Latest Trends in Ship Cybersecurity Regulations

— IACS UR E26/E27 and the Society's Initiatives —

Machinery Department, Plan Approval and Technical Solution Division, ClassNK
Management Systems & Maritime Training Certification Department, Business Assurance Division, ClassNK

1. INTRODUCTION

The rapid digitalization of ships in recent years has increased the risk of cyberattacks. The maritime industry is experiencing a sharp rise in damage caused by ransomware, and actual cyberattacks on ships have also been reported. In this context, ship cybersecurity has gained attention, and the International Association of Classification Societies (hereinafter referred to as IACS) has formulated IACS Unified Requirements (hereinafter referred to as UR) E26 and E27, which came into effect on July 1, 2024, for ships contracted for construction on or after that date. This paper outlines the background and trends in ship cybersecurity regulations, focusing on UR E26 and E27, as well as the Society's initiatives.

1.1 Cybersecurity Threats Surrounding Ships

Traditionally, ship systems such as navigation equipment, engine control systems, and cargo monitoring systems relied on physical connections and controls, and threats such as cyberattacks were not anticipated. However, with the introduction of IoT technology to improve operational efficiency and safety, and the recent launch of relatively inexpensive, high-capacity maritime Internet services such as Starlink provided by SpaceX in the United States and the adoption of automated navigation technology under development, there are an increasing number of cases of ship systems being interconnected via computers and the Internet. As a result, ship systems are increasingly exposed to cyberspace, and the risk of cyberattacks is becoming apparent.

According to statistics from the MTS-ISAC[*1], a maritime-focused cybersecurity information sharing and analysis organization in the United States, 15 % of all cyberattacks on the maritime sector in June 2024 were directed at ships. This clearly shows that cyberattacks on ships are definitely occurring and that the number of such attacks is on the rise.

In light of this situation, there is growing interest in cybersecurity in the maritime industry, and countermeasures are required for ships as well.

The specific cyberattack methods reported include ransomware hijacking of ship management systems, GPS spoofing[*2] to falsify location information, and phishing scams to steal crew members' personal information. Table 1 shows the main examples of such attacks.

Table 1 Examples of cyberattacks

2017 June: Maersk, a major shipping company, was hit by a cyberattack using ransomware called NotPetya, affecting its business locations worldwide. The attack disrupted the company's container shipping operations and is said to have caused hundreds of millions of dollars in losses.[3)]
2017 June: In the Black Sea, at least 20 ships experienced anomalies in their GPS receivers, showing their location to be about 32 km inland despite actually being at sea. This phenomenon is strongly suspected to be due to a GPS spoofing attack.[2)]
2019 May: According to the Marine Safety Information Bulletin issued by the U.S. Coast Guard (USCG), there have been reports of cases where emails were sent to ships from email addresses posing as PSC authorities in an attempt to extract confidential information contained in arrival notifications.[5)]
2023 January: The server of DNV's ship management software was attacked by ransomware, restricting access to online functions.[6)]

[*1] Abbreviation for Maritime Transportation System Information Sharing and Analysis Center (MTS-ISAC), an organization that shares and analyzes information on cybersecurity in the maritime field.
[*2] A type of cyberattack that misleads the position information of GPS receivers by transmitting fake GPS signals. There is a risk that this may disrupt the ship's course or cause a collision.

From past reported cases, it is clear that IT systems[*3] on ships are being targeted by cyberattacks such as ransomware and malware. On the other hand, the impact of cyberattacks on OT systems[*4] is still largely unknown, as details such as specific damage and attack methods are rarely made public. One reason for this is that if cybersecurity measures are inadequate, it is difficult to even notice that an attack has occurred. In addition, the risk of disclosing details of an attack could lead to damage to a company's reputation and loss of trust from business partners, as well as triggering further cyberattacks, which seems to be another reason why companies are hesitant to disclose information.

1.2 Trends in International Cybersecurity Countermeasures

In response to the increasing cybersecurity risks to ships, the International Maritime Organization (hereinafter referred to as IMO) and IACS are working to strengthen cybersecurity measures for ships.

1.2.1 IMO Initiatives

The IMO is progressively strengthening its efforts related to ship cybersecurity.

