Research Article
Turkish Journal of Maritime and Marine Sciences

DOI: 10.52998/trjmms.1531150
Volume: 10 Special Issue: 1 (2024) 31-50

Maritime Cyber Security: Adopting a Checklist Based on IACS UR E26 Standard

IACS UR E26 Standardına Dayalı Gemi Siber Güvenlik Kontrol Listesinin Benimsenmesi

Türk Denizcilik ve Deniz Bilimleri Dergisi

Cilt: 10 Özel Sayı: 1 (2024) 31-50

Gizem KAYIŞOĞLU[1,*], Emre DÜZENLİ[1], Pelin BOLAT[1], Fırat BOLAT[1]
[1]*Istanbul Technical University, Maritime Faculty, 34940, İstanbul-Türkiye*

ABSTRACT

The efficient operation of ship systems that control navigation, communications, sensors, and power and machinery is dependent on the increasing digitization of the maritime sector and the intense use of information and operational technologies. The goal of issuing and enforcing global regulations and standards is to lessen the impact of potential dangers that could jeopardize on-board systems, network and data integrity, and operation, functionality and safety. At this point, "Cyber Resilience of Ships" (UR E26) is recently released by the International Association of Classification Societies (IACS) to address the need to improve ships' cyber resilience. This regulation will be applicable to new ships built on and after 1 July 2024. This study aims to create a check list for ship cyber security based on IACS UR E26 standard. A ship cyber security checklist was developed by first analyzing ship operational technologies, identifying potential cyber risks and vulnerabilities, and then creating a checklist in accordance with the IACS UR E26 standard to ensure cyber security on board. With a focus on clean seas and safe ships, the IACS provides technical assistance, verifies compliance, and conducts research and development to enhance maritime safety, security and regulation. This study provides practical tool to ships for ship cyber security management under the safety management system besides IACS standard benefits. Creating a checklist in accordance with the IACS UR E26 standard also allows ship owners and operators to comply with the standards and facilitate inspection processes. This reduces the effort spent to comply with international regulations. It helps to proactively manage cyber risks by providing a systematic approach to ship cyber security management.

Key Words: Maritime cyber security, Ship cyber security check list, Ship cyber resilience, IACS UR E26

Article Info
Received: 10 August 2024
Revised: 05 September 2024
Accepted: 08 September 2024

*(corresponding author)
E-mail: yukselg@itu.edu.tr

To cite this article: Kayışoğlu, G., Düzenli, E., Bolat, P., Bolat, F. (2024). Maritime Cyber Security: Adopting a Checklist Based on IACS UR E26 Standard, *Turkish Journal of Maritime and Marine Sciences*, 10 (Special Issue: 1): 31-50. doi: 10.52998/trjmms.1531150.

ÖZET

Seyir, iletişim, sensörler, güç ve makine kontrol sistemlerinden oluşan gemi sistemlerinin verimli bir şekilde çalışması, denizcilik sektörünün artan dijitalleşmesine ve bilgi ve operasyonel teknolojilerin yoğun kullanımına bağlıdır. Küresel düzenlemeler ve standartların amacı, gemideki sistemlere, ağ ve veri bütünlüğüne, operasyona, işlevselliğe ve güvenliğe zarar verebilecek potansiyel tehlikelerin etkisini azaltmaktır. Bu noktada, Uluslararası Klas Kuruluşları Birliği (IACS) tarafından gemilerin siber dayanıklılığını iyileştirme ihtiyacını ele almak için yakın zamanda "Gemilerin Siber Dayanıklılığı" (UR E26) yayınlandı. Bu düzenleme, 1 Temmuz 2024'ten itibaren inşa edilen yeni gemiler için geçerli olacaktır. Bu çalışma, IACS UR E26 standardına dayalı olarak gemi siber güvenliği için bir kontrol listesi oluşturmayı amaçlamaktadır. Gemi operasyonel teknolojilerinin analiz edilmesi, potansiyel siber risk ve güvenlik açıklarının belirlenmesi ve bu doğrultuda IACS UR E26 standardına uygun bir siber güvenlik kontrol listesi oluşturulması yoluyla bir gemi siber güvenlik kontrol listesi geliştirilmiştir.Temiz denizlere ve güvenli gemilere odaklanan IACS, teknik yardım sağlar, uyumluluğu doğrular ve deniz güvenliğini, emniyetini ve düzenlemesini geliştirmek için araştırma ve geliştirme yürütür. Bu çalışma, IACS standartının faydalarının yanı sıra emniyet yönetim sistemi kapsamında gemi siber güvenlik yönetimi için gemilere pratik bir araç sağlar. IACS UR E26 standardına uygun bir kontrol listesi oluşturmak, gemi sahiplerinin ve operatörlerinin standartlara uymasını ve denetim süreçlerini kolaylaştırmasını da sağlar. Bu, uluslararası düzenlemelere uymak için harcanan çabayı azaltır. Gemi siber güvenlik yönetimine sistematik bir yaklaşım sağlayarak siber riskleri proaktif bir şekilde yönetmeye yardımcı olur.

Anahtar Sözcükler: Denizel alanda siber güvenlik, Gemi siber güvenlik kontrol listesi, Gemi siber dayanıklılığı, IACS UR E26

1. INTRODUCTION

The maritime industry is undergoing a significant transformation driven by the rapid digitization of ship systems and the widespread adoption of information and operational technologies. These advancements have enabled more efficient control of critical systems such as navigation, communications, sensors, and power management, which are essential for the safe and effective operation of modern ships (Kanwal *et al*., 2024). However, this increased reliance on digital technologies has also introduced new vulnerabilities, particularly in the realm of cyber security.

As ships become more connected, the potential risks associated with cyber threats have escalated, posing significant dangers to on-board systems, network integrity, and overall operational safety (Palbar Misas *et al*., 2024). Cyber-attacks on ships can lead to severe consequences, including disruptions in communication, navigation failures, data breaches, and even physical damage to ship machinery (Silverajan and Vistiaho, 2019). Recognizing the critical need to address these emerging risks, the International Association of Classification Societies (IACS) has developed the Unified Requirements (UR) on the "Cyber Resilience of Ships" (UR E26) standard, which will come into effect for new ships contracted for construction on or after July 1, 2024 (IACS, 2024). The UR E26 standard represents a proactive approach to enhancing the cyber resilience of ships by providing a comprehensive framework for managing cyber risks throughout the ship's lifecycle. This includes guidelines for the design, construction, and operation of ships with a focus on protecting vital systems against cyber threats.

This study aims to contribute to the ongoing efforts to improve maritime cyber security by developing a practical checklist based on the IACS UR E26 standard. This checklist is designed to assist ship owners and operators in implementing effective cyber security measures as part of their safety management systems. By systematically addressing potential vulnerabilities, the checklist not only facilitates compliance with international regulations but also helps to ensure the continuous and safe operation of ship systems, thereby minimizing the risk of operational disruptions and unexpected failures.

The importance of cyber resilience in the maritime sector cannot be overstated. As digital technologies continue to evolve, the ability to safeguard ship systems against cyber threats will be crucial in maintaining the safety, security, and efficiency of global maritime operations. This paper seeks to provide a practical tool for achieving these goals, reinforcing the essential role of cyber security in the modern maritime landscape.

2. LITERATURE REVIEW

Maritime cyber security has gained increasing attention due to the growing interconnectedness of ships and maritime infrastructure. Research in this field has focused on developing risk assessment techniques and intrusion detection tools (Bolbot *et al*., 2022). The integration of navigational systems on ships, while enhancing safety, also introduces cyber vulnerabilities that require regular maintenance and security testing (Svilicic *et al*., 2019). To address these challenges, academic institutions are developing specialized curricula and research centers dedicated to maritime cyber security (Zăgan *et al*., 2018).

