Cyber-attacks against the autonomous ship

Georgios Kavallieratos[1], Sokratis Katsikas[1,2], and Vasileios Gkioulos[1]

[1] Norwegian University of Science and Technology, Department of Information Security and Communications Technology, Gjøvik, Norway
(georgios.kavallieratos, sokratis.katsikas, vasileios.gkioulos)@ntnu.no,
sokratis.katsikas@ouc.ac.cy

[2] Open University of Cyprus, School of Pure and Applied Sciences, Latsia, Nicosia, Cyprus

Abstract. Autonomous ships transferring valuable cargoes and humans in a more efficient and cost effective manner will soon be state of the art technology. Yet, their ICT system architecture and operations have not been defined in full detail. Moreover, multiple cyber security issues remain open and should be addressed. No study to date has analyzed fully the architecture of the autonomous ship, even less so have potential cyber threats and cyber attacks been identified. In this paper we identify and categorize systems that make up an autonomous ship, we propose a generic system architecture, and we analyze the cyber security of the ship by leveraging the STRIDE threat modeling methodology to identify potential cyber attacks, and to analyze the accordant risk. The results will support ship designers and industry towards improving the autonomous ship system architecture and making ship operations more secure.

Keywords: Autonomous ship · Cyber-Security · Cyber-physical systems · Risk analysis · STRIDE · Threats.

1 Introduction

Information and Communications Technology (ICT) adoption rates on board ships are increasing at an impressive rate over the past few years. Examples of current ship-based cyber systems include:

- navigation, positioning and identification systems;
- communications systems, including voice and data communications;
- integrated bridge systems;
- control systems for electro-mechanical systems on board.

Today's leading manufacturers and ship operators innovate using the latest ICT systems, going beyond traditional engineering to create ships with enhanced monitoring, communication and connection capabilities; such ships are collectively referred to as "Cyber-Enabled Ships (C-ES)". These include ships that can be controlled by remote onshore services, anytime and anywhere [1], and fully autonomous ships. Companies such as Rolls-Royce have already designed crew-less ships which can be controlled from a distance and will be able to sail by the end of 2020 and to travel open seas by 2035 [2]. Most of the cyber systems found on board ships today, and those that will be found in the remotely operated or fully autonomous ships of the future are cyber-physical systems, in which the physical process is controlled by computer-based systems. The interconnections of these systems have not been fully analyzed yet.

The adoption of ICT in any industry has always been accompanied with an enlargement and diversification of the cyber risks that the industry is facing, with existing risks being increased and new risks being introduced. This is mainly due to the fact that whereas traditional operations were designed with no need for cyber security in mind, modern ICT-enabled operations are allowed to be accessed and controlled through the industry's enterprise information system, through interfaces that are rarely adequately secure. As the enterprise system is more often than not connected to the Internet, the end result is that cybersecurity-unaware systems are made potentially accessible to outsiders. Therefore, it is not surprising that almost all known attacks against industrial control systems have been launched by first compromising the enterprise system and subsequently using it as a stepping stone to attack the control system. The shipping industry and the cyber-enabled ship in particular is no exception. As C-ESs become increasingly integrated across freight and passenger transport networks, their security by design becomes an imperative requirement. The EU Directive on the security of network and information systems includes such systems among the most critical societal infrastructures that already rely heavily on digital services, while disruption of their operations can lead to financial and environmental damage, or even endanger human safety.

In this paper we first identify cyber systems that are found on board ships and we define the system architecture of the C-ES. We then use Microsoft's STRIDE methodology [3] to study attacks against such systems. In the sequel, we define specific criteria for the impact and likelihood levels and we determine the risk level that these attacks pose, by leveraging the risk matrix. The contribution of this paper is twofold:

- An ICT system architecture of the C-ES has been defined;
- Attacks against the C-ES have been identified and the accordant risk has been analyzed.

The remainder of this article is structured as follows: Section 2 reviews related work. Section 3 presents the proposed C-ES ICT architecture. In section 4 we briefly discuss STRIDE, and the reasons that led us to use it, as well as the results of its application to the C-ES. Finally, section 6 summarizes our conclusions and proposes directions for future work.

2 Related work

Most of the previous work on autonomous ships is focused on the systems and communication architecture as part of the work within the EU MUNIN project

[4]. Namely, the Information and Communications Technology (ICT) architecture of unmanned merchant ships is provided by Rødseth *et al.* in [5], and the communication architecture is illustrated by Rødseth *et al.* in [6]. Further, the MUNIN project deliverables analyze the architectures and the operations of the bridge [7], the Shore Control Center [8] and engine rooms [9]. Also, Ø.J. Rødseth in [10] describes a risk assessment method which is safety-oriented and does not examine cyber-security threats and vulnerabilities. Significant work in the field of autonomous vessels has also been done in the AAWA project [2], including the identification of the need for cyber security, and the highlighting of general safety and security issues which have been posed by Jalonen *et al.* in [2].

