https://doi.org/10.53656/ped21-7s.16appr

Education and Aspects of Maritime Security

APPROACH TO SHIP'S IT AND OT SYSTEMS CYBERSECURITY IMPROVEMENT

Stoyno Stoynov, Borislav Nikolov
Nikola Vaptsarov Naval Academy (Bulgaria)

Abstract. Daily cyber-attacks on ships' IT and OT systems are not a rare occurrence anymore. This has been taken into account in recent years and the IMO has issued directives and circulars with recommendations for increasing the cybersecurity of ship information systems as part of the overall ship security system. The effect of a successful cyber-attack of any kind, on elements of the ship's IT and OT systems, can have a disastrous impact not only on the ship itself but also on the environment. While modern ships can be designed and all modern methods implemented to reduce and prevent the possibility of cyber-attacks onboard existing ships, it is not possible to achieve this security level and it is necessary to implement various solutions. At the same time, the ships' crew is declining worldwide and most ships do not have IT officers or trained staff onboard to maintain the ship's information systems. Because of that, the solutions that need to be put in place to increase the security of ship's information systems must be easy to implement, use, and maintain. This article examines the need and some technical solutions that can be used to improve the cybersecurity of ship's IT and OT systems in response to the existing cyber-attacks and threats in the global shipping and maritime industry.

Keywords: ship's information technology systems; ship's operational technologies systems; unified threat management; cybersecurity; cloud-based service; virtual appliance

Introduction

In June 2017, at a session of the Maritime Safety Committee (MSC) of the World Maritime Organization (IMO), Resolution MSC.428 (98) "Maritime Cyber Risk Management in Safety Management System" was adopted, according to which as of 01 January 2021 all ships must have a developed Cyber Risk Management plan as part of the Ship Management System. The resolution states that approved Ship Safety Management Systems (SMS) should take into account the Ship's Cyber Threat Management Plan following the objectives and functional requirements of the International Safety Management (ISM) code. It also encourages the Maritime Administrations to ensure that Shipboard Cyber Threat Management Plans are

reviewed and properly implemented in Safety Management Systems no later than the first annual review of the company's compliance document after 1 January 2021.

In July 2017, the International Maritime Organization issued a circular MSCFAL.1/Circ.3 "Guidelines on Maritime Cyber Risk Management", based on which Recommendations to the ship's cyber threat management plan were created[1]. The IMO guidelines also emphasize that the effective management of the ship's cyber threats must begin at a high management level. This management should implement a culture of ship cyber threat awareness on all levels and individual ship commands, also to ensure a comprehensive and flexible cyber threat management regime that is ongoing and continuously assessed through effective feedback mechanisms.

Systems that rely on digitalization, automation, and integration are being increasingly used on board. Those systems require a Cyber Threat Management Plan. As technology continues to evolve, information technology (IT) and operational technology (OT) on ships are networked together and most often connected to the Internet. This carries a higher risk of unauthorized access or malicious attacks on ship systems and networks. Risks may also arise from personnel who have access to onboard systems, such as the introduction of malware via removable media (USB flash memory or hard disk).

In recent years, ships' IT/OT systems and information systems ashore serving the shipping industry have been at a very high technological level and have been the subject of various types of cyber-attacks. A possible cyber-attack would jeopardize or impede the security and/or control of the ship and its systems. While all new and newly built ships can be designed to implement all necessary methods to reduce and prevent the possibility of cyberattacks, onboard existing ships it is not easily possible to achieve this and it is necessary to implement various additional measures. Because the ships' crew is declining worldwide and most ships do not have IT officers or trained crew onboard to service and maintain the ship's information systems, the technical solutions that need to be put in place to increase the security of ships IT/OT must be easy to implement, to use and to maintain.

There are many examples in world shipping where financial losses have occurred as a result of various cyber incidents. Some of the most notable are:

– In September 2020, the French shipping company CMA CGM SA saw two of its subsidiaries in Asia hit with a ransomware attack that caused significant disruptions to IT networks, though it did not affect the moving of cargo[2].

– The Clarksons Cyber Security Hack – In a series of high-profile hacks in corporate America, including Deloitte, Yahoo, and Equifax, Clarksons, the world's largest shipbroker, suffered a cyber-attack in November 2017 via an "unauthorized access gained via a single and isolated user account"[3].

