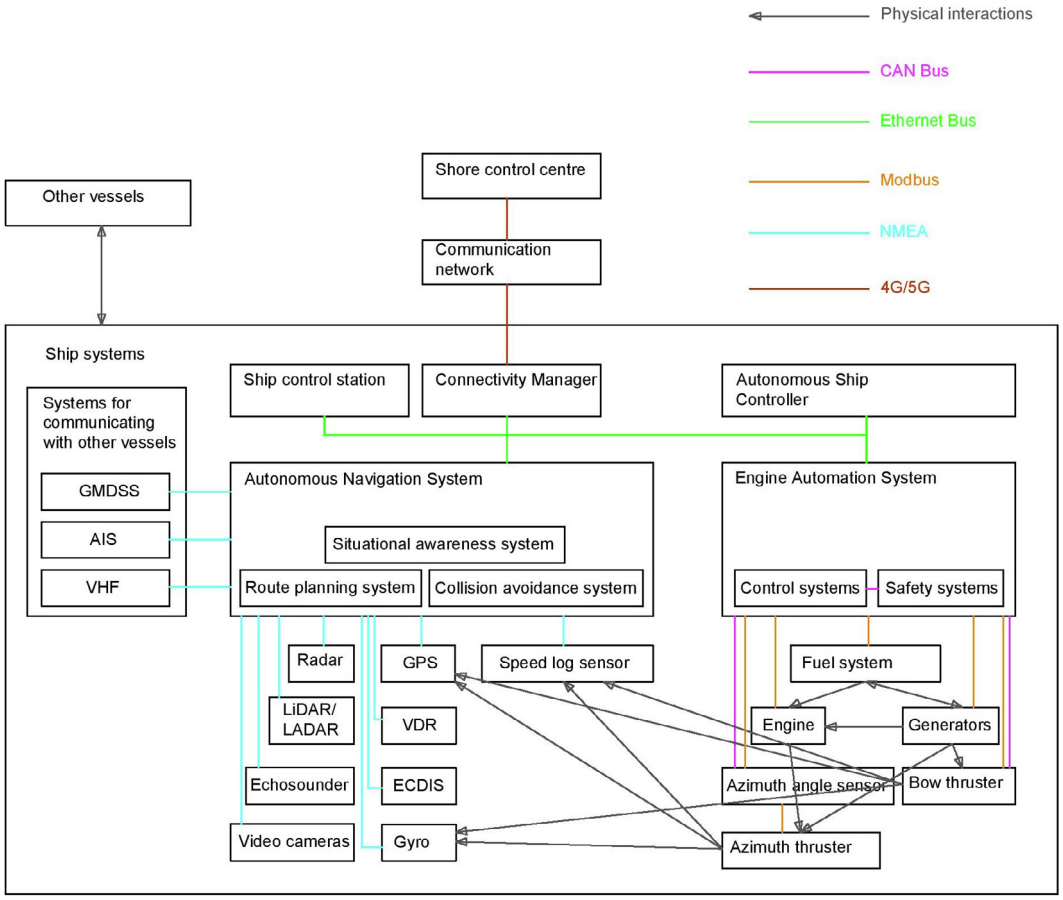

Fig. 2. Schematic diagram of the fully autonomous PSB systems and interactions.