- ISPS Code

The ISPS Code (International Ship and Port Facility Security Code), adopted in 2004, focuses on physical security measures for ships and port facilities. While it does not directly require cybersecurity measures, it does require that the Ship Security Assessment (SSA) and Ship Security Plan (SSP) address vulnerabilities in computer-based systems and networks, and establish procedures for the protection of confidential information in electronic form. These are the foundation of cybersecurity measures. The ISPS Code is mandatory for Contracting Governments to the SOLAS Convention (International Convention for the Safety of Life at Sea).

- Resolution MSC.428(98)

Resolution MSC.428(98), adopted in 2017, recommends incorporating cyber risk management in a ship's Safety Management System (SMS). It requires that cyber risks be assessed in the same way as other risks in ship operations, and that appropriate measures be taken. This resolution is a recommendation, but many flag states have made it mandatory.

- GUIDELINES ON MARITIME CYBER RISK MANAGEMENT (MSC-FAL.1/Circ.3)

MSC-FAL.1/Circ.3, approved[*5] in 2017, supports the implementation of Resolution MSC.428(98). It provides specific recommendations on the roles, activities, and measures of shipping companies to assist ship operators and shipowners in implementing cyber risk management. It also refers to cybersecurity guidelines and standards issued by IACS, Baltic and International Maritime Council (hereinafter referred to as BIMCO), National Institute of Standards and Technology (hereinafter referred to as NIST)[*6], and others. While the GUIDELINES ON MARITIME CYBER RISK MANAGEMENT itself is not mandatory, it serves as a reference for ship operators and shipowners to establish and operate an effective cyber risk management system.

1.2.2 IACS Initiatives

IACS established the Cyber Systems Panel in 2016, where experts from each classification society gather to share information on the latest cybersecurity technologies and threats and discuss the development of unified rules.

- Twelve IACS Recommendations (hereinafter referred to as Rec.)

By November 2018, twelve Recs. had been published. These recommendations provide specific guidelines for ship cybersecurity measures, covering a wide range of areas which are recommended procedures for software maintenance of shipboard equipment and systems, recommendations concerning manual/local control capabilities for software dependent machinery systems, contingency plans for onboard computer based systems, network architectures, data assurance, the physical security of onboard computer based systems, the network security of onboard computer based systems, vessel system design, inventory lists of computer based systems, integration, remote update/access and communication and interfaces.

- Rec. No. 166

[*3] Abbreviation for Information Technology (IT) system, a system that collects, processes, stores and transmits data. On board ships, PCs for clerical work, etc. fall under this category.

[*4] Abbreviation for Operational Technology (OT) system, a system that monitors and controls physical processes and equipment. On board ships, systems such as navigation equipment, engine control systems, and cargo monitoring systems also fall under this category.

[*5] Regular updates are carried out, and MSC-FAL.1/Circ.3/Rev.2 was approved in 2022.

[*6] US government agency that conducts research and development on technology, measurement and standards. Also develops various guidelines and frameworks in the field of cybersecurity.

Prior to the development of UR E26 and E27, work was undertaken to consolidate the above twelve Recs. into one, and in May 2020, Rec. No. 166 was issued as a recommendation on cyber resilience. It summarizes the recommended cybersecurity measures for the construction and operation of new ships. It comprehensively shows the matters to be considered in each stage of ship design, construction, and operation, and specifically includes measures based on risk assessment, network separation, access control, system updates and crew education.

- UR E26 and E27

Based on the results of its previous efforts, IACS newly formulated two URs, E26 and E27, in April 2022, which stipulate requirements for cybersecurity. These are requirements for capabilities (hereinafter referred to as cyber resilience) to reduce the occurrence of cyber incidents due to cyberattacks, etc., to mitigate their impact, and to ensure early recovery in the event of an incident, based on the premise that cyberattacks will occur. UR E26 mainly stipulates the framework for cyber resilience of the entire ship, and UR E27 stipulates the security requirements for systems and equipment installed on board ships. The purpose of these is to realize ships with at least a minimum level of cyber resilience.