Maritime cyber security guidelines are crucial due to increasing technological dependence and cyber threats in the shipping industry. The International Maritime Organization (IMO) has developed guidelines for cyber risk management, emphasizing the need to address cyber risks in Safety Management Systems by 2021 (IMO, 2022). These guidelines focus on key shipboard Operational Technology systems, including communication, propulsion, navigation, and cargo management (Rajaram *et al*., 2022). They provide risk assessment methods, mitigation measures, and checklists to enhance vessel cyber hygiene (Rajaram *et al*., 2022; Rana, 2019). The guidelines also address the vulnerabilities of Internet of Things (IoT) devices and modern security frameworks used in ships (Ashraf *et al*., 2022). Implementation of these guidelines is crucial for safeguarding against cyber incidents such as GPS interference and malware attacks. National authorities, like the British government, have adopted these guidelines to develop country-specific cyber security practices for ships (Rana, 2019).

In the literature, various studies have demonstrated the cyber vulnerabilities of bridge navigation systems such as GNSS (Santamarta, 2014; Hyra, 2019), VDR (Hyra, 2019; Soner *et al*., 2023a), ECDIS (Hyra, 2019; Jo *et al*., 2022; Kayisoglu *et al*., 2022), and AIS (Hyra, 2019; Tran *et al*., 2021; Soner *et al*., 2023b). Moreover, Kayisoglu *et al*. (2023) examined the CORAS framework to ensure cyber hygiene in shipboard radar systems.

Besides above-mentioned guidelines and researches, iTrust, (2022) lists existing guidelines for maritime cyber security. These are American Bureau of Shipping (ABS) – "The Guide for Cybersecurity Implementation for the Marine and Offshore Industries", Baltic and International Maritime Council (BIMCO) – "Guidelines on Cyber Security Onboard Ships", Det Norske Veritas (DNV) – "Class guideline-Cyber Secure", Det Norske Veritas (DNV) – "Cyber Security Resilience Management for Ships and Mobile Offshore Units in Operation", and Institution of Engineering and Technology (IET) – "Code of Practice Cyber Security for Ships". All these guidelines with the IACS UR E26 provide comprehensive framework to implement cyber security onboard ships. However, this study differs from both existing academic research and guidelines in terms of mapping the cyber security measures for the shipboard operational technologies.

3. METHODOLOGY

In this study, it is aimed to create a ship cyber security check list by using IACS UR E26 standard. For this purpose, firstly, ship operational technologies (OT) are examined and their configuration systems in terms of their technological infrastructure, data communication, transferring and processing, and usage function are understood as the context and asset identification by utilizing several maritime cyber security guidelines, ship equipment manufacturer catalog and operational guides, and literature. Then the vulnerabilities of the ship systems and the cyber risks that can occur after the vulnerabilities can be exploited by the malicious people are defined.

The analytical methodologies used in our work include a thorough examination of ship operating technology. First, the current setups and technical infrastructures of ship systems were assessed using a range of marine cyber security standards and literature. The accuracy of the instruments used in this procedure has been verified by comparing them with industry-recognized criteria and standards and verifying them against available literature.

The reliability of the study was guaranteed by using widely utilized protocols in such analyses that have been shown successful in prior research. The verification of the identified cyber hazards and vulnerabilities was conducted by a comparison with documented incidents and guideline papers found in the literature. Furthermore, in order to guarantee the coherence of the results, further studies explored various situations and possibilities throughout the course of the research. Finally, the cyber security checklist for ships is created to ensure cyber mitigation onboard ships by presenting the ships compatibility with IACS UR E26. In this context, the flow diagram for the methodology is as in Figure 1.

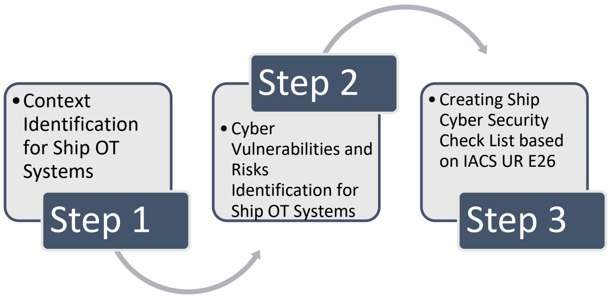

• Context Identification for Ship OT Systems
Step 1
Step 2
• Cyber Vulnerabilities and Risks Identification for Ship OT Systems
• Creating Ship Cyber Security Check List based on IACS UR E26
Step 3

Figure 1. Flow diagram

3.1. IACS UR E26 – Cyber Resilience of Ships

In order to give stakeholders with the technological means to create cyber resilient ships, International Association of Classification Societies (IACS) Unified Requirements (UR) on the "Cyber Resilience of Ships" (UR E26) aims to establish a minimal set of specifications for cyber resilience of ships (IACS UR E26, 2022). The ship as a whole is the focus of IACS UR E26, which aims to provide a foundation for future URs and industry standards that tackle cyber resilience in systems, equipment, and components. It is stated in IACS UR E27 "Cyber Resilience of On-Board Systems and Equipment" that the on-board systems and equipment must meet minimum standards for cyber resilience.

The standard includes mandatory and non-mandatory parts for new ships contracted for construction on or after July 1, 2024. One of these ship types that standard is applicable on as mandatory is cargo ships of 500 gross tonnage (GT) and upwards engaged in international voyages. IACS UR E26 aims to maintain robust cyber security for ships by ensuring secure system design, secure remote connections, and secure manufacturing infrastructure. It is the best practices of ISO 27001 and NIST cyber security framework on the ships.

IACS UR E26 applies to OT systems onboard ships, i.e. those Computer Based Systems (CBSs) using data to control or monitor physical processes that can be vulnerable to cyber incidents and, if compromised, could lead to dangerous situations for human safety, safety of the vessel and/or threat to the environment. In particular, the CBSs used for the operation of the following ship functions and systems are considered communication, navigation, electrical, engine room, cargo control, mooring, ballast systems and any Internet Protocol (IP)-based communication interface from CBSs including crew welfare systems, administrative systems, passenger networks as showed in Figure 2 (Witherby *et al*., 2023).