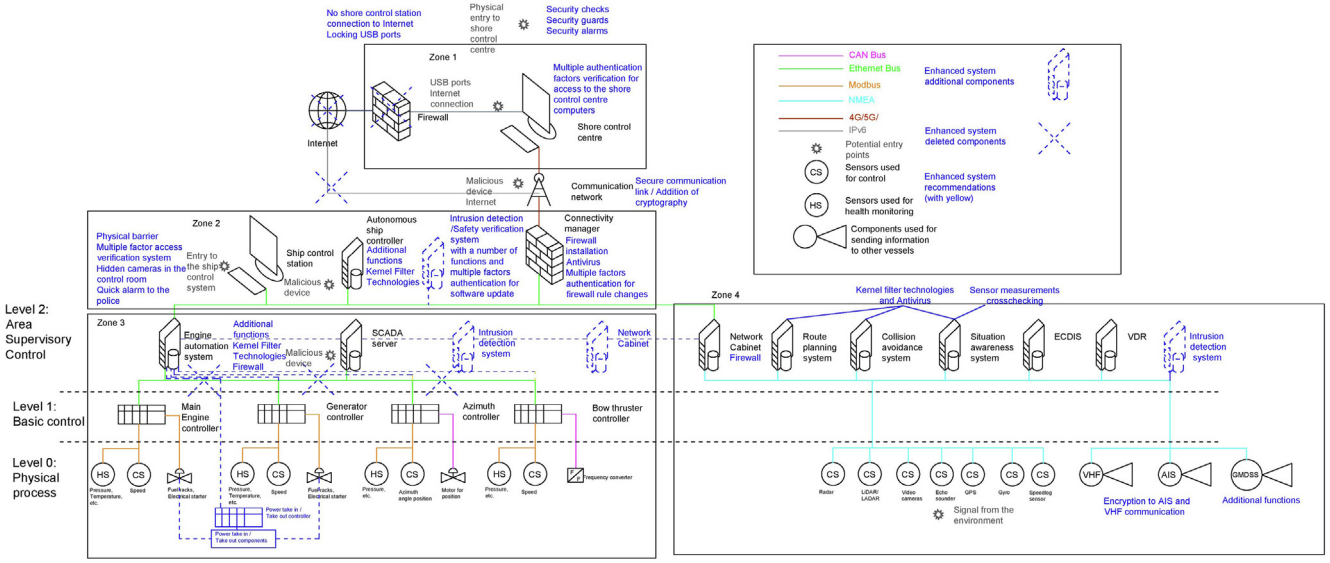

Fig. 3. Fully autonomous PSB systems logical modelling for baseline and enhanced system design.

ship controller, in case of a Denial of Service (DoS) attack. Sanity checks and filter application for the GPS signals measurements, as well as addition of anti-interference antennas are also proposed to be added in the investigated systems configuration to reduce the impact of the GPS signal loss. For some of the critical components (autonomous ship controller, intrusion detection system and navigation system), it is suggested that they operate in a kernel function, so that no software is installed without permission. It is also suggested that the situation awareness system carries out continuous sanity checks of the received measurements (speed, GPS, etc.). For the specific vessel, it is also suggested to install Power Take-In Power Take-Out technologies and interconnect them with the Diesel Generator sets, thus ensuring the propulsion power availability in case of failures in the Diesel Generator set or the ship main engine. Additional control measures are also indicated in Fig. 3.

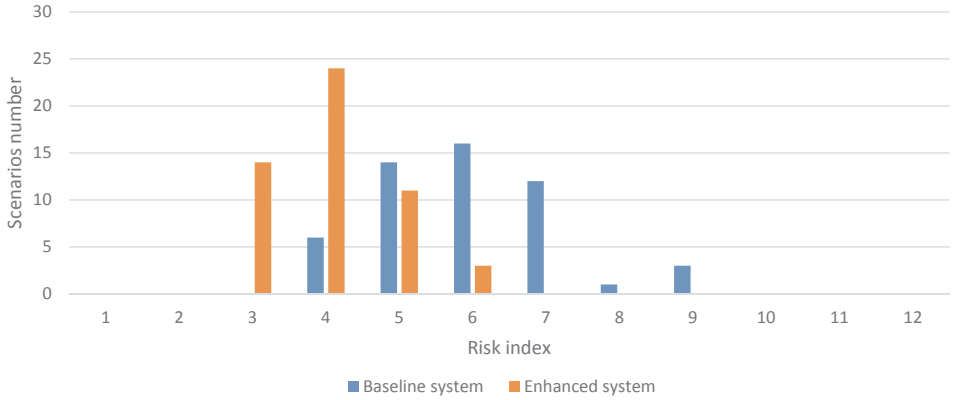

Fig. 4. Scenarios number vs risk index for baseline and enhanced system design.

4.4. Discussion on the proposed method and results

Based on the CYRA-MS application, it can be stated that the method allowed for the incorporation to the cyber risk analysis of different consequences types including safety, environmental and financial. Furthermore, the method included more potential attack scenarios than the STRIDE (Kavallieratos et al., 2019) or the MaCRA (Tam and Jones, 2019) methods. The method has been aligned with the FSA risk matrix facilitating the qualification of the new system and its approval by classification societies or derivation of prescriptive requirements for similar type of vessels at national level. As it has been also demonstrated in Section 4.3, the method supported the identification of various control measures enhancing the design. The provision of specific rules and guidelines for the scenarios identification and ranking is also expected to facilitate the cyber risk assessment process and improve its repeatability. This can be argued as the identification is implemented based on a formalised system representation and the ranking is implemented based on the available resources and guidelines bypassing the lack of relevant statistical data.

The method is a way to go forward with respect to ranking, when no or scarce statistical data is available. The method results could be validated when the relevant accident statistical data is available, but this data might take long to be accumulated. The method potentially could be enhanced by analysing the incidents data and estimating the leading/lagging safety and cybersecurity indicators, which could be another way to validate and update the method. Still, it is expected that the availability of accident data would constitute a better ground for making cyber risk assessments. Improvement of the obtained results fidelity can be achieved by the involvement of an experts' team. Continuous update of the list in Appendix B is also important for the method application and accuracy.