Initially, UR E26 and E27 were scheduled to come into force on January 1, 2024, but IACS revised UR E27 in September 2023 and UR E26 in November of the same year, based on feedback from the industry, clarification of inspection requirements, and limitations on the applicable ships. The revised versions of UR E26 and E27 came into effect on July 1, 2024 for ships for which construction contracts are concluded on or after that date.[*7]

2. OBJECTIVES AND OVERVIEW OF UR E26 AND E27 REQUIREMENTS

This chapter explains the objectives and overview of the UR E26 and E27 requirements. For details of the requirements, please refer to the Society's own guidelines, which are introduced in Chapter 3.

2.1 Relationship between UR E26 and E27

UR E26 stipulates a comprehensive framework for ensuring the cyber resilience of the entire ship, while UR E27 stipulates specific technical requirements for individual systems and equipment within the scope of UR E26. UR E26 also clarifies the cooperation and division of responsibilities among stakeholders, while UR E27 requires suppliers to ensure the security of computer based systems under their responsibility. (Fig. 1)

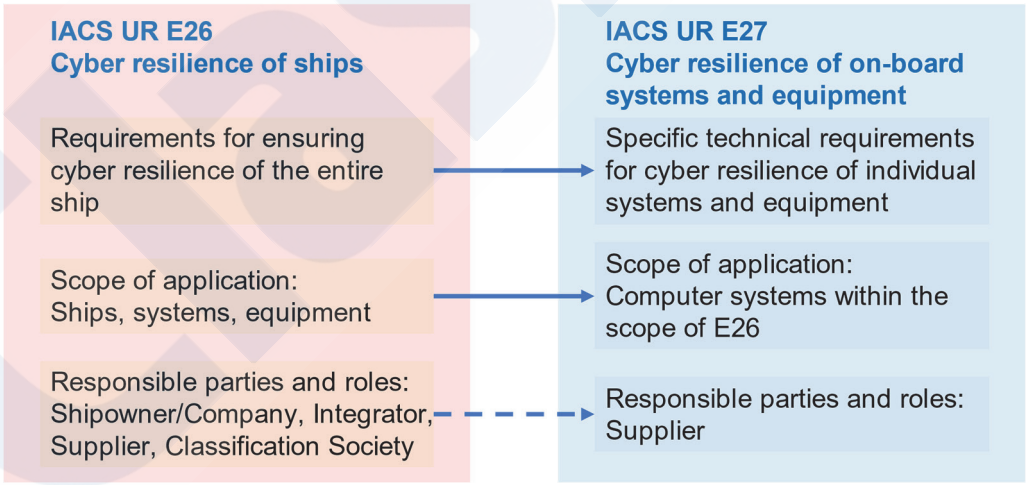

Fig. 1 Relationship of UR E26 and E27

2.2 Objectives and Overview of UR E26 Requirements

UR E26 is a rule that applies to the entire ship and mainly stipulates requirements related to shipyards (systems integrators) and shipowners. Specifically, it aims to safely integrate Operational Technology (OT) systems and Information Technology (IT) systems into the ship's network throughout the various stages of ship design, construction, commissioning, and operation, and stipulates requirements such as "Identify," "Protect," "Detect," "Respond" and "Recover."

[*7] The initial versions were withdrawn before the start of application.

2.2.1 UR E26 Objectives and the NIST Cybersecurity Framework

The requirements of UR E26 are organized and defined based on the five core elements of the NIST Cybersecurity Framework, referring to Rec. 166, guidelines from each classification society, BIMCO guidelines, NIST SP 800-53 and others. The objectives for each element are tailored to the specific characteristics of the ship so as to achieve the following goals (Fig. 2):

- Identify: To gain a comprehensive understanding of the ship's systems, the people involved, data, equipment, etc., and to identify and deepen the organizational understanding of cybersecurity risks.
- Protect: To implement measures to safeguard the ship from cyber incidents and to ensure the continuation of ship operations even in the event of an attack.
- Detect: To establish mechanisms for promptly detecting and identifying the signs of cyber incidents.
- Respond: To implement response measures to minimize damage in the event of detecting a cyber incident.
- Recover: To secure means for swift recovery and return to normal operation if ship functions are impaired due to a cyber incident.