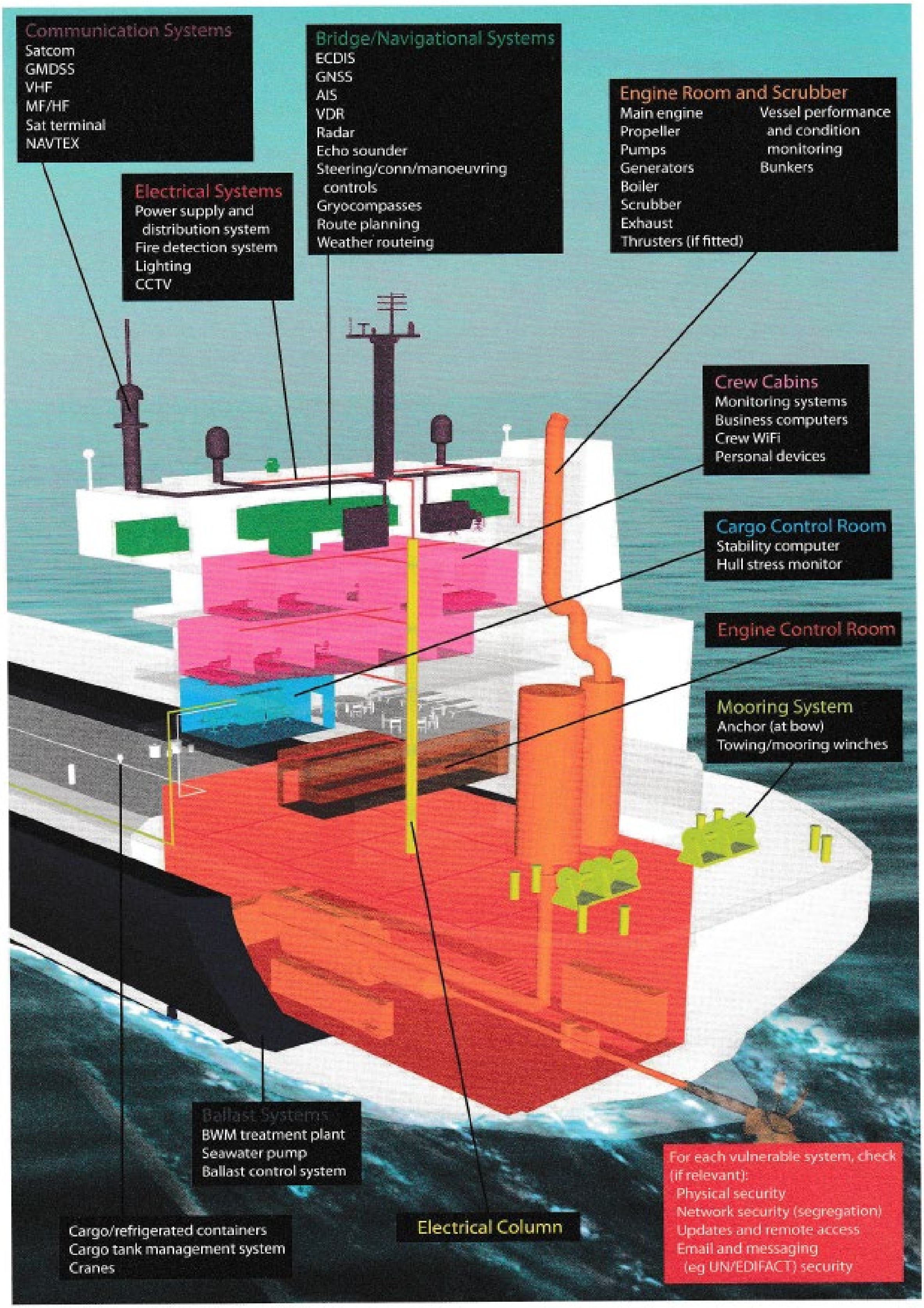


Figure 2. Ship OT systems and their cyber security implications (Witherby *et al*., 2023)

Ship CBSs security capabilities and documentation are designed and set on the ship according to IACS UR E27. System integrators as the stakeholder submit the design documents to the Class society for verification and approval of compliance with requirements in the UR E26. System integrators and shipowner maintain construction, commissioning and operation respectively by keeping the documents updated in accordance with procedure for management of change (MoC). Accordingly, it is concluded that IACS URs integrate each other and the stakeholders including shipyards, system integrator, shipowner, and Class societies work systematically and make cooperation between them according to IACS requirements. This work process and stakeholders' role are shown in Figure 3 (DNV-GL, 2022).

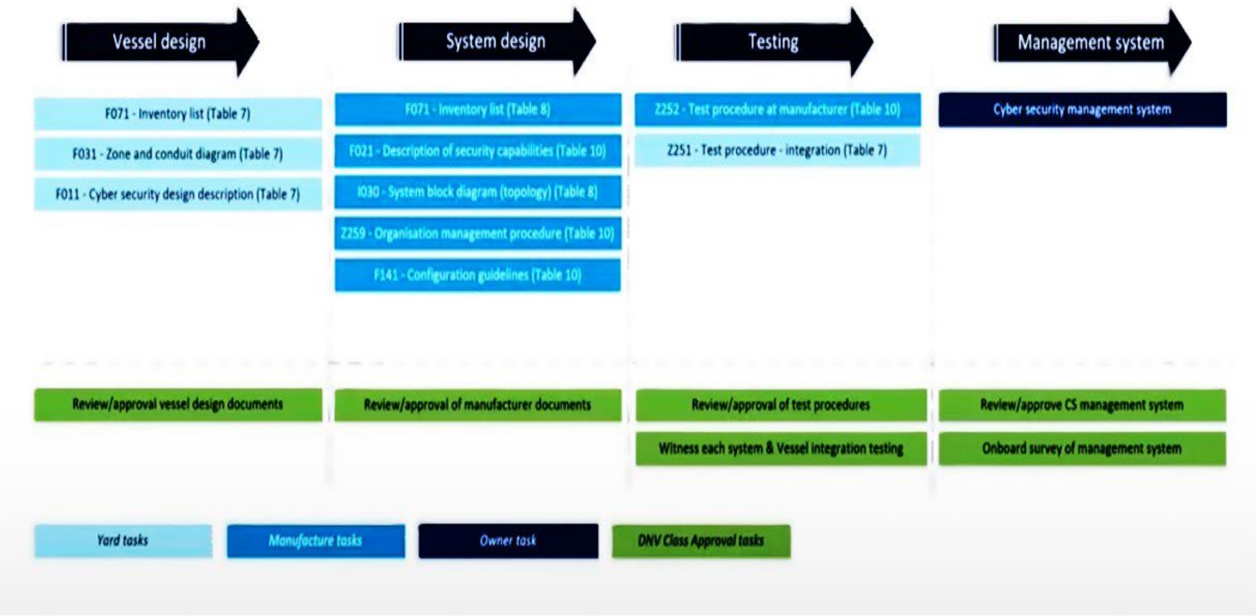
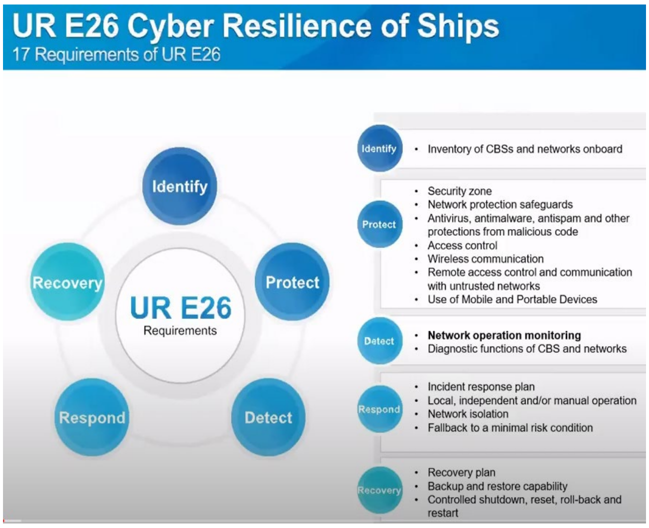

Vessel design
System design
Testing
Management system
F071 - Inventory list (Table 7)
F031 - Zone and conduit diagram (Table 7)
F011 - Cyber security design description (Table 7)
F071 - Inventory list (Table 8)
F021 - Description of security capabilities (Table 10)
I030 - System block diagram (topology) (Table 8)
Z259 - Organisation management procedure (Table 10)
F141 - Configuration guidelines (Table 10)
Z252 - Test procedure at manufacturer (Table 10)
Z251 - Test procedure - integration (Table 7)
Cyber security management system
Review/approval vessel design documents
Review/approval of manufacturer documents
Review/approval of test procedures
Witness each system & Vessel integration testing
Review/approve CS management system
Onboard survey of management system
Yard tasks
Manufacture tasks
Owner task
DNV Class Approval tasks

Figure 3. IACS UR E26 work process

IACS UR E26 involves seventeen requirements under the NIST cyber security framework that includes Identify, Protect, Detect, Respond, and Recovery. The other main part of the standard is demonstration of compliance during design and construction phases, upon ship commissioning, and during the operational life of the ship. Its supplementary part is related to risk assessment for exclusion of CBS from the application of requirements. It also includes security level categorizations from category I to category III, which are suitable with the IACS UR E22 "Computer-based Systems". IACS UR E22 requirements apply to design, construction, commissioning and maintenance of computer-based systems where they depend on software for the proper achievement of their functions. These requirements apply to systems which provide control, alarm, monitoring, safety, or internal vessel communication functions that are subject to classification requirements. Examples of such systems are navigation systems and radio communication system required by SOLAS chapter V and IV, and vessel loading instrument/stability computer (IACS UR E22, 2023). Accordingly, IACS UR E26 integrates with the IACS UR E27 and IACS UR E22.