On the other hand, it could be argued that the identified scenarios ranking can be misleading as hackers may intentionally target at implementing the scenarios with low ranking. This would be feasible, provided that hackers have access to the relevant risk assessment data. For this reason, only the critical scenarios are provided herein. In addition, the scenarios ranking considers a number of parameters, primarily the interest level, which depict the scenarios that would be of interest for each attack group. Hence, scenarios with low ranking will hardly attract the attention of specific attack groups.

In addition, it could also be argued that the derived results are generic and applicable to all types of autonomous vessels. However, as Tam and Jones (2018) demonstrated, the results of risk assessment differentiate for different vessel types. An example scenario is obtaining physical access to the ship control centre. It is much easier to get physical access to an inland waterways vessel due to its operation in canals rather than to the short sea going or oceangoing vessels. Furthermore, the ranking differentiates based on the different control measures/barriers availability, connectivity levels and architecture, as well as system complexity. Different types of control measures/barriers can be implemented to the same vessel to ensure its safety. The implementation of risk assessment is also important for obtaining the approval from the classification societies.

One deficiency of the method is that it does not consider complex attacks on the protective measures. For instance, an first attack could compromise a protective measure, so that the primary attack (identified using CYRA-MS) follows. Yet, this scenario would require much more resources. However, these scenarios can be tackled by additional analysis employing much more detailed methods. Similarly, the proposed method considers simple safety scenarios. However, more complex safety scenarios potentially could be identified using other methods, after this analysis is implemented for the initially identified critical components. The use of the FSA matrix only provided a rough estimation of the risk metrics considering simpler scenarios. The potential consequences are not considered in great detail, which can also lead to wrong rankings. Finally, the drawback of the method is the independent consideration of the different attack groups. This practically means that additional system analysis is required for each attack group. Yet, grouping and facilitating the implementation of CYRA-MS method is a suggestion for future research.

5. Conclusions

This study aimed at developing a novel cyber risk assessment method for ship systems. The method is based on the identification of potential attack groups, the system components vulnerabilities, attack scenarios and ranking based on specific guidelines. The method was applied for identifying and ranking the cyber-attacks scenarios, which can be implemented by terrorists, in the case of the navigation and propulsion control systems of a fully autonomous inland ship.

The main findings of this study are the following:

- The proposed method allowed for estimating the risk metric for a number of attack scenarios for the investigated autonomous vessel by incorporating pertinent parameters and guided the safety enhancement of the investigated vessel system design.
- Attacks on the shore control centre and the ship control station, targeting at obtaining privileged access, have the highest potential safety implications and thus can be of high interest to terrorists for the specific vessel. Malware installation on the collision avoidance system and the situation awareness system have also significant safety implications as well.
- The investigated vessel system safety can be enhanced by adding firewalls on the conduits between the different control zones, increased redundancy in the communication between control zones as well as installing intrusion detection systems in different zones and eliminating internet communication links.

Table 12
Critical CYRA-MS scenarios with initial Risk Index (RI) greater or equal than 8.

a/a	System	Attack	Feared event	Likelihood Ranking							Consequences Ranking							RI	Safety/cybersecurity/ security barriers	New values				RI new
				TL	AL	IL	EE	EL	VL	FI	Safety (1)	Environment (2)	Financial (3)	1	2	3	SI			EL	VL	FI	SI	
1	Shore control centre	Combination of social engineering with malware installation	Access to shore control centre for performing other attacks	4	5	5	5	5	5	5	Ship control system modification leading to ship colliding with other vessels	Minor	Severe damage to ship due to accident	4	1	3	4	9	Isolation of shore control centre from the company business network/Closing USB ports/Advanced intrusion detection systems and Antivirus	4	3	2	4	6
2	Shore control centre	Getting access to the shore control centre	Taking remote control over ship	4	5	5	5	5	5	5	Remote control from ship leading to accident	Minor	Severe damage to ship due to accident	4	1	3	4	9	Security control at the shore control centre to the room/ Presence of guards/Use of complex authentication system to get into the ship control systems	4	3	2	4	6
10	Ship control station	Physical attack	Terrorist in ship control station	4	5	5	5	5	5	5	Terrorists gaining control over ship and attacking other ships	Minor	Damages to the navigation systems	4	1	2	4	9	Two or three factors authentication - Physical barrier to the control room (door, etc.) - Cameras for intrusion detection and alarm - Quick alarm to police	4	2	1	4	5
7	Connectivity manager	Malware installation	Modification of access and	4	5	5	3	5	5	4	Installation of malware on other	Minor		4	1	3	3	8	Firewall on the connectivity manager/Special	4	3	1	4	5