– In June 2017, Maersk was hit by the non-Petya malware as part of a national attack. The virus stopped the company's operations in Rotterdam, Los Angeles, Mumbai, Auckland, and many more ports around the world[3].

– Over two years starting from June 2011, the Port of Antwerp suffered from continuous cybersecurity attacks that controlled the movement and location of containers. This allowed drug traffickers to hide illegal substances among the legitimate cargo[3)].

– Offshore oil workers unintentionally uploaded malware that disrupted computer networks by downloading infected files of pornography and illegal music directly, and by bringing infected laptops and USB drives on board. The malware disabled the signals to the dynamic positioning thrusters, so the MODU drifted off of the well site. For safety reasons, the well was temporarily shut down[3)].

– In June 2017 at least 20 ships in the Black Sea were reporting false data was being transmitted, indicating the ships were 32km inland of their actual position. It is now believed to have been a result of a GNSS spoofing attack (Otto 2020).

Each of the cyber incidents presented above is a result of human error. To minimize these and other errors it is recommended end-users be familiarized with vulnerabilities in computer systems and networks. That can be achieved through organized training. This is also relevant for any kind of computer network not only for the ships'.

Following the requirements of the International Maritime Organization through the Recommendations to the Ship Cyber Threat Management Plan and the need to enhance cybersecurity of ship's IT/OT systems by using easy to implement, to use and to maintain devices, the use of Unified Threat Management (UTM) is one of the solutions to the problem. In any case, staff training (both on a ship and ashore) remains the fundamental process to reduce the possibility of cyber incidents. This training must be periodic and on all levels of competencies and responsibilities.

Ship cybersecurity improvement

To reduce the impact of cyber threats in all fields of human activity, the maritime industry included, there are two types of activities. These are the procedures and the training, as well as the technical means and measures.

Cybersecurity procedures and training on ships

Based on the BIMCO publication entitled "The Guidelines on Cyber Security Onboard Ships" version 4, procedural controls are focused on how personnel uses the onboard systems[4)]. Several types of procedures can be introduced to improve a ship's cybersecurity.

Cybersecurity is the responsibility of not only the IT department but all employees. Because of that, the first and the most important procedural action is the training, and awareness, of all of both onboard and shore-side personnel.

The awareness procedures must cover at least the risks related to internet usage, emails, the usage of own devices in a corporate network, antivirus programs,

removable devices, and other risks related to specific ship's onboard and ashore activities.

The training must be focused on technical cybersecurity measures and must be conducted in a realistic environment. Usually, on a ship's board, there are no such conditions. Therefore, the training must be conducted ashore before the crew members responsible for the implementation of the technical cybersecurity measures start their contract.

Other procedural actions related to ship's cybersecurity, which are of no less importance, are as follows[4]:

– Policy for granting guest/visitor access to ship's computer network – that includes every one person who is not part of ship's crew but wants to use different ship's computer network devices such as workstations, printers, and so on. Guest/visitor are authorities, technicians, agents, port and terminal officials, and also the ship's owner representatives;

– Policy for granting remote access to ship's computer network – this policy should determine who can have remote access to ship's IT and OT systems, in what circumstances can remote access be used and what can be done through remote access;

– Policy for ashore support in case of a cyber incident;

– Policy for administrative privileges usage – this kind of privilege should be restricted to certain crewmembers. User privileges must be removed as soon as possible once a crewmember leaves the board;

– Policy for IT and OT software upgrades and maintenance – it is required to ensure the full software lifecycle of this systems;

– Policy for updates of antivirus and antimalware tools (both software and physical tools) – it is mandatory for these tools to have up-to-date definitions distributed on a timely basis;

– Policy for removable media devices control – the removable devices can be used for data leakage or malware introduction;

– Policy for data destruction and physical equipment disposal – must ensure that there is no sensitive information stored on equipment that will be disposed of;

– Any other ship and/or company's specific policies related to cybersecurity.

All the mentioned procedures and policies, including the training and awareness, must be implemented to acquire a required level of ship's IT and OT systems cybersecurity. This procedure list is exemplary and should not be seen as exhaustive.

No matter how well the procedures and policies are designed and implemented, they are not enough. Furthermore, some procedures and policies require the use of technical devices to implement them. Since most merchant ships lack IT specialists, the cybersecurity devices should be easy to use and, if possible, combine several functions. For this reason, Unified Threat Management (UTM) type devices are extremely suitable.