The requirements of IACS UR E26 are shown in Figure 4 (DNV-GL, 2022). It is firstly required to identify inventory list of CBSs and networks onboard ships. Then, main security measures with protection function are required to be set onboard ships. These requirements cover security zone, network protection safeguards, antivirus, antimalware, and other protections from malicious code, access control, wireless communication, remote access control and communication with untrusted networks and use of mobile and portable devices. The Identify and Protection functions of the standard are almost already implemented onboard ships on service as required International Safety Management (ISM) Code. The International Maritime Organization (IMO) safety code has included a cyber chapter with specific compliance terms including mandatory obligation: MSC-FAL.1/Circ.3 Guidelines on maritime cyber risk management. According to the regulation, all vessels are required to implement the necessary cyber security measures no later than 2021 (IMO, 2022) However, the distinctive aspect of IACS UR E26 rather than exist measures under ISM Code starts with the Detect function of the standard. For setting detect function that means cyber-attack detection function on board ships, standard is required network operation monitoring. This is the most significant part for the new constructed ships to ensure cyber security. In Figure 5, an example of network monitoring system is shown (DNV-GL, 2022). The main principle of it is that secure zones for the each OT systems networks of ships are set. Layer 2 switches collect the data packets on each network via network packet collectors. These packets are transferred to Layer3 switch that is called as ship network security device. Internal network data is secured through internal and external firewalls. Ship network security device in the demilitarized zone (DMZ) is equipped with a security management system. By this way, the collected network data is analyzed real time by the cyber security analysts and any anomalies on the systems can be detected by experts and additional security systems such as intrusion detection and prevention systems (IDS/IPS). Additional security functions of the IACS UR E26 are cyber incident response and recovery plans.



UR E26 Cyber Resilience of Ships

17 Requirements of UR E26

Identify
- Inventory of CBSs and networks onboard

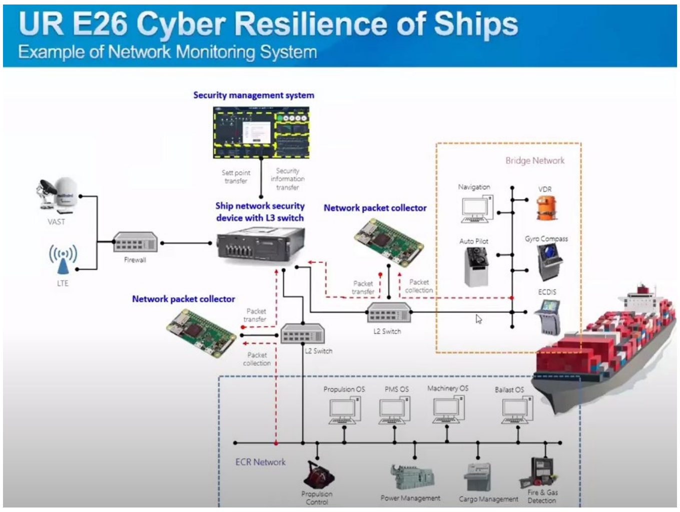
Protect
- Security zone
- Network protection safeguards
- Antivirus, antimalware, antispam and other protections from malicious code
- Access control
- Wireless communication
- Remote access control and communication with untrusted networks
- Use of Mobile and Portable Devices

Detect
- **Network operation monitoring**
- Diagnostic functions of CBS and networks

Respond
- Incident response plan
- Local, independent and/or manual operation
- Network isolation
- Fallback to a minimal risk condition

Recovery
- Recovery plan
- Backup and restore capability
- Controlled shutdown, reset, roll-back and restart

Figure 4. Requirements of IACS UR E26 (DNV-GL, 2022).



UR E26 Cyber Resilience of Ships

Example of Network Monitoring System

Figure 5. Example for network monitoring system

Cyber security requirements for ships according to IACS UR E26 are as in Table 1

Table 1. IACS UR E26 requirements (IACS UR E26, 2022)

Requirement Code	Requirement Name	Section in the Standard	Requirement Definition
R1	Vessel Asset Inventory	4.1.1	An inventory of hardware and software (including application programs, operating systems, if any, firmware and other software components) of the CBSs in the scope of applicability of this UR and of the networks connecting such systems to each other and to other CBSs onboard or ashore shall be provided and kept up to date during the entire life of the ship.
R2	Security Zones and Network Segmentation	4.2.1	All CBSs in the scope of applicability of this UR shall be grouped into security zones with well-defined security policies and security capabilities. Security zones shall either be isolated (i.e. air gapped) or connected to other security zones or networks by means providing control of data communicated between the zones (e.g. firewalls/routers, simplex serial links, TCP/IP diodes, dry contacts, etc.). Only explicitly allowed traffic shall traverse a security zone boundary
R3	Network protection safeguards	4.2.2	Security zones shall be protected by firewalls or equivalent means as specified in section 4.2.1. The networks shall also be protected against the occurrence of excessive data flow rate and other events which could impair the quality of service of network resources. The CBSs in scope of this UR shall be implemented in accordance with the principle of Least Functionality, i.e. configured to provide only essential capabilities and to prohibit or restrict the use of non-essential functions, where unnecessary functions, ports, protocols and services are disabled or otherwise prohibited.
R4	Antivirus, antimalware, antispam and other protections from malicious code	4.2.3	CBSs in the scope of applicability of this UR shall be protected against malicious code such as viruses, worms, trojan horses, spyware, etc.
R5	Access control	4.2.4	CBSs and networks in the scope of applicability of this UR shall provide physical and/or logical/digital measures to selectively limit the ability and means to communicate with or otherwise interact with the system itself, to use system resources to handle information, to gain knowledge of the information the system contains or to control system components and functions. Such measures shall be such as not to hamper the ability of authorized personnel to access CBS for their level of access according to the least privilege principle.
R5.1	Physical access control	4.2.4.3.1	CBSs of Cat.II and Cat.III shall generally be located in rooms that can normally be locked or in controlled space to prevent unauthorized access, or shall be installed in lockable cabinets or consoles. Such locations or lockable cabinets/consoles shall be however easy to access to the crew and various stakeholders who need to access to CBSs for installation, integration, operation, maintenance, repair, replacement, disposal etc. so as not to hamper effective and efficient operation of the ship.
R5.2	Physical access control for visitors	4.2.4.3.2	Visitors such as authorities, technicians, agents, port and terminal officials, and shipowner representatives shall be restricted regarding access to CBSs onboard whilst on board, e.g. by allowing access under supervision.
R5.3	Physical access control of network access points	4.2.4.3.3	Access points to onboard networks connecting Cat.II and/or Cat.III CBSs shall be physically and/or logically blocked except when connection occurs under supervision or according to documented procedures, e.g. for maintenance. Independent computers isolated from all onboard networks, or other networks, such as dedicated guest access networks, or networks dedicated to passenger recreational activities, shall be used in case of occasional connection requested by a visitor (e.g. for printing documents).