(*continued on next page*)

Table 12 (*continued*)

a/a	System	Attack	Feared event	Likelihood Ranking							Consequences Ranking							RI	Safety/cybersecurity/ security barriers	New values				RI new
				TL	AL	IL	EE	EL	VL	FI	Safety (1)	Environment (2)	Financial (3)	1	2	3	SI			EL	VL	FI	SI	
			communication settings								components with subsequent loss of control over ship and its systems		Severe disruption of operations						authentication requirements for firewall rules change/Advanced intrusion detection systems and Antivirus					

Table A.1
Abbreviation list.

AIS	Automatic Identification System
BV	Bureau Veritas
CISA	Cybersecurity and Infrastructure Security Agency
CPHA	Cyber Preliminary Hazard Analysis
CYRA-MS	CYber-Risk Assessment for Marine Systems
DoS	Denial of Service
ECDIS	Electronic Chart Display Information System
FSA	Formal Safety Assessment
GMDSS	Global Maritime Distress and Safety System
GPS	Global Positioning System
HazId	Hazard Identification
IMO	International Maritime Organisation
IT	Information Technologies
LADAR	Laser Detection And Ranging
LiDAR	Light Detection And Ranging
MaCRA	Maritime Cyber-Risk Assessment
OT	Operational Technologies
PHA	Preliminary Hazard Analysis
PLC	Programmable Logic Controller
PSB	Pallet Shuttle Barge
RADAR	RAdio Detection And Ranging
SCADA	System Control And Data Acquisition
STRIDE	Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service and Elevation of Privilege
VDR	Voyage Data Recorder
VHF	Very High Frequency

Table A.2
Nomenclature list.

AL	Activity level [attack per ship-year]
CL1	Connectivity level [-]
CL2	Connectivity level [-]
EE	Ease of exploitation [-]
EL	Exposure level [-]
F	Frequency [per ship-year]
FI	Frequency index [-]
H	High [-]
IL	Interest level [-]
L	Low [-]
M	Medium [-]
RI	Risk Index [-]
S	Severity [fatalities]
SI	Severity index [-]
TL	Technological level [-]
VL	Vulnerability level [-]

In conclusion, the proposed method can constitute a valuable tool for conducting risk assessments and the design enhancement of autonomous and smart vessels facilitating the approval of a new ship design. Future research initiatives could focus on further enhancement of the presented method, on enhancing the ranking accuracy, on aggregating the different risk scores for different attack groups, supporting the cost-benefit analysis and on a more detailed cyber-security analysis.

Acknowledgements

The study was carried out in the framework of the AUTOSHIP project (AUTOSHIP, 2019), which is funded by the European Union's Horizon 2020 research and innovation programme under agreement No 815012. The authors also greatly acknowledge the funding from DNV GL AS and RCCL for the MSRC establishment and operation. The opinions expressed herein are those of the authors and should not be construed to reflect the views of EU, DNV GL AS, RCCL or other involved partners in the AUTOSHIP project. The reviewers and participants of ISSAV 2019 conference are kindly acknowledged for their valuable comments to the conference paper presented at ISSAV 2019 conference.

Appendix A. Abbreviation and nomenclature list

See Tables A.1 and A.2.

Appendix B. Vulnerabilities, entry points and attack types on system components

A list of vulnerabilities, potential entry points and attack types for various ship components is provided in Table B.1.

Table B.1
List of vulnerabilities, potential entry points and attack types for various ship components.