Nevertheless, the security of the autonomous ship has been examined and analyzed only scarcely. Specifically, Lloyds in [1] commented on the cyber-security of the cyber-enabled ship, but only as a consideration. Also, Tam *et al.* in [11] proposed a method to assess the cyber-risk of C-ES, but the analysis was done for three specific models of ships without extending to all systems and sub-systems, while the potential attacks were only examined from the attacker's perspective. In [12] a generic system architecture is discussed by Katsikas as well as threats, vulnerabilities and risks against this generic architecture. Yet, the system architecture and its components have not been specified. No previous work has proposed a detailed system architecture or has implemented a holistic threat analysis to identify potential attacks that may occur in the systems of such a ship by leveraging specific vulnerabilities.

The methodology to be used is important for the identification of all the attacks, threats and vulnerabilities of a system. Many threat analysis methodologies have been proposed in the literature [13], [14]. Among the most prominent ones, Attack Trees requires understanding each subsystem separately and provides an overview about the attack surface, without taking under consideration essential data for the threat scenario. Chun Yu Cheung in [15] concludes that in the Attack Trees the initial attacker's goal must be known, and the method places emphasis in the sophistication of the attack. The Threat Modeling framework based on Attack Path analysis (T-MAP) is another method, which considers the severity weights that derive from attack paths. According to [13], this method works with Commercial Off the Shelf (COTS) systems, hence its is inappropriate for the C-ES case. Risk Reduction Overview (RRO) is a method which depends on the initial risk of the target system [16]. This requires knowing potential vulnerabilities as early as the design phase, which limits its applicability to the C-ES case, whose components' design is not available in sufficient detail. The Petri net methodology is a quite complex one, while the Attack Library method, is based on the attacker's perspective [17]. In contrast, methods with defender perspective examine the targeted systems thoroughly and their scope is to defend them.

Shafiq Hussain *et al.* in [13] compare different threat modeling methodologies and conclude that most of academia and industry use the STRIDE methodology or its variants. Another comparative analysis of threat models has been carried out in [14]; the authors concluded that the STRIDE method and its variants extract the most rigorous results in contrast with the other six methodologies and frameworks that were considered. It is important to note that most of the threat methodologies require the analysis of the target architecture to be available in full detail; this makes them inappropriate for the C-ES, as such details have not yet become available, and they would be expected to depend on specific implementations. Based on the above findings, STRIDE was selected as the most appropriate method to use to analyze threats against the C-ES. More detail on STRIDE is provided in section 4.1.

3 The ICT architecture of the cyber-enabled ship

For the definition of the architecture we follow a tree-based structure which consists of the systems and sub-systems of the C-ES according to MUNIN deliverables and the BIMCO report "The Guidelines of Cyber Security Onboard Ships" [18].

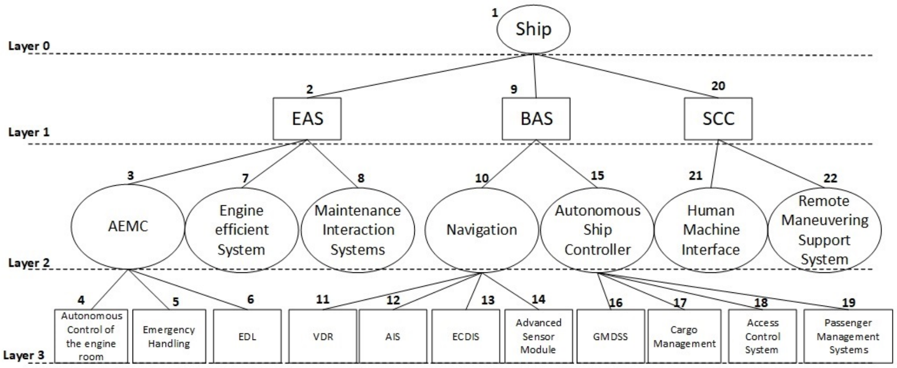


Fig. 1: Systems architecture

Figure 1 presents the schematic of the proposed architecture, structured in three layers. The top layer is the C-ES, while layer one comprises the Engine Automation Systems (EAS), the Bridge Automation Systems (BAS) and the systems in the Shore Control Center (SCC). Layer two comprises the sub-systems of EAS (the Autonomous Engine Monitoring and Control systems-AEMC, the Engine Efficiency System, and the Maintenance Interaction System); the sub-systems of BAS (the Navigation systems, and the Autonomous Ship Controller system-ASC); the sub-systems of SCC (the Remote Maneuvering Support System, and the Human Machine Interface-HMI). The third layer comprises the sub-systems of AEMC (the Engine Data Logger-EDL, the Autonomous Control of the Engine Room, and the system for handling emergency situations); the sub-systems of Navigational systems (the VDR, the automatic identification system-AIS, the Electronic Chart Display and Information System-ECDIS, the GPS and the Advanced Sensor Module); and the systems of the Autonomous Ship Controller (the Global Maritime Distress and Safety System-GMDSS, the cargo management systems, the access control systems, and the passenger systems-PSMS). These are discussed in some more detail in the sequel.