Fig. 2 Five core elements of the NIST Cybersecurity Framework[4)]

2.2.2 Ships Subject to UR E26

The following ships, etc., are subject to UR E26:

- Passenger ships (including passenger high-speed craft) engaged in international voyages
- Cargo ships of 500 GT and upwards engaged in international voyages
- High speed craft of 500 GT and upwards engaged in international voyages
- Mobile offshore drilling units of 500 GT and upwards
- Self-propelled mobile offshore units engaged in construction (i.e., wind turbine installation, maintenance and repair, crane units, drilling tenders, accommodations, etc.)

Application to ships not engaged in international voyages and cargo ships of less than 500 GT is not mandatory.

2.2.3 Systems Subject to UR E26

UR E26 applies to onboard OT systems with the following functions, where the impact of a cyber incident could endanger human safety, the safety of the ship or the environment:

(a) Propulsion
(b) Steering
(c) Anchoring and mooring
(d) Electrical power generation and distribution
(e) Fire detection and extinguishing systems
(f) Bilge and ballast systems, loading computers
(g) Watertight integrity and flooding detection
(h) Lighting (e.g., emergency lights, low location lights, navigation lights, etc.)
(i) Any required safety system whose disruption or functional impairing may pose risks to ship operations (e.g., emergency shutdown systems, cargo safety systems, pressure vessel safety systems, gas detection systems, etc.)
(j) Navigational systems required by statutory regulations
(k) Internal and external communication systems required by class rules or statutory regulations

Furthermore, UR E26 stipulates that any IP-based communication interfaces connected to these OT systems are also to be within the scope of application. Therefore, systems and equipment other than the above OT systems may also be subject to UR E26.

2.2.4 Risk Assessment and Exemptions under UR E26

UR E26 states that if the systems integrator can demonstrate to the classification society that a system meets four criteria and considers three additional criteria, and the classification society approves, then that system can be excluded from the requirements of UR E26.

2.3 Overview and Objectives of UR E27 Requirements

UR E27 is a rule that applies to systems and equipment installed on board ships, and mainly stipulates requirements related to suppliers. Specifically, it defines the requirements for the cyber resilience of systems and equipment, the interface between onboard users and computer based systems, and the product development requirements for new products aiming to ensure cyber resilience at the product level.

2.3.1 Scope of Application of UR E27

UR E27 stipulates that it is applicable to computer based systems specified in UR E26 on ships subject to UR E26.

2.3.2 Security Capability Requirements of UR E27

UR E27 specifically defines the requirements for security capabilities to be implemented in systems. These requirements are based on IEC 62443-3-3, an international standard for the security of industrial automation and control systems, and some parts of it have been adopted. Specifically, 30 “required security capabilities” and 11 “additional required security capabilities” for computer based systems connected to untrustworthy networks are defined. These security capabilities are specific countermeasures that computer based systems should have, such as “authentication,” “access control,” “encryption” and “anti-malware.” By meeting these requirements, the risk of cyberattacks can be reduced, and the security of the system can be ensured.

2.3.3 Secure Development Lifecycle (SDLC) Requirements of UR E27

UR E27 defines requirements for the lifecycle related to the development and maintenance of secure products, and requires the introduction of a development process that considers security in the development of systems and equipment. Specifically, seven requirements are defined, such as “Controls for private keys,” “Security update documentation,” “Dependent component security update documentation,” “Security update delivery,” “Product defence in depth,” “Defence in depth measures expected in the environment” and “Security hardening guidelines.” This allows for the elimination of security vulnerabilities from the development stage, leading to the construction of more secure systems.

3. SOCIETY INITIATIVES AND SUPPORT FOR UR E26 AND E27

This is the first time that cybersecurity measures have been incorporated as mandatory requirements for newbuilding ships, and the impact is significant. Therefore, the Society has been working on prompt rulemaking and information dissemination. The Society has been providing information such as its own guidelines explaining the requirements of UR E26 and E27 for suppliers, shipyards and shipowners who need to comply with the requirements, interactive workshops with specific examples for compliance and explanatory videos.

3.1 Incorporation of UR E26 and E27 into the Society’s Rules

Following the issuance of UR E26 and E27, the Society incorporated these requirements into its rules. To incorporate the two URs into Part X and Part B of the Rules for the Survey and Construction of Steel Ships, as well as the “Guidance for the Approval and Type Approval of Materials and Equipment for Marine Use,” the Society held deliberations by an expert committee consisting of experts (December 2023) and the Technical Committee (January 2024), and issued a revised version on June 27, 2024.