	Attack vector		Attack types	Control barriers
Component	Entry point	Vulnerabilities		
Ship control centre/Ship operating company	Open USB ports (BIMCO, 2018a; Lund et al., 2018) Open communication bridges between smart devices and the shore control system (Oates et al., 2017) System connections to World Wide Web (BIMCO, 2018a) Company online services (BIMCO, 2018a)	Humans (Flaus, 2019) Poorly configured firewalls (Flaus, 2019)	Social engineering attack (Phishing, Spear phishing) (BIMCO, 2018a; Flaus, 2019) Malware installation (BIMCO, 2018a; Lund et al., 2018; Oates et al., 2017) Water holing, scanning (BIMCO, 2018a) Shoulder, Video-recording attack (Guerar et al., 2020)	Training (BIMCO, 2018a) Closing the USB ports (BIMCO, 2018a) Automatic scanning for devices connected to USB ports (BIMCO, 2018a) Communication links/segregation between the communication networks using firewalls (Chapple et al., 2018) Securing user profiles (BIMCO, 2018a) Advanced intrusion detection systems and antivirus (Bozdal et al., 2018; Kang et al., 2018) Intrusion prevention systems (BIMCO, 2018a)
Communication with ship	Malicious device Link on website	Communication protocol vulnerabilities, lack of encryption (DNV GL, 2016; Flaus, 2019)	DoS attack, man in the middle attack, access to system (Wingrove, 2020)	
Ship control network	Malicious device (Flaus, 2019; Rider, 2020) Communication links with internet (BIMCO, 2018a)	Some protocols are in the broadcast mode (information sent to all the nodes), no encryption available (Flaus, 2019)	DoS attack (Bozdal et al., 2018; Kang et al., 2018) Masquerade, eavesdropping, injection and replay attacks (El-Rewini et al., 2019) Network access attack, traffic confidentiality attack, traffic integrity attack, side channel attack (Flaus, 2019) Fuzzy attack (Tariq et al., 2020)	Intrusion detection system (Bozdal et al., 2018; Kang et al., 2018) IT and OT segregation from ship networks used for entertainment (BIMCO, 2018a)
Connectivity manager/ Firewalls	Constitutes access point due to connection to satellites	Errors in communication, firewall configurations (CISA, 2019b; DNV GL, 2016; Flaus, 2019; IEC, 2011b; Oates et al., 2017) Default passwords in use (Doyle, 2017; Munro, 2017; Oates et al., 2017) Inappropriate share of passwords (Chapple et al., 2018; Svilicic et al., 2019a) Lack of authentication procedures (Svilicic et al., 2019b) Missing protection on communication ports (Ilascu, 2019)	Malware installation/gaining access to the rest of the system components	Vulnerability scanner running (Oates et al., 2017) Two or three factors authentication requirements for the system access (Chapple et al., 2018) Audit log activities Use of strong passwords (BIMCO, 2018a)
Ship controllers	Ship connection with the shore Communication links with internet (BIMCO, 2018a)	Exposure to patching, vulnerabilities of operating system, long system operating time (Oates et al., 2017), buffer overflow and command injection vulnerabilities (Santamarta, 2015) Outdated software, ECDIS is frequently updated (Wingrove, 2018)	DoS, malware installation, logic bombs, backdoors (Oates et al., 2017), SQL injections (DNV GL, 2016; Flaus, 2019), data tampering (Santamarta, 2015), sensor freezing (Shinohara and Namerikawa, 2017), subverting the supply chain (BIMCO, 2018a), obtaining control (Munro, 2017), erasing information (Santamarta, 2015)	Training (BIMCO, 2018a) Closing the USB ports (BIMCO, 2018a) Automatic scanning for devices connected to USB ports (BIMCO, 2018a) Intrusion detection system application, use of kernel technologies, antivirus (Wingrove, 2018), two or three factors authentication requirements for software update System backup (BIMCO, 2018a)
Ship control station	Constitutes an entry point	Close proximity to shore/No crew or incapable crew in the ship control station	Physical attack with subsequent cyber attack, Shoulder, video-recording attack (Guerar et al., 2020)	Two or three factors authentication for getting access to the system, strong physical barrier to the control room, cameras for intruders detection
VHF, AIS, GMDSS	Used for sending/receiving information – constitute entry points	No encryption available	Eavesdropping, jamming (Balduzzi et al., 2014) Illusion, bogus information, Sybil, impersonation, alteration/replay, masquerade, collusion, delay, timing attack (El-Rewini et al., 2019; Wang et al., 2020)	Sanity checks for sensors measurements
LiDAR/LADAR sensor/ RADAR	Interface between the environment and the controller	Dependability on the surface reflectiveness	Dazzling, spoofing (Brooks, 2016) (Wingrove, 2018), Adversarial attacks (Boloor et al., 2020; Tu et al., 2020)	Redundancy in sensors/systems used for situational awareness Cross check with other sensors measurements
Video cameras	Interface between the environment and the controller	Dependability on input image	Dazzling, spoofing (Alguliyev et al., 2018; Brooks, 2016) Adversarial attacks (Boloor et al., 2020)	Redundancy in sensors/systems used for situational awareness Cross check with other sensors measurements
GPS	Interface between the environment and the controller	Weak signal	Jamming (Borio et al., 2012; Boyes and Isbell, 2017; Farid et al., 2018), spoofing (Goward, 2017; Newman, 2019), delay (Omitola et al., 2018)	Sanity checks, signal filtering (Borio et al., 2012; Boyes and Isbell, 2017; Farid et al., 2018), blocking antennas, setting antennas at different locations, using high-elevation satellites, detection sensors for interference, jamming and spoofing signals, back up sensors (US department of Homeland Security, 2017)