1. **Engine Automation Systems - EAS:** Described in full detailed by Schmidt *et al.* in [9], it includes all the systems which are responsible for the generation and management of the ship's power and propulsion systems.
    1.1. **Autonomous Engine Monitoring and Control-AEMC:** Is connected directly with the mechanical parts of the ship.
        1.1.1. **Autonomous Control of the Engine Room:** Is responsible for the correct operation of the engines. It is interconnected with the propulsion system, power generation system, fuel system, rudder systems and evaporation system.
        1.1.2. **Emergency Handling-EmH:** Implements the appropriate countermeasures to avoid potential damage in the infrastructure, and includes the alarm systems.
        1.1.3. **Engine Data Logger-EDL:** Is responsible for recording all the information about the ship's engine operation.
    1.2. **Engine Efficiency System-EES:** Monitors the appropriate ship's operation, consisting of preventive tools for maintenance.
    1.3. **Maintenance Interaction System-MIS:** Provides technical, managerial and administrative maintenance in the engine room.
2. **Bridge Automation System-BAS:** Is fully analyzed in [7] by Burmeister *et al.* and consists of all the sub-systems which exist in a ship's bridge, with the most crucial one being the navigational and the management systems.
    2.1. **Navigation System:** Gives the appropriate directions to the ship for reaching its destination. The NAS interacts directly with many systems.
        2.1.1. **Voyage Data Recorder-VDR:** Gathers and stores all the information about the ship's condition, its position, its movements, and recordings from engine and radio systems. More detail on its operations cabn be found in [19].
        2.1.2. **Automatic identification system-AIS:** Provides information which, together with other systems, helps authorities and other ships to monitor sea traffic, thereby ensuring the ship's safety.
        2.1.3. **Electronic Chart Display and Information System-ECDIS:** Transmits useful information and contributes to improving the ship's security and safety [20]. It is mandatory for all vessels.
        2.1.4. **Advanced Sensor Systems-ASS:** Produces reliable information about the ship's positioning.
    2.2. **Autonomous Ship Controller:** Is responsible for the data assessment, derived from the sensors and the SCC. It constitutes an additional control for the autonomous systems. A description of the system can be found in [21]
        2.2.1. **Global Maritime Distress and Safety System-GMDSS:** Is a set of security procedures, equipment, and communication protocols. Its operation is fully described in [19] and in [20].

2.2.2. **Cargo Management / Cargo Control Room-CCR:** Is responsible for the efficient cargo control and management. BIMCO *et al.* in [18] and Rolls-Royce in [2] describe this system.

2.2.3. **Access Control system:** Is responsible for the ship's access control, either physically or remotely [18].

2.2.4. **Passenger service system:** Serves the ship's customers/passengers, with the goal of implementing efficient identity management and access control in the infrastructure [18].

3. **Shore Control Center-SCC:** Is a subsystem that controls and navigates one or more ships from the shore, proposed by MUNIN [8].

3.1. **Human Machine Interface-HMI:** Through this system humans can operate the C-ES under various conditions [8, 2].

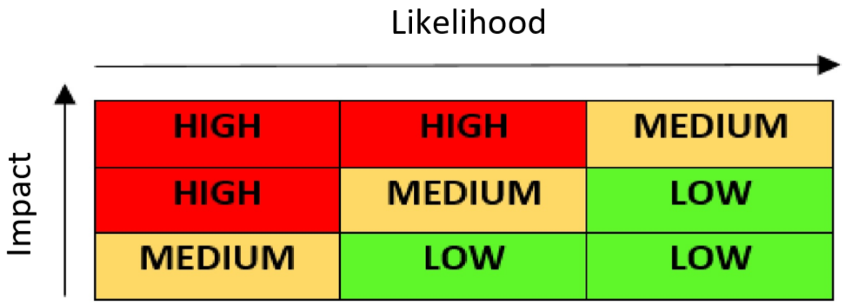
3.2. **Remote Maneuvering Support System-RMSS:** Is an information system which allows the execution of secure autonomous procedures under the control of the SCC [8].

4 Identifying and analyzing attacks against the Cyber-Enabled Ship

4.1 Methodology

STRIDE stands for Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service and Elevation of Privilege. The method was developed by Loren Kohnfelder and Praerit Garg in 1999. The STRIDE threats are described by Adam Shostack in [22]. Namely, Spoofing is the capability of the adversary to pretend someone or something else. Tampering is the alteration or disruption of a disk, network or memory of the system. Further, Repudiation is a threat which refers to someone's allegation that didn't do something which influences the system's operation or were not responsible for the results which derived from his actions. Information disclosure is another threat which reveals confidential information to the people who not suppose to see it. The next STRIDE threat is Denial of Service which violates the availability of the system and its task is to absorb all the possible resources which system needs to operate correctly. The last STRIDE threat is the Elevation of Privilege and according to this an adversary could execute unauthorized actions. STRIDE attempts to discover potential threats and vulnerabilities as early as the design phase and analyzes each threat by answering questions according to specific security properties. STRIDE collects and combines the results of active and passive threats.