Unified Threat Management

The main purpose of Unified Threat Management (UTM) devices is to protect small (or medium) size business' networks. The UTM can be a physical hardware device, software, or even a cloud service. By design, UTM combines several security features and is constituted to help protect a computer network from different security threats. Risks to overall security can include malware and targeted cyber attacks to multiple parts of the network communication structure, as well.

UTMs and Next-generation firewalls are sometimes misidentified by mistake. One of the major distinctions, that can be pointed out, is that NGFW mostly offers fewer additional features, compared to the UTM devices. It should be stated that NGFW do provide increased protection, which is lacking in traditional firewalls. Service failure protection and intelligence applications and intrusion prevention systems are also in place for NGFW. UTM, on the other hand, does offer features for network security such as spam and URL filtering, IDS/IPS, antivirus software, Virtual Private Networks (VPN). Those come on top of the NGFW[5]. That list of features will only expand in time. The convenience of using UTM is that it offers a singular, simplified platform for a wide variety of information security features.

The onboard network security depends on the implementation of IT/OT systems. A focal point is the adoption of corporate policy based on risk assessment. The unforeseen miss of built-in mechanisms for cyber risk management at the construction level of a ship is among the major concerns in the maritime industry today. It is recommended that the network layout and network management be planned for all newly built ships. Prevention of direct and unmonitored connection between controlled and any other networks should be in place at all times. The following precautions need to be added for such prevention to take place:

– Network segmentation;
– Traffic management;
– Encryption protocols management;
– Certificates management.

It is essential to consider the physical location of primary network devices, including servers, switches, firewalls, and cabling. This will provide access restriction and preserve the physical security of the network installation. That will provide regulation to the network entry points.

Each network design needs to include a network administration and management infrastructure for all the used devices including the endpoints.

Ship networks should usually provide the following[4] (Fig. 1):

– Communication between OT endpoints;
– Management and control of OT equipment;
– Ship administration and other business tasks;
– Internet access.

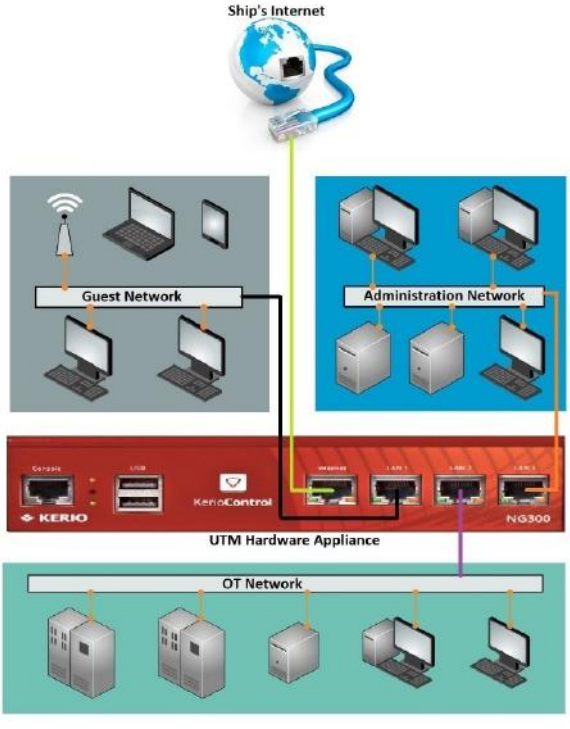

Figure 1. Ship's IT/OT network partitioning using UTM hardware appliance[4]

A division between public and system networks on the ship must be in place as a security measure. To complete such this objective, an appropriate combination of the following techniques can be used[4)]:

– Network firewalls;
– Network switches;
– Virtual local area networks (VLANs).

In the example shown in Figure 1, the network is segmented with an installed UTM hardware appliance with an integrated firewall that supports three VLANs iv for different endpoints, as follow:

– VLAN for OT equipment and systems;
– Configuration of Management VLAN and network monitoring;
– VLAN for the crew and guests, providing internet access.

All the implemented techniques and security measures must not affect the operation of a ship's systems, especially during a cyber incident. Each OT network aboard has several endpoints which are very important as they control the operation and security of the system[4)].

The use of a multi-layered strategy should be in place, to ensure maximization of the protection level of the ship's systems[4)].