References

AAWA, 2016. AAWA project introduces the project's first commercial ship operators.
ABS, 2018. Cybersecurity implementation for the marine and offshore industries, In: ABS (Ed.), ABS CyberSafetyTM VOLUME 2.
Alguliyev, R., Imamverdiyev, Y., Sukhostat, L., 2018. Cyber-physical systems and their security issues. Comput. Industry 100, 212–223.
AUTOSHIP, 2019. Autonomous Shipping Initiative for European Waters.
Balduzzi, M., Pasta, A., Wilhoit, K., 2014. A security evaluation of AIS automated identification system. In: ACMpp. 436–445.
BIMCO, 2018a. The Guidelines on Cyber Security Onboard Ships Version 3.0.
BIMCO, 2018b. Maritime Cyber Survey 2018 - the results.
Blue Lines Logistics, 2015. Blue Lines Logistics News.
Bolbot, V., Puisa, R., Theotokatos, G., Boulougouris, E., Vassalos, D., 2019a. A comparative safety assessment for DC and DC with hybrid power systems in a windfarm SOV using STPA, In: Banda, O. (Ed.), European STAMP Workshop & Conference, Helsinki, Finland.
Bolbot, V., Theotokatos, G., Boulougouris, E., Psarros, G., Hamann, R., 2020. A novel method for safety analysis of Cyber-Physical Systems - Application to a ship exhaust gas scrubber system. Safety.
Bolbot, V., Theotokatos, G., Boulougouris, E., Vassalos, D., 2019b. Comparison of diesel-electric with hybrid-electric propulsion system safety using System-Theoretic Process Analysis, Propulsion and Power Alternatives. Royal Institute of Naval Architects, London, United Kingdom, pp. 55–61.
Bolbot, V., Theotokatos, G., Bujorianu, L.M., Boulougouris, E., Vassalos, D., 2019c. Vulnerabilities and safety assurance methods in Cyber-Physical Systems: a comprehensive review. Reliab. Eng. Syst. Safety 182, 179–193.
Bolbot, V., Theotokatos, G., Vassalos, D., 2018. Using system-theoretic process analysis and event tree analysis for creation of a fault tree of blackout in the Diesel-Electric Propulsion system of a cruise ship. In: International Marine Design Conference XIII. CRC Press, Helsinki, Finland, pp. 691–699.
Boloor, A., Garimella, K., He, X., Gill, C., Vorobeychik, Y., Zhang, X., 2020. Attacking vision-based perception in end-to-end autonomous driving models. J. Syst. Arch., 101766.
Borio, D., Driscoll, C.O., Fortuny, J., 2012. GNSS Jammers: Effects and countermeasures. In: 2012 6th ESA Workshop on Satellite Navigation Technologies (Navitec 2012) & European Workshop on GNSS Signals and Signal Processing, pp. 1–7.
Boyes, H., Isbell, R., 2017. Code of practice - cyber security for ships, In: Technology, T.I. o.E.a. (Ed.), London, United.
Bozdal, M., Samie, M., Jennions, I., 2018. A survey on CAN bus protocol: attacks, challenges, and potential solutions. In: 2018 International Conference on Computing, Electronics & Communications Engineering (iCCECE). IEEE, pp. 201–205.
Bradbury, D., 2019. Cyberattack Lands Ship in Hot Water. NakedSecurity.
British Standards Institution (BSI), 2004. Functional safety - Safety instrumented systems for the process industry sector -IEC-61511, Part 3: Guidance for determination of the required safety integrity levels. British Standards Instituition, London, United Kingdom.
Brooks, Z., 2016. Hacking driverless vehicles.
BV, 2018. Rules on Cyber Security for the Classification of Marine Units, In: BV (Ed.), NR 659 DT R00, Paris, France.
Chapple, M., Stewart, J.M., Gibson, D., 2018. (ISC) 2 CISSP Certified Information Systems Security Professional Official Study Guide. John Wiley & Sons.
CISA, 2019a. CISA - Industrial Control Systems.
CISA, 2019b. ICS Alert (ICS-ALERT-19-225-01) - Mitsubishi Electric smartRTU and INEA ME-RTU.
ClassNK, 2019. Cyber security management system for ships.
Cormier, A., Ng, C., 2020. Integrating cybersecurity in hazard and risk analyses. J. Loss Prevent. Process Indust. 64, 104044.
Daffey, K., 2018. Technology Progression of Maritime Autonomous Surface Ships.
DNV GL, 2015. Technology outlook 2025. DNV GL, Hovik, Norway.