It is important to note that we implemented STRIDE in the proposed, tree-structured architecture, where each branch is a distinct system or subsystem of the C-ES. This allows us to extract results which remain valid despite internal architectural modifications, as long as each system or subsystem of the architecture remains operationally the same, and regardless of its placement in the ship's architecture. The risk analysis is carried out by considering the likelihood of an attack and its impact. For the risk analysis of the C-ES we employed he risk matrix of figure 2 and used the criteria shown in table 1 and in table 2 to assess risk. These criteria take into account the attack likelihood and the respective impact, and follow [23].


Likelihood
Impact

HIGH	HIGH	MEDIUM
HIGH	MEDIUM	LOW
MEDIUM	LOW	LOW

Fig. 2: Risk Matrix

High (H)	1. Threats that could result in loss of human life. 2. Threats that could result in wide energy loss. 3. Threats that may cause damage in the infrastructure. 4. Threats that will lead to personal information leakage. 5. Threats that will result in economical damage and client loss. 6. Threats that will result in system malfunction.
Medium (M)	1. Threats that could cause procedure disruption in real time. 2. Threats that could result in miscalculations in the systems, thus influencing the operations. 3. Threats that could result in bad reputation for the company and client's dissatisfaction. 4. Threats that may cause information disclosure. 5. Threats that could influence the system's integrity. 6. Threats that could influence the system's availability. 7. Threats that could result in legal sanctions. 8. Threats that could cause network information leakage.
Low (L)	1. Threats that could result in operation delay or disruption in non-critical procedures. 2. Threats that could result in leakage of non-sensitive data.

Table 1: Threat Criteria

Very Likely (VL)	1. The adversary is highly motivated and capable, and there are no deployed countermeasures. 2. Existing popular exploits which can be executed at any time. 3. High system's exposure to the Internet.

Moderate (M)	1. The adversary is highly motivated and capable, while the systems countermeasures are not enough to prevent the attack. 2. The system's vulnerability is widely known, but the attacker has to gain physical access to the system. 3. Systems are not directly exposed to the Internet.
Rare (R)	1. The attacker is not highly motivated or does not have the necessary knowledge to perform an attack, or the deployed countermeasures are sufficient. 2. An attacker must have administrative rights to perform the attack. 3. The system is not connected with external networks or systems.

Table 2: Likelihood Criteria

4.2 Applying STRIDE to the Cyber-Enabled Ship

A full analysis of attacks against the systems and subsystems of the Cyber-Enabled Ship as shown in 1 using STRIDE has been carried out in [24]. In the interest of adhering to space limitations, in this section we present a selected subset of the results of [24]. The selection criteria were the diversity and representativeness of the results. In the tables that follow ”I” stands for ”Impact”, ”L” stands for ”Likelihood” and ”R” stands for ”Risk”.

T	**Engine Automation System-EAS**	**I**	**L**	**R**
S	An adversary providing false information that the lubrication systems do work efficiently, when they do not, could result in engine damage. The system's exposure to the Internet is medium.	H	M	H
T	Tampering with a command to the engine control could lead to physical damage to the ship or to human injury.	H	R	M
R	Most of the system's operations are crucial for the ship; thus, the repudiation of actions is not acceptable.	M	R	L
I	Information disclosure will not adversely affect operations or the environment.	L	R	L
D	The availability of this system is very important, since the interruption of its operations will restrain the ship and most of its subsystems.	H	M	H
E	An attacker that gains administrative rights, may execute commands that can be catastrophic to the infrastructure.	H	R	M

Table 3: Engine Automation Systems-EAS

T	**Bridge Automation Systems-BAS**	**I**	**L**	**R**
S	Identity spoofing caused by malware can be used to cause damage to the infrastructure and/or to humans. The system's exposure to the Internet is high.	H	M	H

T	Data tampering could cause disruption of crucial operations. This can lead to damage to the cargo, the ship or the infrastructure	H	R	M
R	The repudiation of actions is not allowed in this system, as it is a crucial component and these actions could adversely affect human safety.	H	R	M
I	A breach of confidentiality may pose serious risks to the security of the cargo and to the infrastructure in general.	M	M	M
D	In systems which are responsible for ensuring the security and safety of operations, a data delay or loss is unacceptable. Loss of availability in such a system could expose the ship to a high risk.	H	M	H
E	An attacker with administrator access in the system has full ship control.	H	R	M