Table 1 (continued). IACS UR E26 requirements (IACS UR E26, 2022)

Requirement Code	Requirement Name	Section in the Standard	Requirement Definition
R5.4	Removable media controls	4.2.4.3.4	A policy for the use of removable media devices shall be established, with procedures to check removable media for malware and/or validate legitimate software by digital signatures and watermarks and scan prior to permitting the uploading of files onto a ship's system or downloading data from the ship's system.
R5.5	Management of credentials	4.2.4.3.5	CBSs and relevant information shall be protected with file system, network, application, or database specific Access Control Lists (ACL). Accounts for onboard and onshore personnel shall be left active only for a limited period according to the role and responsibility of the account holder and shall be removed when no longer needed. is not necessary to "uniquely" identify and authenticate all human users. CBSs which require strong access control may need to be secured using a strong encryption key or multi-factor authentication. Administrator privileges shall be managed in accordance with the policy for access control, allowing only authorized and appropriately trained personnel full access to the CBS, who as part of their role in the company or onboard need to log on to systems using these privileges
R5.6	Least privilege principle	4.2.4.3.6	Any human user allowed to access CBS and networks in the scope of applicability of this UR shall have only the bare minimum privileges necessary to perform its function. The default configuration for all new account privileges shall be set as low as possible. Wherever possible, raised privileges shall be restricted only to moments when they are needed, e.g. using only expiring privileges and one-time-use credentials. Accumulation of privileges over time shall be avoided, e.g. by regular auditing of user accounts.
R.6	Wireless communication	4.2.5	Wireless communication networks in the scope of this UR shall be designed, implemented and maintained to ensure that: - Cyber incidents will not propagate to other control systems - Only authorised human users will gain access to the wireless network - Only authorised processes and devices will be allowed to communicate on the wireless network - Information in transit on the wireless network cannot be manipulated or disclosed
R7	Remote access control and communication with untrusted networks	4.2.6	User's manual shall be delivered for control of remote access to onboard IT and OT systems. Clear guidelines shall identify roles and permissions with functions. For CBSs in the scope of applicability of this UR, no IP address shall be exposed to untrusted networks. Communication with or via untrusted networks requires secure connections (e.g. tunnels) with endpoint authentication, protection of integrity and authentication and encryption at network or transport layer. Confidentiality shall be ensured for information that is subject to read authorization.
R8	Use of Mobile and Portable Devices	4.2.7	The use of mobile and portable devices in CBSs in the scope of applicability of this UR shall be limited to only necessary activities and be controlled in accordance with UR E27 section 4.1 item 10. For any CBS that cannot fully meet these requirements, the interface ports shall be physically blocked. Mobile and portable devices shall only be used by authorised personnel. Only authorised devices may be connected to the CBSs. All use of such devices shall be in accordance with the shipowner's policy for use of mobile and portable devices, taking into account the risk of introducing malware in the CBS.

Table 1 (continued). IACS UR E26 requirements (IACS UR E26, 2022)

Requirement Code	Requirement Name	Section in the Standard	Requirement Definition
R9	Network operation monitoring	4.3.1	Networks in scope of this UR shall be continuously monitored, and alarms shall be generated if malfunctions or reduced/degraded capacity occurs. Measures to monitor networks in the scope of applicability of this UR shall have the following capabilities: (i) Monitoring and protection against excessive traffic, (ii) Monitoring of network connections, (iii) Monitoring and recording of device management activities, (iv) Protection against connection of unauthorized devices, (v) Generate alarm if utilization of the network's bandwidth exceeds a threshold specified as abnormal by the supplier. See UR E22 section 7.2.1. Intrusion detection systems (IDS) may be implemented, subject to the following: (i) The IDS shall be qualified by the supplier of the respective CBS, (ii) The IDS shall be passive and not activate protection functions that may affect the performance of the CBS, (iii) Relevant personnel should be trained and qualified for using the IDS
R10	Verification and diagnostic functions of CBS and networks	4.3.2	CBSs and networks in the scope of applicability of this UR shall be capable to check performance and functionality of security functions required by this UR. Diagnostic functions shall provide adequate information on CBSs integrity and status for the use of the intended user and means for maintaining their functionality for a safe operation of the ship.
R11	Incident response plan	4.4.1	An incident response plan shall be developed by the shipowner covering relevant contingencies and specifying how to react to cyber security incidents. The Incident response plan shall contain documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of incidents against CBSs in the scope of applicability of this UR. The Incident response plan shall provide procedures to respond to detected cyber incidents on networks by notifying the proper authority, reporting needed evidence of the incidents and taking timely corrective actions, to limit the cyber incident impact to the network segment of origin. The incident response plan shall, as a minimum, include the following information: (i) Breakpoints for the isolation of compromised systems, (ii) A description of alarms and indicators signalling detected ongoing cyber events or abnormal symptoms caused by cyber events, (iii) A description of expected major consequences related to cyber incidents, (iv) Response options, prioritizing those which do not rely on either shut down or transfer to independent or local control, if any, (v) Independent and local control information for operating independently from the system that failed due to the cyber incident, as applicable. The Incident response plan shall be kept in hard copy in the event of complete loss of electronic devices enabling access to it.
R12	Local, independent and/or manual operation	4.4.2	Any CBS needed for local backup control as required by SOLAS II-1 Regulation 31 shall be independent of the primary control system. This includes also necessary Human Machine Interface (HMI) for effective local operation. The CBS for local control and monitoring shall be self-contained and not depend on communication with other CBS for its intended operation. If communication to the remote control system or other CBS's is arranged by networks, segmentation and protection safeguards as described in 4.2.1 and 4.2.2 shall be implemented. This implies that the local control and monitoring system shall be considered a separate security zone.

Table 1 (continued). IACS UR E26 requirements (IACS UR E26, 2022)

Requirement Code	Requirement Name	Section in the Standard	Requirement Definition
R13	Network isolation	4.4.3	It shall be possible to terminate network-based communication to or from a security zone. Where the Incident Response Plan indicates network isolation as an action to be done, it shall be possible to isolate security zones according to the indicated procedure, e.g. by operating a physical ON/OFF switch on the network device or similar actions such as disconnecting a cable to the router/firewall. There shall be available instructions and clear marking on the device that allows the personnel to isolate the network in an efficient manner. Individual system's data dependencies that may affect function and correct operation, including safety, shall be identified, clearly showing where systems must have compensations for data or functional inputs if isolated during a contingency.
R14	Fallback to a minimal risk condition	4.4.4	As soon as a cyber incident affecting the CBS or network is detected, compromising the system's ability to provide the intended service as required, the system shall fall back to a condition in which a reasonably safe state can be achieved. Fall-back actions may include: (i) bringing the system to a complete stop or other safe state; (ii) disengaging the system; (iii) transferring control to another system or human operator; (iv) other compensating actions. Fall-back to minimum risk conditions shall occur in a time frame adequate to keep the ship in a safe condition. The ability of a system to fall back to a minimal risk condition shall be considered from the design phase by the supplier and the systems integrato
R15	Recovery plan	4.5.1	A recovery plan shall be made by the shipowner to support restoring CBSs under the scope of applicability of this UR to an operational state after a disruption or failure caused by a cyber incident. Details of where assistance is available and by whom shall be part of the recovery plan.
R16	Backup and restore capability	4.5.2	CBSs and networks in the scope of applicability of this UR shall have the capability to support back-up and restore in a timely, complete and safe manner. Backups shall be regularly maintained and tested.