DNV GL, 2016. DNVGL-RP-0496 - Cyber security resilience management.
DNV GL, 2019. Part 6 Additional class notations Chapter 5 Equipment and design features Section 21 Cyber security. In: GL, D. (Ed.), Part 6 Chapter 5 Section 21.
Doyle, W., 2017. Cyber threat the maritime industry must redouble its efforts to secure IT systems and data. Maritime reporter and Engineering News.
EBIOS, 2019. EBIOS Risk Manager. In: d'information, A.n.d.l.s.d.s. (Ed.), Paris, France.
El-Rewini, Z., Sadatsharan, K., Selvaraj, D.F., Plathottam, S.J., Ranganathan, P., 2019. Cybersecurity challenges in vehicular communications. Vehicular Commun., 100214.
Eloranta, S., Whitehead, A., 2016. Safety aspects of autonomous ships. In: Gl, D.N.V. (Ed.), 6th International Maritime Conference, Germany, Hamburg, pp. 168–175.
Farid, M.A., Ahmad, M., Ahmed, S., Rahim, S.S., 2018. Impact and detection of GPS jammers and countermeasures against jamming. Int. J. Scientific Eng. Res. 9, 47–54.
Flaus, J.-M., 2019. Cybersecurity of Industrial Systems. ISTE Ltd, London, United Kingdom.
Glomsrud, J.A., Xie, J., 2019. A structured STPA safety and security co-analysis framework for autonomous ships. In: Beer, M., Zio, E. (Eds.), European Safety and Reliability conference, Germany, Hannover.
Goward, A., 2017. Mass GPS Spoofing Attack in Black Sea? The Marine executive.
Guerar, M., Verderame, L., Merlo, A., Palmieri, F., Migliardi, M., Vallerini, L., 2020. CirclePIN: A novel authentication mechanism for smartwatches to prevent unauthorized access to IoT devices. ACM Trans. Cyber-Phys. Syst. 4, 1–19.
Gunes, V., Peter, S., Givargis, T., Vahid, F., 2014. A survey on concepts, applications, and challenges in cyber-physical systems. KSII Trans. Internet Inform. Syst. 8, 4242–4268.
Guzman, N.H.C., Kufoalor, D.K.M., Kozin, I., Lundteigen, M.A., 2019. Combined safety and security risk analysis using the UFoI-E method: A case study of an autonomous surface vessel. In: 29th European Safety and Reliability Conference, pp. 4099–4106.
Höyhtyä, M., Huusko, J., Kiviranta, M., Solberg, K., Rokka, J., 2017. Connectivity for autonomous ships: Architecture, use cases, and research challenges. In: 2017 International Conference on Information and Communication Technology Convergence (ICTC). IEEE, pp. 345–350.
IEC, 2011a. IEC 27005 - Information technology - security techniques - Information security risk management.
IEC, 2011b. Information technology — Security techniques — Information security risk management - ISO 27005. International Standard organisation, Switzerland.
IEC, 2018. Security for industrial automation and control systems - IEC 62443.
Ilascu, I., 2019. Most Cyber Attacks Focus on Just Three TCP Ports.
IMO, 2008. MSC-MEPC.3/Circ.3 Casualty-Related Matters* Reports On Marine Casualties And Incidents.
IMO, 2016a. Interim guidelines on maritime cyber risk management, MSC.1-CIRC.1526, p. 6.
IMO, 2016b. International Convention for the Prevention of Pollution from Ships (MARPOL).
IMO, 2017. Measures to enhance maritime security MSC-FAL.1/Circ.3, In: committee, M. s. (Ed.).
IMO, 2018. Revised guidelines for formal safety assessment (FSA) for use in the IMO rule-making process, London, p. 71.
ISO/IEC, 2016. Information technology — Security techniques — Information security management systems (ISO/IEC 27000). British Standard Institution.
Jones, K.D., Tam, K., Papadaki, M., 2016. Threats and impacts in maritime cyber security.
Kang, T.U., Song, H.M., Jeong, S., Kim, H.K., 2018. Automated reverse engineering and attack for CAN using OBD-II. In: 2018 IEEE 88th Vehicular Technology Conference (VTC-Fall). IEEE, pp. 1–7.
Kavallieratos, G., Katsikas, S., Gkioulos, V., 2019. Cyber-Attacks Against the Autonomous Ship. In: Katsikas, S.K., Cuppens, F., Cuppens, N., Lambrinoudakis, C., Antón, A., Gritzalis, S., Mylopoulos, J., Kalloniatis, C. (Eds.), Computer Security. Springer International Publishing, Cham, pp. 20–36.