Table 4: Bridge Automation Systems-BAS

T	**Shore Control Center-SCC**	**I**	**L**	**R**
S	The SCC could be compromised by an adversary with access to another users credentials. This could lead to a catastrophic scenario for the ships cargo, or the ship itself, and could put human lives at risk. The system's exposure to the Internet is high.	H	M	H
T	Data tampering could lead to a system crash. Changing the navigation information, for example, can cause a change of destination.	H	R	M
R	The consequences of repudiation are crucial and not acceptable. Every action must be attributable to a known person.	M	R	L
I	A breach of confidentiality could lead to loss of cargo and could induce economic damage to the shipping company.	L	R	L
D	Loss of availability could cause loss of the capability to monitor the ship, and to acquire data which contribute to the efficient sailing. This sub-system works in real time and this makes its availability crucial.	H	M	H
E	This threat could cause violation of the systems integrity, availability and confidentiality since an adversary with elevated privileges could control the entire ship.	H	R	M

Table 5: Shore Control Center-SCC

T	**Autonomous Engine Monitoring and Control-AEMC**	**I**	**L**	**R**
S	An adversary with elevated privileges could execute unauthorized actions which will expose the engines to high risk. The system's exposure to the Internet is medium.	H	R	M
T	Data integrity violations can cause malfunctions, since critical operations are executed by this sub-system, e.g. rudder control.	H	M	H
R	The repudiation of actions is critical, since process disruption can lead to the shipping company's economic loss or even to jeopardize human safety.	H	R	M

I	The leak of information will not cause an operational malfunction to the system.	L	M	L
D	Loss of availability could cause significant consequences to the infrastructure, since the AEMC is the main control system of the engines, the vessel's speed and the power production.	H	M	H
E	The acquisition of administrative rights will cause the execution of unauthorized actions which could damage the infrastructure.	H	R	M

Table 6: Autonomous Engine Monitoring and Control AEMC

T	**Engine Efficiency System-EES**	**I**	**L**	**R**
S	An adversary could alter fuel consumption data. This may lead to engine malfunction and could cause delay to the ship's operations. The system's exposure to the Internet is medium.	H	M	H
T	The violation of integrity will put at risk the entire infrastructure, by impeding maintenance in case of errors.	H	R	M
R	The repudiation of an action is unacceptable; every action must be fully attributable.	M	R	L
I	Disclosure of system information will not cause significant impact to the ship or to the shipping company.	L	R	L
D	Disruption of system operation could lead to a malfunction of engine systems without, however, extended damage.	H	M	H
E	An attacker with administrative rights will be able to stop the operation of many systems, and to alter data which adversely affect the capability to monitor the ship's operation from the shore.	H	R	M

Table 7: Engine Efficiency System

T	**Maintenance Interaction Systems-MIS**	**I**	**L**	**R**
S	An adversary with elevated privileges could interrupt operations by preventing a maintenance procedure. The system's exposure to the Internet is medium.	H	R	M
T	By tampering the Key Performance Indicator values, an attacker could effect a false notification to the SCC of need for maintenance of the system.	H	M	H
R	Repudiation of actions in this sub-system is unacceptable, as responsibilities must be fully attributable to specific persons.	M	R	L
I	The system's operation does not entail sensitive data, so a possible information disclosure does not have significant impact to the system's operation or to the ship.	L	R	L
D	The availability of this system is crucial. If an attacker manages to render this system unavailable, s/he could inflict a malfunction in the infrastructure and/or economic loss.	H	M	H
E	Gaining administrative rights in this system could cause economic damage and bad reputation for the shipping company.	H	R	M

Table 8: Maintenance Interaction Systems

T	Navigation Systems-NavS	I	L	R
S	An adversary using another user's credentials could inflict a malfunction, and will be able to change the ship's course. This could cause economic damage for the shipping company and damages to infrastructure. This sub-system's exposure to the Internet is high.	H	M	H
T	The violation of system's integrity could cause cargo loss or damage to the components of the ship or even to the entire infrastructure.	H	M	H
R	The repudiation of actions in this sub-system is unlikely, since the persons who manage and operate it are known.	H	R	M
I	The leak of navigational information could lead to cargo loss and damage to the infrastructure. Legal consequences may arise for the shipping company too.	H	M	H
D	Loss of availability could cause economic damage to the company, since the vessel will not be able to sail.	H	M	H
E	If an adversary gains elevated privileges in this sub-system, s/he will be able to change the ship's destination.	H	R	M

Table 9: Navigation Systems

T	Autonomous Ship Controller-ASC	I	L	R
S	Malware infection could cause damage to the cargo management systems or to the GMDSS. This system's exposure to the Internet is high.	H	M	H
T	The alteration of data and files in this sub-system is unacceptable, since it could result in system destruction. Also an attacker could change the ship's course.	H	R	M
R	This system handles crucial sub-systems; this is why all the actions and procedures are fully attributable to each person separately and repudiation is unacceptable.	M	R	L
I	The data handled by this sub-system are related to the ship information and its environment, and most of them are sensitive.	M	R	L
D	The availability of this system is very important since without it the ship may not be able to sail.	H	M	H
E	An adversary with administrative rights will be capable to change system parameters and influence operations. This could harm the infrastructure and result in litigation against the shipping company.	H	R	M