Note: Pink: Identify Function in the NIST; Blue: Protection Function in the NIST; Yellow: Detect Function in the NIST; Grey: Response Function in the NIST; Green: Recovery Function in the NIST

3.2. Ship OT Systems and Cyber Risks

Ship OT systems are shown in Figure 2. The cyber risks are examined for each ship OT systems as in Table 2 by utilizing "Guidelines for Cyber Risk Management in Shipboard Operational Technology Systems" published by iTrust, (2022). The Table 2 highlights the broad spectrum of cyber risks that can impact the various OT systems on ships, ranging from communication and navigation to propulsion and cargo management. The potential impact of these risks includes disruption of operations, unauthorized access to sensitive information, and even physical safety hazards. Therefore, addressing these risks through robust cyber security measures is essential to maintaining the integrity and safety of maritime operations. Accordingly, phishing emails involve deceptive emails designed to trick users into revealing sensitive information or downloading malicious software. In the context of SATCOM and ICS, phishing attacks could compromise the security of communication channels, potentially leading to unauthorized access to critical information (Kesseler, 2019). Vulnerabilities in outdated software can be exploited by attackers to gain control over communication systems, leading to disruptions or unauthorized access (DNV-GL, 2016). Eavesdropping refers to unauthorized interception of communications. For SATCOM, ICS, and VOIP it could lead to the exposure of sensitive information, endangering the vessel's operations (Kavallieratos *et al.*, 2019). Unauthorized access of vessel network involves an attacker gaining unauthorized entry into the vessel's network, potentially leading to a full-scale compromise of the ship's communication infrastructure (Tucci, 2017). a DoS attack, which aims at overwhelming the system to disrupt normal operations, incapacitate the WLAN, disrupting network services on the ship, and hampering operational efficiency (Reilly and Jorgensen, 2016). Man-in-the-middle (MITM) attack involves intercepting and potentially altering communications between two systems. In the context of these critical systems, a MITM attack could lead to severe operational disruptions or safety hazards (Kayisoglu *et al.*, 2023). Malicious software could be used to disrupt, damage, or gain unauthorized access to these systems, potentially leading to catastrophic failures in propulsion or power management. Malware attack, DoS attack, and Spoofing could severely disrupt navigation by either corrupting data, overwhelming the system, or providing false navigational information, potentially leading to navigational errors (Martínez *et al.*, 2024). Ransomware and malware attack could result in the encryption of critical data or disruption of the cargo management processes, leading to operational delays or financial losses (Tam and Jones, 2019).

Table 2. Ship OT systems and cyber risks (iTrust, 2022)

Ship OT Systems	Ship OT Sub-Systems	Cyber Risks
Communication Systems	Satellite Communication System (SATCOM) and Integrated Communication System (ICS)	○ Phishing emails ○ Outdated VSAT software ○ Eavesdropping ○ Cross-site scripting attack ○ Unauthorized access of vessel network
	Voice Over Internet Protocol (VOIP)	○ Denial of Service (DoS) attack ○ Eavesdropping ○ Vishing
	Wireless Local Area Network (WLAN)	○ DoS attack ○ Access point tampering ○ Eavesdropping
Propulsion, Machinery and Power Control Systems	Engine System	○ Man-in-the-middle (MITM) attack ○ Malware attack
	Fuel Oil System	○ MITM attack ○ Malware attack
	Alarm Monitoring and Control System	○ MITM attack ○ Malware attack
	Power Management System (PMS)	○ MITM attack ○ Malware attack
Navigation Systems	Electronic Chart Display and Information System (ECDIS)	○ Malware attack ○ DoS attack ○ Spoofing
	Radio Detection and Ranging (RADAR)	○ Malware intrusion ○ MITM attack
	Automatic Identification System (AIS)	○ Spoofing ○ Replay attack ○ Frequency hopping attack
	Global Positioning System (GPS)	○ GPS spoofing ○ GPS jamming
	Global Maritime Distress Safety System (GMDSS)	○ Spoofing ○ Eavesdropping ○ DoS attack
	Voyage Data Recorder (VDR)	○ Malware attack ○ Remote code execution
	Integrated Navigation System (INS)	○ MITM attack ○ Remote code execution
Cargo Management Systems	Cargo Control Room (CCR)	○ Ransomware ○ Malware attack
	Ballast Water System (BWS)	○ Malware attack ○ Phishing emails

3.3. Ship Cyber Security Check List

Based on IACS UR E26, this study aims to create a checklist for ship cyber security. For this purpose, ship OT systems and their cyber risks are examined as Table 2. Then, the attack method for each cyber risks and their mitigations are investigated. Accordingly, IACS requirements are transformed to security control items and matched with applicable ship OT system as in Table 3.

Table 3. Ship cyber security checklist

Requirement Code	**Requirement Name**	**SATCOM and ICS**	**VOIP**	**WLAN**	**Engine System**	**Fuel Oil System**	**Alarm Monitoring and Control System**	**Power Management System (PMS)**	**ECDIS**	**RADAR**	**AIS**	**GPS**	**GMDSS**	**VDR**	**INS**	**CCR**	**BWS**
R1	Vessel Asset Inventory	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
R2	Security Zones and Network Segmentation		✓				✓				✓						✓
R3	Network protection safeguards		✓				✓				✓						✓
R4	Antivirus, antimalware, antispam and other protections from malicious code	✓				✓	✓	✓	✓						✓	✓	
R5	Access control	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
R5.1	Physical access control	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
R5.2	Physical access control for visitors	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
R5.3	Physical access control of network access points	✓			✓	✓	✓	✓			✓						✓
R5.4	Removable media controls	✓				✓	✓		✓	✓	✓			✓	✓	✓	
R5.5	Management of credentials	✓			✓	✓	✓										
R5.6	Least privilege principle	✓			✓	✓	✓										
R.6	Wireless communication			✓													

Table 3 (continued). Ship cyber security checklist

Requirement Code	Requirement Name	SATCOM and ICS	VOIP	WLAN	Engine System	Fuel Oil System	Alarm Monitoring and Control System	Power Management System (PMS)	ECDIS	RADAR	AIS	GPS	GMDSS	VDR	INS	CCR	BWS
R7	Remote access control and communication with untrusted networks	✓			✓	✓	✓		✓					✓		✓	✓
R8	Use of Mobile and Portable Devices	✓				✓	✓		✓	✓	✓			✓	✓	✓	
R9	Network operation monitoring		✓				✓					✓					✓
R10	Verification and diagnostic functions of CBS and networks		✓				✓					✓					✓
R11	Incident response plan	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
R12	Local, independent and/or manual operation	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
R13	Network isolation		✓				✓					✓					✓
R14	Fallback to a minimal risk condition	✓			✓	✓				✓	✓	✓					
R15	Recovery plan				✓	✓				✓	✓	✓					
R16	Backup and restore capability						✓	✓						✓			