Kavallieratos, G., Katsikas, S., Gkioulos, V., 2020. SafeSec Tropos: Joint security and safety requirements elicitation. Comput. Stand. Interfaces 70, 103429.
Kriaa, S., Pietre-Cambacedes, L., Bouissou, M., Halgand, Y., 2015. A survey of approaches combining safety and security for industrial control systems. Reliab. Eng. Syst. Safety 139, 156–178.
LR, 2019. Procedures for the assessment of cyber security for ships and ships systems.
Lund, M.S., Hareide, O.S., Jøsok, Ø., 2018. An attack on an integrated navigation system.
Marine Electronics and Communications, 2017. Ships are riddled with malware, Marine Electronics and Communications.
Maritime affairs directorate of France, 2016. Cyber security Assessment and protection of ships, In: Ministry of environment, e.a.t.s.o.F. (Ed.).
MUNIN, 2016. Maritime Unmanned Navigation through Intelligence in Networks.
Munro, K., 2017. OSINT from ship satcoms.
Newman, N., 2019. Cyber pirates terrorising the high seas. Engineering and Technology.
NIST, 2019. Computer security resource center.
Oates, R., Roberts, J., Twomey, B., 2017. Chains, Links and Lifetime: Robust Security for Autonomous Maritime Systems. Marine Electrical and Control Systems Safety, Glasgow, United Kingdom, pp. 46–53.
Omitola, T., Downes, J., Wills, G., Zwolinski, M., Butler, M., 2018. Securing navigation of unmanned maritime systems.
Rider, D., 2020. Maritime meets cyber security, The Maritime Executive.
Santamarta, R., 2015. Maritime Security: Hacking into a Voyage Data Recorder (VDR).
Schmidt, M., Fentzahn, E., Atlason, G.F., Rødseth, H., 2015. D8.7: Final report: Autonomous engine room.
Shang, W., Gong, T., Chen, C., Hou, J., Zeng, P., 2019. Information security risk assessment method for ship control system based on fuzzy sets and attack trees. Security Communic. Networks 2019, 11.
Shinohara, T., Namerikawa, T., 2017. On the vulnerabilities due to manipulative zero-stealthy attacks in cyber-physical systems. SICE J. Control, Measur., Syst. Integr. 10, 563–570.
Stefani, A., 2013. An introduction to ship automation and control systems. Institute of Marine Engineering, Science & Technology, United Kingdom, London.
Svilicic, B., Kamahara, J., Celic, J., Bolmsten, J., 2019a. Assessing ship cyber risks: a framework and case study of ECDIS security. WMU J. Maritime Affairs 18, 509–520.
Svilicic, B., Rudan, I., Frančić, V., Mohović, D., 2019b. Towards a cyber secure shipboard radar. J. Navigation 1–12.
Tam, K., Jones, K., 2018. Cyber-risk assessment for autonomous ships. In: 2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security). IEEE, pp. 1–8.
Tam, K., Jones, K., 2019. MaCRA: a model-based framework for maritime cyber-risk assessment. WMU J. Maritime Affairs 18, 129–163.
Tariq, S., Lee, S., Kim, H.K., Woo, S.S., 2020. CAN-ADF: The Controller Area Network Attack Detection Framework. Computers & Security, 101857.
Tu, J., Ren, M., Manivasagam, S., Liang, M., Yang, B., Du, R., Cheng, F., Urtasun, R., 2020. Physically Realizable Adversarial Examples for LiDAR Object Detection. arXiv preprint arXiv:2004.00543.
U.S. Coast Guard, 2019. Cyber adversaries targeting commercial vessels.
United States Coast Guard, 2015. Cyber strategy, Washington D.C.
US department of Homeland Security, 2017. Improving the Operation and Development of Global Positioning System (GPS) Equipment Used by Critical Infrastructure.
Wang, P., Wu, X., He, X., 2020. Modeling and analyzing cyberattack effects on connected automated vehicular platoons. Transp. Res. Part C: Emerg. Technol. 115, 102625.
Wingrove, M., 2017. Shipborne systems most vulnerable to cyber-attack, Marine electronics & communications. Riviera Maritime Media Ltd, United Kingdom, Enfield, p. 27.
Wingrove, M., 2018. 'Impregnable' radar breached in simulated cyber attack.
Wingrove, M., 2020. Secure VSAT to prevent cyber attacks.
Yara, 2018. Yara Birkeland press kit.