In addition, an effective in-depth protection strategy requires a thorough understanding of the possible attack vectors of a ship's OT systems. The attacks may aim to affect one or more of the following[4)]:

– Network equipment backdoors and weaknesses;
– Exploitable networking protocols vulnerabilities;
– Vulnerabilities in OT endpoints and sensors;
– Unprotected databases.

To perform applicability tests in a ship computer network, a practical installation with configured both Kerio Control Firewall and Sophos NG Firewall has been created. In figure 2, the topology of the practical installation is presented. The real practical installation is shown in figure 3.

The creation of the practical installation is dictated by the need to design and configure VLANs, create user groups and user accounts, introduce group rules, including the use and prioritization of ship Internet traffic, security, and IPS in conditions that are as close as possible to the real conditions of most of the existing merchant ships.

Two different UTM devices were used for the realization of the practical installation. In this way, the advantages and disadvantages of each of them can be assessed. At the same time, a reduction in the effect of their disadvantages is achieved.

As an Internet service provider two 3G routers, GlobeSurfer III and GlobeSurfer III+ were used, each of them with two LAN ports. They deliver simultaneously Internet to the two hardware UTM devices. Thus, with a practical installation and wiring, the simultaneous connection of the two firewalls is realized, which in practice protects separate networks.

Each UTM device is connected to the 3G routers in Load-Balancing network interface mode. Other available options are Failover mode and Single link mode in the case of a single Internet provider. Based on internal rules for each UTM, their network traffic is routed through the 3G routers to achieve a load balancing for the UTM's WAN interfaces. These rules are set by the manufacturers so the network administrator needs to select only the operation mode of the devices. To reduce network traffic 3G routers are set to connect to the Internet only when there is an attempt to send data via the Internet. This will reflect the network speed for the clients.

The technical characteristics of GlobeSurfer III and GlobeSurfer III+ are available on their manufacturer's website.

The UTM solutions used in the practical installation were the Kerio Control NG 100w hardware appliance and the Sophos XG Firewall software appliance. The second UTM solution is a Sophos OS 18.0 software installed on Windows OS on a hardware device HP ProLiant DL380 G7 Server (Fig. 2 and Fig. 3).

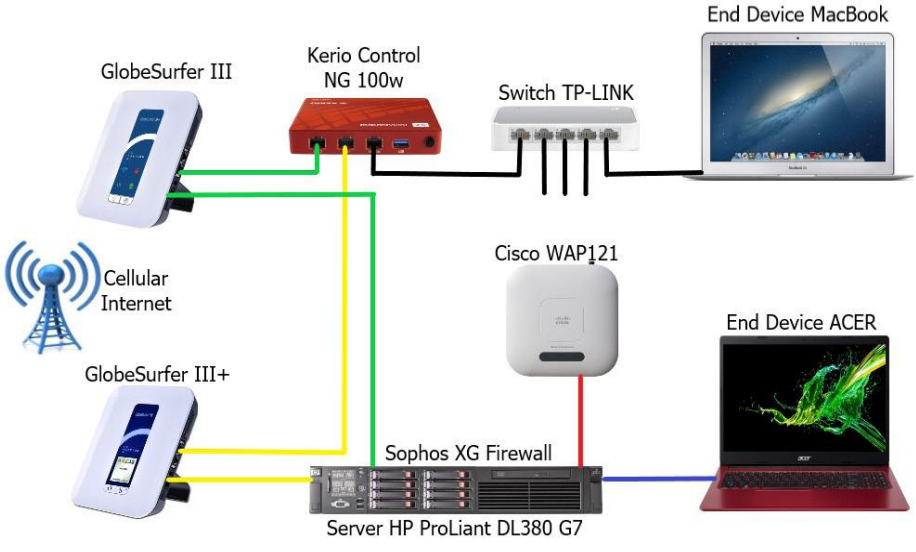

Figure 2. A principle topology of practical IT network installation with internet access redundancy by using UTMs from different vendors