Fig. 3 shows the structure of Part X of the Rules for the Survey and Construction of Steel Ships, which mainly stipulates the requirements of the two URs.

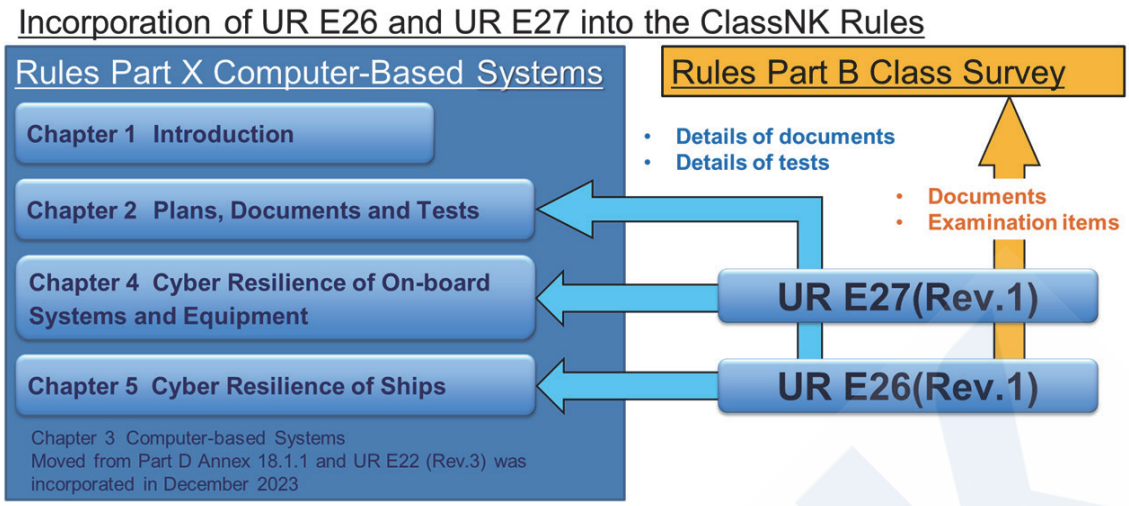

Fig. 3 Incorporation of UR E26 and E27 into the Society's Rules
(Structure of Part X of Rules for Steel Ships)

The Society has newly established provisions for "Approval of Use*8 of Systems and Equipment with Improved Cyber Resilience" in Chapter 10 of Part 7 of the "Guidance for the Approval and Type Approval of Materials and Equipment for Marine Use." This allows suppliers to obtain a certificate of approval for use in advance, certifying that equipment, etc., that meets the cybersecurity requirements complies with the regulations, before preparing for installation on board ships.

3.2 Guidelines Explaining the Requirements of UR E26 and E27

First, the Society believes that it is necessary to have equipment that meets the cybersecurity requirements available in the market. Therefore, the Society issued its own guidelines "Guidelines on Cyber Resilience of Onboard Systems and Equipment" in November 2023 to explain UR E27, which stipulates the requirements for equipment.

Furthermore, in July, 2024, the Society issued its own guidelines "Guidelines on Cyber Resilience of Ships" to explain the requirements of UR E26. Fig. 4 shows each guideline and their structure.