4. FINDINGS AND DISCUSSION

This study provides a practical tool for ship cyber security. The obtained checklist can be used as a map for application of the IACS UR E26 onboard ships. According to the Table 3, Vessel Inventory List should be implemented for the whole computer based shipboard operational systems. The vessel asset inventory includes information about the system in the ship's network (system category, security zone where the system is installed), the location and connections of the systems, and the systems' hardware and software. For network devices (switches, firewalls, routers, etc.) and security devices (IDS, Security Information and Event Management (SIEM), etc.) IACS UR E26 is required to be additionally installed by the systems integrator and the inventory information should be filled by them. Security Zones and network segmentation illustrate how systems are grouped when constructing the network on the ship, and how communication between different groups is controlled, providing both physical and logical information. For instance, In the Table 3, SATCOM and ICS, VOIP, and WLAN can be grouped in one network segregation and called as Communication Systems in the security zone. Network protection covers a multitude of technologies, rules and configurations designed to protect the integrity, confidentiality and availability of networks. The threat environment is always changing, and attackers are always trying to find and exploit vulnerabilities. There are many layers to consider when addressing network protection. Attacks can happen at any layer in the network layers model, so network hardware, software and policies must be designed to address each area. While physical and technical security controls are designed to prevent unauthorized personnel from gaining physical access to network components and protect data stored on or in transit across the network, procedural security controls consist of security policies and processes that control user behaviour. The design of network shall include means to meet the intended data flow through the network and minimize the risk of denial of service (DoS) and network storm/high rate of traffic. Estimation of data flow rate shall at least consider the capacity of network, data speed requirement for intended application and data format. Therefore, network safeguard protection should be applied on the systems in each network segregation. In this context, firewall is configured to allow only whitelisted sources or IP addresses within a subnet. Virtual Private Network is used while accessing the Internet. IP address is private, and it is not available on any public domain such as in Shodan. Malware protection should be implemented on CBSs onboard ships. On CBSs having an operating system for which industrial-standard anti-virus and anti-malware software is available and maintained up-to-date, anti-virus and/or anti-malware software should be installed, maintained and regularly updated, unless the installation of such software impairs the ability of CBS to provide the functionality and level of service required. On CBSs where anti-virus and anti-malware software cannot be installed, malware protection shall be implemented in the form of operational procedures and physical safeguards. As the CBSs, antivirus software should be installed in the engine and fuel monitoring system, alarm monitoring & control system and power management system. Besides, OS, antivirus, firewall and other applications used in the business computer (The computer used for accessing emails, and VSAT modem's web interface) is updated/patched regularly. Access to CBSs and networks onboard ships and all information stored on such systems should only be allowed to authorized personnel, based on their need to access the information as a part of their responsibilities or their intended functionality. CBSs of Cat.II and Cat.III shall generally be located in rooms that can normally be locked or in controlled space to prevent unauthorized access or shall be installed in lockable cabinets or consoles. Such locations or lockable cabinets/consoles shall be however easy to access to the crew and various stakeholders who need to access to CBSs for installation, integration, operation, maintenance, repair, replacement, disposal etc. so as not to hamper effective and efficient operation of the ship. Visitors such as authorities, technicians, agents, port and terminal officials, and shipowner representatives shall be restricted regarding access to CBSs onboard whilst on board, e.g. by allowing access under supervision. Access points to onboard networks connecting Cat.II and/or Cat.III CBSs should be physically and/or logically blocked except when connection occurs under supervision or according to documented procedures, e.g. for maintenance. Accordingly, for all systems onboard ships access control requirements should be considered. A policy for the use of removable media devices should be established, with procedures to check removable media for malware and/or validate legitimate software by digital signatures and watermarks and scan prior to permitting the uploading of files onto a ship's system or downloading data from the ship's system. In this context, these requirements should be implemented on the systems having ports for the portable devices such as Alarm Monitoring and Control System, Power Management System, ECDIS, VDR, and cargo control systems. Multi-factor authentication (MFA) should set up for accessing the business computer and VSAT web interface. The admin login credentials in engine and fuel monitoring system, alarm monitoring and control system and power management systems should have strong password. On the GMDSS, messages exchanged between ships and port authorities should be authenticated (e.g., PKI schema). Any human user allowed to access CBS and networks in the scope of applicability of this UR shall have only the bare minimum privileges necessary to perform its function. This is called as zero-trust system. A secure encryption standard should be used in wireless networks. USB port blockers should be used to block unused ports in the engine and fuel monitoring system, alarm monitoring and control system and power management system, as well as other systems including ports. USB cleaning station (a separate PC with antivirus software to scan the USB drives before use) should be setup onboard ships. Finally, the incident response plan should provide procedures to respond to detected cyber incidents on networks by notifying the proper authority, reporting needed evidence of the incidents and taking timely corrective actions, to limit the cyber incident impact to the network segment of origin. The incident response plan shall, as a minimum, include the information about (i) breakpoints for the isolation of compromised systems, (ii) a description of alarms and indicators signalling detected ongoing cyber events or abnormal symptoms caused by cyber events, (iii) a description of expected major consequences related to cyber incidents. The incident response plan should be kept in hard copy in the event of complete loss of electronic devices enabling access to it. Incident response plan should be prepared for all systems onboard ships, but recovery plan should be firstly considered for recover operational life of the ship. Therefore, it should be considered system recovery, which are the specified methods and procedures to recover communication capabilities in terms of Recovery Time Objective (RTO), and data recovery, which are the specified methods and procedures to recover data necessary to restore safe state of OT systems and safe ship operation in terms of Recovery Point Objective (RPO). Consequently, the check list is created by considering stages on the design of the ship, setting systems on the ships, and operating ship systems. Hence, the stakeholders, such as shipyards, system integrators, ship owners, and class societies cooperate each other for ensuring cyber security onboard ships. The IACS UR E26 provides not only design of the systems and integration of them into the ship but also maintaining them onboard ships and auditing them in the first and annual surveys of ships.

5. CONCLUSIONS

In an era where the maritime industry is increasingly reliant on digital technologies, ensuring the cyber resilience of ships has become paramount. This study has developed a practical checklist for ship cyber security based on the IACS UR E26 standard. The checklist serves as a comprehensive tool for ship owners and operators, aiding in the systematic management of cyber risks and ensuring compliance with international regulations.

The implementation of this checklist not only facilitates adherence to the IACS UR E26 standard but also enhances the overall safety and security of maritime operations by addressing potential vulnerabilities in ship systems. By adopting a proactive approach to cyber security, the maritime sector can mitigate the risks associated with cyber threats, thereby safeguarding critical systems and ensuring the uninterrupted operation of ships.

As the maritime industry continues to evolve, the importance of robust cyber security measures will only grow. Future research could focus on the continuous improvement of these measures, ensuring they remain effective against emerging threats. Additionally, the integration of this checklist into broader safety management systems could further streamline operations and improve the resilience of maritime infrastructure.

AUTHORSHIP CONTRIBUTION STATEMENT

Gizem KAYİSOGLU: Conceptualization, Methodology, Validation, Formal Analysis, Resources, Writing-Original Draft, Writing, Review and Editing, Visualization, Supervision. **Emre DÜZENLİ:** Conceptualization, Methodology, Validation, Formal Analysis, Resources, Writing-Original Draft, Writing. **Pelin BOLAT:** Conceptualization, Methodology, Validation, Formal Analysis, Resources, Writing-Original Draft, Writing, Review and Editing, Visualization, Supervision. **Fırat BOLAT:** Conceptualization, Methodology, Validation, Formal Analysis, Resources, Writing-Original Draft, Writing.

CONFLICT OF INTERESTS

The authors decelerate that they have no conflict of interest.

ETHICS COMMITTEE PERMISSION

No ethics committee permissions are required for this study.

FUNDING

This work was funded by Istanbul Technical University, Scientific Research Projects, General Research Project, which is titled as “Protection of Ship Bridge Systems Against Cyber Threats: Security Mechanisms and Implementation Strategies” with 45514 project code.

ORCID IDs

Gizem KAYİSOGLU
https://orcid.org/0000-0003-2730-9780
Emre DÜZENLİ
https://orcid.org/0009-0009-5179-1627
Pelin BOLAT
https://orcid.org/0000-0003-4262-3612
Fırat BOLAT
https://orcid.org/0000-0001-9807-7089

6. REFERENCES

Ashraf, I., Park, Y., Hur, S., Kim, S. W., Alroobaea, R., Zikria, Y. Bin, Nosheen, S. (2022). A Survey on Cyber Security Threats in IoT-Enabled Maritime Industry. *IEEE Transactions on Intelligent Transportation Systems*, 1–14. doi:10.1109/TITS.2022.3164678.