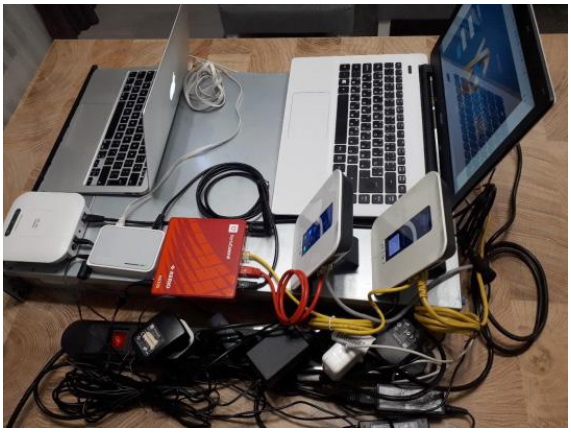

Figure 3. A practical realization of presented IT network with UTMs

Upgrades of the presented topology are related to the protection of the I/O (input/output) modules, which are parts of the ship's OT systems. This can be done by using a WAGO PFC200 controller, which records all measurement and control data, encrypts them directly into the controller via SSL encryption and transmits

the data over a VPN connection based on OpenVPN or IPsec and using SSL/TLS connections. These types of connections allow the transmission of encrypted data, even over wireless communication systems[6].

Additional upgrades of the topology are related to implementing a centralized network monitoring system (NMS). In the current configuration, all events and syslogs are stored locally on every one device. NMS systems can provide summary information about the current state and historical data for the monitored devices. There are many NMS systems available on the market. Some of them can be used remotely. In this case events and syslogs data routing should be configured.

The following administrative tasks were performed for both UTM systems:

– Virtual appliance installation and configuration – only for Sophos NG Firewall;
– Network interfaces setup;
– Necessary VLANs creation;
– Wireless networks setup;
– VPN networks setup;
– User groups creation;
– User accounts creation;
– Network traffic management rules creation;
– IPS configuration;
– Configuration of additional network security settings;
– Antivirus configuration;
– Network traffic prioritization rules creation;
– Content filtering rules creation;
– Remote management and monitoring setup.

The comparison of the installed and presented UTM solutions can be based on their implementation and usage on board of the merchant ships.

Both UTM solutions have found implementation on board ships, and in the last few years, it has been observed that on board ships the Internet networks are upgraded by adding of Kerio Control Firewall or Sophos XG Firewall. Those upgrades are accompanied by the implementation of the ship's action plan in case of cyber threats and attacks, which is the requirement of the International Maritime Organization. Hardware devices are preferred because they require less time to deploy and configure ports and are easier to maintain by the shipboard personnel.

Both of the presented UTM devices are successfully integrated into existing ships' networks. Their implementation in newly built ships depends on the type of ship, the number of users and the shipping company.

High Availability is available as an option for both device types (Kerio Control Firewall and Sophos XG Firewall). That means a second hardware device to be in standby operating mode with the same license, configuration and settings.

Both platforms offer intuitive software, but the Kerio Control Firewall's Graphical User Interface (GUI) is more easily accessible and preferred by shipboard

personnel responsible for maintaining onboard IT systems. The management and monitoring of users' internet traffic, as well as their logging into the ship network, is also better organized by Kerio Control Firewall. On board ships with a large number of crew members and guests (cruise and passenger ships), where there are ship IT specialists, the use and operation of Sophos products are preferred. The main reason is that it takes less time to configure the whole system through the application of group rules that can be easily cloned and applied to a large number of hardware devices, endpoint devices, and user accounts.

Both presented products offer unified management of the security of the ship's network, including almost all known methods and approaches to avoid and prevent cyber threats and attacks to the ship's Internet network, servers and endpoint devices. A secure connection with remote devices for the transmission of confidential ship data is available on both firewalls, the configuration is quick and easy, and with the introduction of traffic control rules, this connection can be disabled with one click when is not in use. In general, both products are preferred for the protection of shipboard IT systems, but Sophos offers an innovative solution through the cloud service "Sandbox". With this service, the identification of suspicious and executable files entering the network via email or websites are sent to the cloud-sandbox for extensive analysis and remote execution to detect zero-day threats before entering the ship's network. This does not affect the network traffic, but must be kept in mind, because in most cases the ship's Internet access is via satellite.

At this moment, only the software company Sophos offers synchronized protection by connecting endpoint devices to the firewall using Security Heartbeat technology. In this case, the XG Firewall monitors the Security Heartbeat status of all Sophos end-devices, allowing you to quickly identify compromised devices and automatically restrict network access of those devices until they are cleaned. This solution can be successfully applied to protect the ship's OT systems by installing Sophos Endpoint Protection software – Intercept X with EDR (End Point Detection and Response) on the end-devices.

Both implemented UTM solutions support remote management and monitoring via cloud applications. Sophos Central offers more options, but at the same time is more complex to work with it and requires support from IT professionals.