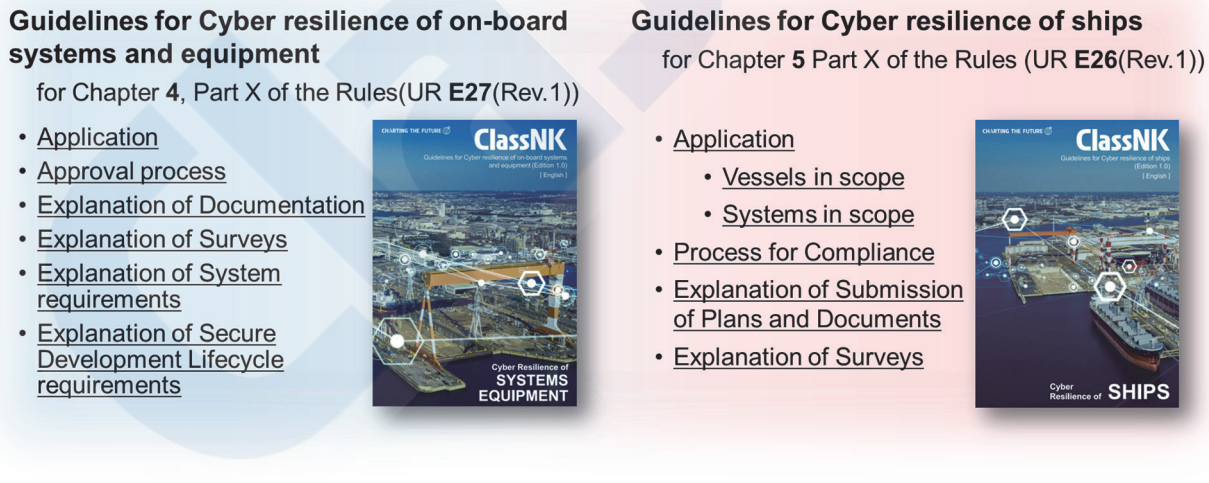

Fig. 4 Guidelines explaining the requirements of UR E26 and E27 and their structure

In particular, the Society aimed to make its two guidelines "easy to understand" as explanatory books by providing many examples that are not mentioned in the URs. For example, the Society provides specific examples of systems to which the cybersecurity requirements apply, such as engine control systems, steering system control systems, fixed CO_2 fire extinguishing

*8 For equipment, etc., for which the rules, etc. stipulate that the approval of the Society for it use must be obtained in advance, before preparing for installation onboard a ship, representative individual products are examined, tested and inspected in advance as stipulated in the Guidance, and the Society approves that the equipment conforms to the provisions.

systems and radars. Fig. 5 shows a part of these.

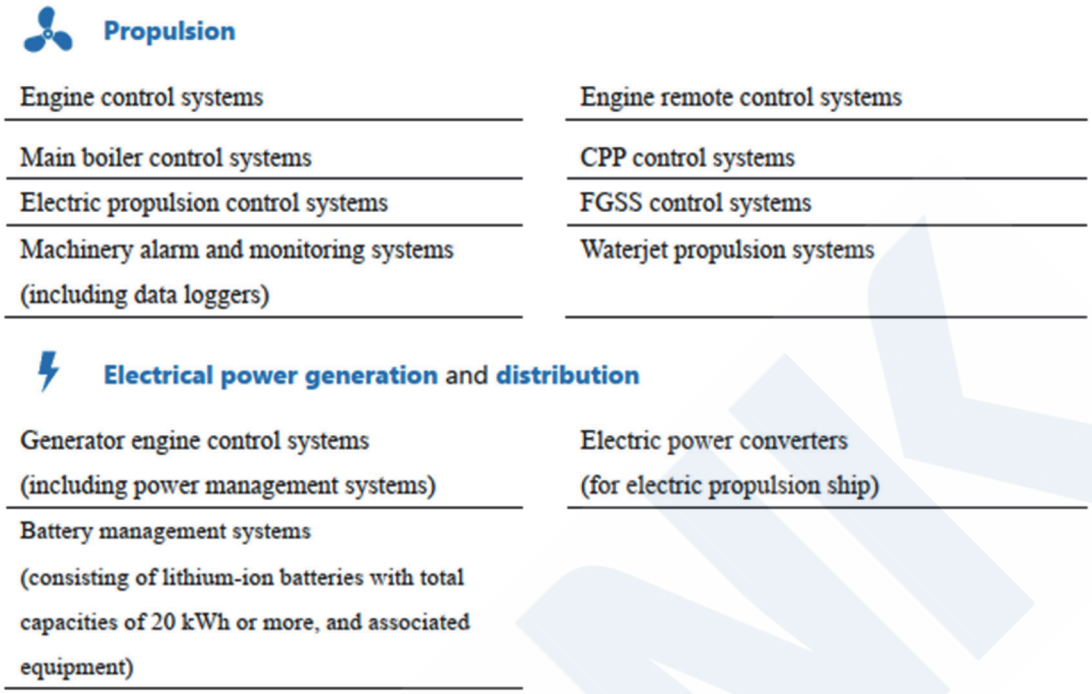

Fig. 5 Examples of systems subject to application in the Guidelines

3.3 Portal Page

On its website, the Society provide explanatory videos and FAQs (which are updated regularly). All of these can be viewed on the portal page that aggregates information and materials related to UR E26/E27 on the website. (https://www.classnk.or.jp/hp/en/activities/cybersecurity/ur-e26e27.html)