Table 10: Autonomous Ship Controller-ASC

T	Human Machine Interface-HMI	I	L	R
S	An attacker could obtain access to the system and critical information. This will influence the entire infrastructure and cause bad reputation for the company or even litigation. This sub-system's exposure to the Internet is high.	H	M	H

T	Data tampering in this system will put the ship in danger since through this system, unauthorized humans in the shore are able to control and monitor the ship.	H	M	H
R	Repudiation of actions in this system is not possible, because its operation is fully defined and its internal procedures stem from other sub-systems.	M	R	L
I	The HMI contains information which are crucial for the ship's sailing. A disclosure of this information could lead to damage, since these relate to the vessel's navigation and management.	H	M	H
D	Availability is critical for secure sailing. If this system becomes unavailable, the vessel will be control-less and invisible to the SCC.	H	M	H
E	An attacker with administrative rights to the system will be able to access sensitive data about the vessel's condition, its customers, and passengers. This could raise legal issues for the shipping company.	H	M	H

Table 11: Human Machine Interface-HMI

T	**Remote Maneuvering Support System-RMSS**	**I**	**L**	**R**
S	An adversary with access privileges could alter the ship's control and manipulate its operation. This could cause malfunction to the ship's systems and delay to its operation. This sub-system's exposure to the Internet is medium.	M	M	M
T	Data tampering can cause damage to the ship's engines, due to the close connection with the EAS.	M	M	M
R	All the actions and procedures in RMSS are predefined and their repudiation is not acceptable.	M	R	L
I	A breach of data confidentiality could reveal information about the vessel's position, but would not cause the malfunction of other systems.	H	M	H
D	An attack which targets the system's availability will influence the infrastructure to high extent and could result in delays in the process.	M	M	M
E	An access to the system with high privileges could cause crucial problems to the infrastructure, as the RMSS is connected directly with the engines and an attacker could manipulate their operation.	H	R	M

Table 12: Remote Maneuvering Support System-RMSS

T	**Emergency Handling-EmH**	**I**	**L**	**R**
S	If an attacker spoofs the identity of the fire alarm system, s/he will be able to activate or deactivate the firefighting system and destroy some ship components. This sub-system's exposure to the Internet is low.	M	M	M
T	The violation of data integrity in this system could start the wrong alarm in the ship. This could lead to ship's flooding and harm the infrastructure.	M	M	M

R	The repudiation of action in this system is unacceptable. All the roles are predefined, and no one should be able to claim that s/he did not start the alarm in case of emergency.	M	R	L
I	A breach of the system confidentiality could not harm the infrastructure to a high extent.	M	R	L
D	Loss of availability could pose a risk to the ship and its cargo, because in a case of emergency SCC will not be notified.	H	M	H
E	If the attacker gains administrative rights in this system, s/he will able to deactivate system alarms.	H	R	M

Table 13: Emergency Handling

T	**Automatic Identification System-AIS**	**I**	**L**	**R**
S	An adversary using another AIS device is able to spoof their identity and receive system information. This sub-system's exposure to the Internet is low.	M	V	M
T	Altering the system's data is an important problem for the ship since AIS has information which may be confidential.	H	M	H
R	AIS is an automatic system and its internal procedures are well defined. Repudiation of its actions is not acceptable and could result in economic damage to the ship owner.	H	V	H
I	As already noted, this system's information is confidential, and its disclosure could cause problems to the infrastructure. Information about cargo and destination are included in this sub-system, so a potential leak may influence the ship's operation.	H	M	H
D	The loss of availability could affect the ship's operations directly, because AIS handles ship traffic information and other static and dynamic information on the vessel.	H	R	M
E	If an adversary gains administrative rights in the system, s/he will be able to execute unwanted action, such as changing ship navigation information.	H	M	H

Table 14: Automatic Identification System-AIS

T	**Electronic Chart Display and Information System-ECDIS**	**I**	**L**	**R**
S	If an unauthorized user gains the credentials of a legitimate user, s/he could inflict damage to the ships infrastructure. This system's exposure to the Internet is medium.	H	M	H
T	Tampering with ECDIS data could cause problems to the ship's operation, since an attacker could intercept the ship's course by changing the maps.	M	M	M
R	The system's actions are well defined, and their repudiation is not acceptable.	M	M	M

I	ECDIS has many interconnections with other systems and subsystems; as such, it handles various pieces of information which may be personal or sensitive. The disclosure of these information could raise legal issues for the shipping company.	H	M	H
D	The loss of ECDIS's availability is unacceptable, since the ship could not sail without it.	H	M	H
E	Gaining administrative rights by unauthorized persons for this system could cause crucial issues for the vessel. An attacker could execute unwanted actions like altering maps. This may lead to economic loss and bad reputation.	M	R	L