One of the important parameters for internet traffic is the bandwidth of the installed UTM devices. The maximum bandwidth of Kerio Control devices – Firewall/UTM throughput is 900/900 Mbps. Sophos XG devices offer higher bandwidth in accordance with the Internet standards, and the maximum bandwidth – Firewall/UTM throughput is respectively 100000/19200 Mbps.

Conclusions

This article addresses the need to increase the cybersecurity of ship information systems in accordance with the requirements of the World Maritime Organization

as after 01 January 2021 all ships must have a developed Cyber Risk Management plan as part of the Safety Management System.

A real practical installation was created to perform the required configuration and compatibility tests. This practical installation can be successfully used to train responsible staff on the ship's board for supporting and maintaining the ship's IT and OT systems. The conducted tests confirm that UTM devices can be successfully used to protect and manage small or medium-size computer networks.

The realized practical installation represents the real ship IT/OT network. It can be used to examine network settings onboard the ship before implementation.

The choice to implement a UTM solution is based on its simplicity and the fact that it contains several security functions integrated into one device (hardware or software). With the implementation of UTM solutions in the ship network, all security functions can be provided by one provider, maintained by one person and managed through one console.

The implementation of UTM solutions in the ship network significantly increases the cybersecurity of the ship's IT/OT systems through the use of all known methods and approaches for network protection.

Implementing at least two UTMs, as it is presented, improves the sustainability of the ship's network and removes the possibility for the occurrence of a single point of failure in Internet access.

Implementing at least two UTMs from different vendors minimizes their disadvantages and weaknesses which is a step for increasing the overall level of a system's cybersecurity.

Acknowledgments. The practical installation of UTM appliances presented in this article and shown on Figure 2 and Figure 3 is a result of the master degree thesis of Stoyno Stoynov. It was successfully used for familiarization and preparation by five yacht Chief Engineers responsible for IT systems onboard of mega yachts under the Sarnia Yachts and West Nautical management.

NOTES

1. MSC-FAL.1-Circ.3 – Guidelines on Maritime Cyber Risk Management. International Maritime Organization. Available online at: https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat).pdf. [Last accessed 13 May 2021].

   MSC 98/23/Add.1 Annex 10 – Resolution MSC.428(98) Maritime Cyber Risk Management in Safety Systems. International Maritime Organization. Available online at: https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/Resolution%20MSC.428(98).pdf. [Last accessed 13 May 2021].

2. Center for Strategic and International Studies (CSIS) – Significant Cyber Incidents Since 2006. Available online at: https://csis-website-prod.s3.amazonaws.com/s3fs-public/210430_Significant_Cyber_Events_List.pdf?B21zjJhsoO3qkgQNyGMmZN5IhAE80S_I. [Last accessed 14 May 2021].
3. Shipping 2030 – Collaboration in the Shipping Industry: Innovation and Technology, AN INDUSTRY REVIEW PAPER. Available online at: https://informaconnect.com/article/pdfs/91705d00-6d9d-4ba3-98a4-9b10c92ad520_Shipping2030_report_Feb16-2018_.pdf. [Last accessed 14 May 2021].
4. The Guidelines on Cyber Security Onboard Ships, Version 4. BIMCO Publications. Available online at: https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships. [Last accessed 14 May 2021].
5. Unified Threat Management (UTM) F.A.Q. QuoStar. 2020. Available online at: https://www.quostar.com/blog/unified-threat-management-faq/. [Last accessed 14 May 2021].
6. 750-8xxx(/xxx-xxx) PFC100/200 Cyber Security for Controller PFC100/PFC200. Available online at: https://www.wago.com/global/d/15739.[Last accessed 14 May 2021].

REFERENCES

Otto, L., 2020. Global *Challenges in Maritime Security: An Introduction*. Springer Nature. ISBN: 978-3-030-34630-0.

Boyes, H., Isbell, R., 2018. *Code of practice – Cyber Security for Ships.* The Institution of Engineering and Technology. ISBN: 978-1-78561-577-1.

✉ **Stoyno Stoynov**
Nikola Vaptsarov Naval Academy
Varna, Bulgaria
E-mail: stoynostoynov@abv.bg

✉ **Borislav Nikolov**
https://orcid.org/0000-0002-6055-8538
Nikola Vaptsarov Naval Academy
Varna, Bulgaria
E-mail: nikolov@naval-acad.bg