The portal page provides the following information and materials and is constantly being updated:

- Related rules
- Application forms for approval of use
- Guidelines
- FAQs
- Explanatory videos

3.4 ClassNK Academy

For those who wish to deepen their understanding in a more specialized manner, the Society has also established a new course on cyber resilience of onboard systems and equipment for developers and designers of marine equipment at the ClassNK Academy. In this course, the Society invites lecturers from the Control System Security Center (CSSC), which is a technology research association engaged in certification work for IEC 62443, an international standard for cybersecurity of industrial equipment and the basis of UR E27. The lecturers explain the basic concepts of the IEC standard, the security capabilities required by UR E27 and the secure development lifecycle.

4. CONCLUSION AND FUTURE PROSPECTS

In this paper, the Society introduced the ship cybersecurity regulations UR E26/E27 and the Society's own initiatives. The cybersecurity environment surrounding ships is changing every day, and the introduction of new technologies such as autonomous ships is expected to require further measures.

In the future, the digitalization and automation of ship operations will accelerate, and the use of cyberspace will advance. In addition to responding to URs and IMO guidelines, multifaceted security enhancements such as responding to automation and autonomy, collecting and sharing threat information, developing security personnel and utilizing new technologies are essential.

The Society's mission is to realize safe and sustainable shipping, and the Society considers improving the cyber resilience of ships to be an important element of that mission. The Society will continue to work with stakeholders to promote initiatives in this area.

REFERENCES

1) K. Nakayama: Current Status of Building Cybersecurity Measures for Ships, Journal of the Japan Institute of Marine Engineering, 2020; 55(5):553-556.
2) The Maritime Executive: Mass GPS Spoofing Attack in Black Sea?, July 11, 2017, https://maritime-executive.com/editorials/mass-gps-spoofing-attack-in-black-sea .
3) Safety4Sea: Maersk Line: Surviving from a Cyber Attack, Safety4Sea, July 8, 2017, https://safety4sea.com/cm-maersk-line-surviving-from-a-cyber-attack/ .
4) National Institute of Standards and Technology: Framework for Improving Critical Infrastructure Cybersecurity Version 1.1, https://www.nist.gov/cyberframework .
5) USCG: Marine Safety Information Bulletin (No. 04-19) (May 24, 2019).
6) DNV AS : Cyber-attack on ShipManager servers – update, published January 23, 2023, https://www.dnv.com/news/cyber-attack-on-shipmanager-servers-update-237931/ .
7) IMO. (2022). Guidelines on Maritime Cyber Risk Management (MSC-FAL.1/Circ.3/Rev.2).
8) IACS: IACS Recommendations, No. 166 (April 2020) "Recommendation on Cyber Resilience."
9) IACS: IACS Unified Requirements, E26 (Rev.1) (November 2023) "Cyber resilience of ships."
10) IACS: IACS Unified Requirements, E27 (Rev.1) (September 2023) "Cyber resilience of on-board systems and equipment."
11) IACS: IACS adopts new requirements on cyber safety, https://iacs.org.uk/news/iacs-adopts-new-requirements-on-cyber-safety/ .
12) IACS: IACS UR E26 and E27 Press Release, https://iacs.org.uk/news/iacs-ur-e26-and-e27-press-release .
13) ClassNK: Guidelines for Designing Cyber Security Onboard Ships (1st Edition) (March 2019).
14) ClassNK: Cyber Security Management System for Ships (1st Edition) (April 2019).
15) ClassNK: Guidelines for Software Security (1st Edition) (May 2019).
16) ClassNK: Guidelines for Designing Cyber Security Onboard Ships (2nd Edition) (July 2020).
17) ClassNK: Guidelines for Cyber resilience of on-board systems and equipment (1st Edition) (November 2023).
18) ClassNK: Guidelines for Cyber resilience of ships (1st Edition) (July 2024).