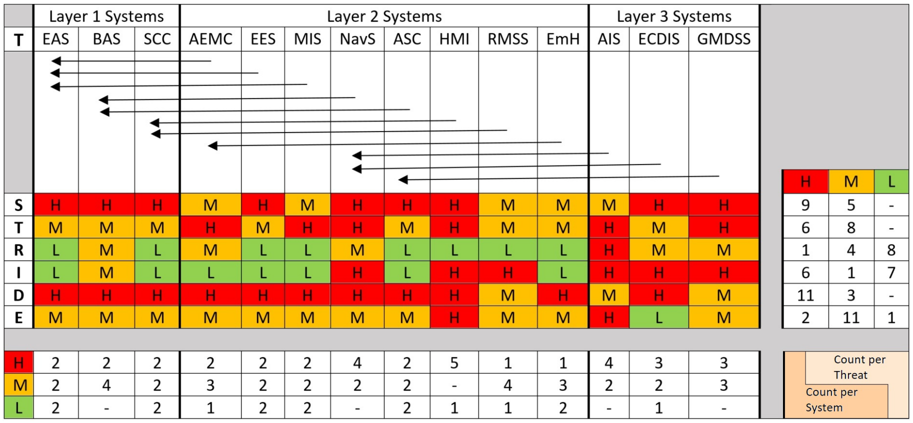
Table 15: Electronic Chart Display and Information System-ECDIS

T	**Global Maritime Distress and Safety System-GMDSS**	**I**	**L**	**R**
S	An attacker could spoof the identity of another ship through GMDSS and transmit false data between the two ships. This will influence the cargo security, raise economic issues and even adversely affect the safety of people on board. This system's exposure to the Internet is high.	H	M	H
T	The violation of data integrity is important, since information about weather conditions and the ship's position are transmitted through this system. The alteration of these could cause economic damage and human injury.	H	M	H
R	Most of the system's actions are crucial for the ship's security and safety. Therefore, repudiation of these actions is unacceptable.	M	M	M
I	GMDSS interacts directly with the SCC and exchanges sensitive information about the ship and its operations. A breach of confidentiality in this system could harm the entire infrastructure.	H	M	H
D	A Disruption of operation of the GMDSS could pose a high risk to the vessel's operation, since this system is the main communication channel in case of emergency.	H	R	M
E	An adversary that has gained access with high privileges could activate or deactivate the vessel's alarms and emergency communication.	H	R	M

Table 16: Global Maritime Distress and Safety System-GMDSS

5 Summary of results and discussion

Figure 3 summarizes the results and main contributions of our study. Specifically, in accordance to the proposed system taxonomy, the connections between parent nodes and their children in 1 are illustrated by arrows, where each arrow is directed from the children systems towards the parent systems. Furthermore, the table depicts all the calculated risk levels. The table also enumerates the number of high, medium and low level threats per system (vertical count), and records the number of times where each threat has appeared across the systems (horizontal count).



	Layer 1 Systems			Layer 2 Systems								Layer 3 Systems					
T	EAS	BAS	SCC	AEMC	EES	MIS	NavS	ASC	HMI	RMSS	EmH	AIS	ECDIS	GMDSS	H	M	L
S	H	H	H	M	H	M	H	H	H	M	M	M	H	H	9	5	-
T	M	M	M	H	M	H	H	M	H	M	M	H	M	H	6	8	-
R	L	M	L	M	L	L	M	L	L	L	L	H	M	M	1	4	8
I	L	M	L	L	L	L	H	L	H	H	L	H	H	H	6	1	7
D	H	H	H	H	H	H	H	H	H	M	H	M	H	M	11	3	-
E	M	M	M	M	M	M	M	M	H	M	M	H	L	M	2	11	1
H	2	2	2	2	2	2	4	2	5	1	1	4	3	3			
M	2	4	2	3	2	2	2	2	-	4	3	2	2	3			
L	2	-	2	1	2	2	-	2	1	1	2	-	1	-			

Count per Threat
Count per System

Fig. 3: Summary

The C-ES systems that have been identified to be the most vulnerable are the HMI, NavS, AIS, ECDIS and GMDSS. It is important to highlight that both AIS and ECDIS are sub-systems of NavS, which also reached high risk levels. By leveraging the information in Figure 3, we can conclude that parent nodes with highly vulnerable children inherit the vulnerabilities of their sub-systems. Further, we should note that the AIS, ECDIS and GMDSS, which have reached the highest risk level in four out of six STRIDE threats, are parts of the infrastructure that has already been adopted by the shipping industry as part of the traditional ship, within the context of the C-ES. Furthermore, these systems are crucial for the efficient and effective operation of the C-ES, since they are strictly connected with the BAS systems. Further, we should focus on the HMI system, since it has reached high risk levels, its exposure to the internet is high, and it is being used by the SCC. Hence, its vulnerabilities should be addressed promptly to avoid critical system malfunctions.