Bolbot, V., Kulkarni, K., Brunou, P., Banda, O.V., Musharraf, M. (2022). Developments and research directions in maritime cybersecurity: A systematic literature review and bibliometric analysis. *International Journal of Critical Infrastructure Protection*, 39: 100571. doi: 10.1016/j.ijcip.2022.100571

DNV-GL, (2016). Cyber security resilience management for ships and mobile offshore units in operation. *DNV-GL Corporate Report*, *DNVGL-RP-0* (September), 1–86.

DNV-GL, Cyber Secure Class Notation, (2022). Accessed Date: 03/07/2024, https://www.dnv.com/services/cyber-secure-class-notation-124600/ is retrieved.

Hyra, B. (2019). Analyzing the Attack Surface of Ships. DTU Compute Department of Applied Mathematics and Computer Science Technical University of Denmark. Accessed Date: 08/07/2024, https://backend.orbit.dtu.dk/ws/portalfiles/portal/218483747/190401_Analyzing_the_Attack_Surface_of_Ships.pdf is retrieved.

IACS, IACS UR E26 and E27 Press Release, (2024). Accessed Date: 05/08/2024, https://iacs.org.uk/news/iacs-ur-e26-and-e27-press-release is retrieved.

IACS UR E22, Computer-based Systems, (2023). Accessed Date: 05/08/2024 https://iacs.s3.af-south-1.amazonaws.com/wp-content/uploads/2023/08/10161629/ur-e22rev3.pdf is retrieved.

IACS UR E26, Cyber Resilience of Ships, (2022). Accessed Date: 05/08/2024, https://www.classnk.or.jp/hp/pdf/info_service/iacs_ur_and_ui/ur_e26_rev.1_nov_2023_cr.pdf is retrieved.

IMO, Guidelines on Maritime Cyber Risk Management, (2022). Accessed Date: 16/06/2024, https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3-Rev.2%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat)%20(1).pdf is retireved.

iTrust, Guidelines for Cyber Risk Manegement in Shipboard Operational Technology Systems, (2022). Accessed Date: 16/06/2024, https://itrust.sutd.edu.sg/research/projects/maritime-cyber/ is retrieved.

Jo, Y., Choi, O., You, J., Cha, Y., Lee, D.H. (2022). Cyberattack Models for Ship Equipment Based on the MITRE ATT&CK Framework. *Sensors*, 22(5): 1860. doi: 10.3390/s22051860.

Kanwal, K., Shi, W., Kontovas, C., Yang, Z., Chang, C.H. (2024). Maritime cybersecurity: are onboard systems ready? *Maritime Policy and Management*, 51(3): 484–502. doi: 10.1080/03088839.2022.2124464.

Kavallieratos, G., Katsikas, S., Gkioulos, V. (2019). Cyber-Attacks Against the Autonomous Ship. In S. K. Katsikas, F. Cuppens, N. Cuppens, C. Lambrinoudakis, A. Antón, S. Gritzalis, J. Mylopoulos, & C. Kalloniatis (Eds.), Computer Security, Springer International Publishing, 11387, pp. 20–36. doi: 10.1007/978-3-030-12786-2.

Kayisoglu, G., Bolat, P., Tam, K. (2022). Evaluating SLIM-based human error probability for ECDIS cybersecurity in maritime. *The Journal of Navigation* 75: 364–1388. doi: 10.1017/S0373463322000534.

Kayisoglu, G., Bolat, P., Tam, K., (2023). A novel application of the CORAS framework for ensuring cyber hygiene on shipboard RADAR. *Journal of Marine Engineering & Technology*, 1–15. doi: 10.1080/20464177.2023.2292782.

Kesseler, G.C. (2019). Cybersecurity in the Maritime Domain. *USCG Proceedings of the Marine Safety & Security Council*, 76(1): 11–13.

Martínez, F., Sànchez, L.E., Santos-Olmo, A., Rosado, D.G., Fernàndez-Medina, E. (2024). Maritime cybersecurity: protecting digital seas. *International Journal of Information Security*, 23(2): 1429–1457. doi: 10.1007/s10207-023-00800-0.

Palbar Misas, J. D., Hopcraft, R., Tam, K., Jones, K. (2024). Future of maritime autonomy: cybersecurity, trust and mariner's situational awareness. *Journal of Marine Engineering and Technology*, 23(3): 224–235. doi: 10.1080/20464177.2024.2330176.

Rajaram, P., Goh, M., Zhou, J. (2022). Guidelines for cyber risk management in shipboard operational technology systems. *Journal of Physics: Conference Series*, 2311(1): 012002. doi: 10.1088/1742-6596/2311/1/012002.

Rana, A. (2019). Commercial Maritime and Cyber Risk Management. *Safety & Defense*, 5(1): 46–48. doi: 10.37105/sd.42.

Reilly, G., Jorgensen, J. (2016). Classification considerations for cyber safety and security in the smart ship era. RINA, Royal Institution of Naval Architects - Smart Ship Technology 2016, Papers, January, pp. 33–39.

Santamarta, R. (2014). SATCOM Terminals: Hacking by Air, Sea, and Land. IOActive. Accessed Date: 23/05/2024, https://www.ioactive.com is retrieved.

Silverajan, B., Vistiaho, P. (2019). Enabling Cybersecurity Incident Reporting and Coordinated Handling for Maritime Sector. 2019 14th Asia Joint Conference on Information Security (AsiaJCIS), 88–95. doi: 10.1109/AsiaJCIS.2019.000-1.

Soner, O., Kayisoglu, G., Bolat, P., Tam, K. (2023a). Cybersecurity risk assessment of VDR. *The Journal of Navigation*, 76(1): 20–37. doi: 10.1017/S0373463322000595.

Soner, O., Kayisoglu, G., Bolat, P., Tam, K. (2023b). Risk sensitivity analysis of AIS cyber security through maritime cyber regulatory frameworks. *Applied Ocean Research*, 142: 103855. doi: 10.1016/j.apor.2023.103855.

Svilicic, B., Rudan, I., Jugović, A., Zec, D. (2019). A Study on Cyber Security Threats in a Shipboard Integrated Navigational System. *Journal of Marine Science and Engineering*, 7(10): 364. doi: 10.3390/jmse7100364.

Tam, K., Jones, K. (2019). MaCRA: a model-based framework for maritime cyber-risk assessment. *WMU Journal of Maritime Affairs*, 18(1): 129–163. doi: 10.1007/s13437-019-00162-2.

Tran, K., Keene, S., Fretheim, E., Tsikerdekis, M. (2021). Marine Network Protocols and Security Risks. *Journal of Cybersecurity and Privacy Communication*, 239–251. doi: 10.3390/jcp1020013.

Tucci, A.E. (2017). Cyber Risks in the Marine Transportation System. In: Cyber-Physical Security Protecting Critical Infrastructure at the State and Local Level, R. M. Clark & S. Hakim (Eds.), Springer International Publishing, Switzerland, pp. 113–131. doi: 10.1007/978-3-319-32824-9_6.

Witherby, BIMCO, ICS, (2023). *Cyber Security Workbook for On Board Ship Use*.

Zăgan, R., Raicu, G., Hanzu-Pazara, R., Enache, S. (2018). Realities in Maritime Domain Regarding Cyber Security Concept. *Advanced Engineering Forum*, 27: 221–228. doi: 10.4028/www.scientific.net/AEF.27.221.