Analyzing the information in Figure 3 from the perspective of threats, it becomes apparent that Denial of Service and Spoofing are the most critical threats for the C-ES systems. Specifically, Denial of Service and Spoofing have been found to be high level threats eleven and nine times respectively. STRIDE threats such as Tampering and Elevation of Privileges have been recognized as medium level threats, since they refer to more sophisticated and difficult to execute attacks, while in order to exploit these vulnerabilities the adversary should be highly motivated. Finally, Repudiation and Information Disclosure are low criticality threats for the C-ES systems.

6 Conclusions and future work

In this work we systematically classified the systems and sub-systems of Cyber-Enabled Ships, providing a taxonomy of the components that constitute the C-ES's ICT architecture; this was used as input to the STRIDE threat modeling methodology to identify attacks against the C-ES and to assess the accordant risk. The results show that the C-ES faces some high risks, related particularly to the AIS, the ECDIS and the GMDSS. At the sub-system level, high risks are posed by attacks against the HMI and the Navigation system, whereas their own sub-systems have been found to be vulnerable in high risk attacks as well. These risks propagate upwards in the architecture, resulting in high risks for the BAS and the SCC, whereas the risk associated with the EAS is lower. For future work, we intend to extend these results by utilizing other threat modeling and analysis methods, and also to integrate the notion of safety risk in the analysis. We also intend to define appropriate countermeasures to reduce the identified risks.

References

1. Lloyds Register. Cyber-enabled ships. page 20, 2016.
2. Rolls-Royce. Remote and autonomous ship-the next steps. page 88, 2016.
3. Microsoft. The stride threat model, 2009.
4. MUNIN. Maritime unmanned navigation through intelligence in networks, 2016.
5. Ø. J. Rødseth and A . Tjora. A system architecture for an unmanned ship. 05 2014.
6. Ø. J. Rødseth, B. Kvamstad, T. Porathe, and H. C. Burmeister. Communication architecture for an unmanned merchant ship. In *2013 MTS/IEEE OCEANS - Bergen*, pages 1–9, June 2013.
7. H.-C. Burmeister, W. Bruhn, L. Walther, J. A. Morus, and B. Sage-Fuller. Munin d8.6: Final report: Autonomous bridge. Technical report, 2015.
8. S. N. MacKinnon, Y. Man, and M. Baldauf. Munin d8.8 final report shore control centre. Technical report, 2015.
9. M. Schmidt, E. Fentzahn, G. F. Atlason, and H. Rødseth. Munin 8.7 final report autonomous engine room. Technical report, 2015.
10. Ø. J. Rdseth and H.C. Burmeister. Risk assessment for an unmanned merchant ship. *TransNav*, 9(3):357–364, 2015.
11. K. Tam and K. Jones. Cyber-risk assessment for autonomous ships. page 9, 2018.
12. Sokratis K. Katsikas. Cyber security of the autonomous ship. In *Proceedings of the 3rd ACM Workshop on Cyber-Physical System Security*, CPSS '17, pages 55–56, New York, NY, USA, 2017. ACM.
13. S. Hussain, A. Kamal, S. Ahmad, G. Rasool, and S. Iqbal. Threat modelling methodologies: A survey. 26:1607–1609, 01 2014.
14. F. Sidi, A. J. Marzanah, L. S. Affendey, M. Zolkepli T. M. Ming M. F. A. Mokthi M. Daud N. B. Zainuddin I. Ishak, N. M. Sharef, and R. A. Hamid. A comparative analysis study on information security threat models: A propose for threat factor profiling. *Journal of Engineering and Applied Sciences*, 12:548–554, 2017.
15. Chun Yu (CY) Cheung. Threat modeling techniques, 2016.
16. H. Havinga and O. Sessink. *Risk Reduction Overview Manual*, version 1.0 edition, 2014.
17. S. Krishnan. A hybrid approach to threat modelling. page 24, 2017.
18. ICS INTERCARGO INTERTANKO OCIMF BIMCO, CLIA and IUMI. The guidelines on cyber security onboard ships. page 51.
19. W. Bruhn, H. C. Burmeister, L. Walther, J. Morus, M. Long, M. Schaub, and E. Fentzahn. Munin d5.2: Process map for autonomous navigation. Technical report, 2013.

20. D. Kokotos, D. Linardatos, N. B. Nikitakos, and E. S. Tzannatos. *Information and communication technologies in shipping industry(In Greek)*. Stamoulis, 2011.
21. H. Nordahl Ø. J. Rdseth. Nfas-definitions for autonomous merchant ships. 10 2017.
22. A. Shostack. *Threat Modeling: Designing for Security*. Wiley Publishing, 1st edition, 2014.
23. B. Jelacic, D. Rosic, I. Lendak, M. Stanojevic, and S. Stoja. Stride to a secure smart grid in a hybrid cloud. In *CyberICPS/SECPRE@ESORICS*, 2017.
24. Georgios Kavallieratos. Cyber-attacks against the cyber-enabled ship, 2018.