

# KR Maritime Cyber Safety News & Report



**Vol. 060**  
**Dec. 2023**



# CONTENTS

---

## **Maritime Cyber Safety News**

- IACS, UR E26 & E27 Rev.1 issued
- Swedish Club to offer cyber security insurance from 2024
- DP World Australia resumes operations at ports after cyber attack
- NorthStandard provides tips to identify phishing emails

## **Maritime Cyber Security Expert Column**

- Measures to strengthen smart ship convergence security: Necessity of security guidelines and vulnerability inspection
- Introduction to risk management-based cybersecurity framework

## **Advertisement**

- KR Cyber Security E-LEARNING & Training Tool

# IACS, UR E26 & E27 Rev.1 issued

*Source : IACS*

IACS enhances its Unified Requirements (URs) on Cyber Safety to reflect new survey requirements, industry feedback and applicability. In an increasingly digitalised and interconnected world, where the maritime industry continues to adopt, at pace, new digital technologies, it remains imperative to focus on cyber threats and attacks that could compromise operations, safety and data integrity.

To address the need to enhance the cyber resilience of ships, last year IACS published UR E26 “Cyber Resilience of Ships”, and UR E27, “Cyber Resilience of On-Board Systems and Equipment”, which applied to new ships from 1 January 2024.

Since the publication of these requirements, and as experience of cyber security oversight in the maritime sector grows, the need for a standardized approach to survey requirements has been identified along with further enhancements resulting from industry feedback.

Additionally, and to address the challenges regarding the implementation of new cyber requirements in smaller and non-conventional vessels, the scope of applicability of these URs have been categorised as mandatory and non-mandatory compliance depending on vessel types and sizes.

These improvements have resulted in extensive changes to the two URs and so **they will now supersede the originals and will be applied to new ships contracted for construction on and after 1 July 2024.** To avoid confusion, the original versions, along with their previous application date of 1 Jan 2024, have been withdrawn. The revised version of URE27 is available on the IACS website (<https://iacs.org.uk/resolutions/unified-requirements/ur-e>). The revised version of URE26 is still being finalized and will be published before the end of the year. **(Editor: 1 Nov. 2023 issued.)**

IACS Secretary General, Robert Ashdown, said ‘Incorporating industry feedback to ensure IACS requirements are clear in their applicability and are capable of being consistently applied in ship surveys, is important in ensuring that measures to enhance cyber resilience have the desired impact. As a result, and given that the original requirements had not yet entered into force, IACS has decided to apply only the revised requirements from 1 July 2024. It is believed that industry will welcome the clarity that this decision brings.’

# Swedish Club to offer cyber security insurance from 2024

*Source : Safety4sea The Editorial Team*

The Swedish Club has announced that from 1 January 2024, it will offer all Club members Cyber Insurance coverage, providing reassurance and support in the event of a cyber attack. This move makes The Swedish Club one of the first marine insurers to provide such coverage and is in alignment with the guidelines set by the IMO for cyber security.

The IMO cyber security guidelines aim to provide managers and crew with the capabilities to cope effectively with cyber attacks that occur on computer-based systems on board ships. The cover will be offered at preferential rates to all vessels insured for H&M and/or P&I through the Club, with three packages available depending on the level of cover needed.

Thomas Nordberg, Managing Director of The Swedish Club says: “As the industry’s ‘All-in-One Club’ we have worked hard to build a reputation for providing our members with comprehensive support for all their operational needs, and offering this cyber insurance is a natural progression in our commitment to them.”

“Partnered with our loss prevention efforts, this initiative now addresses the escalating threat of cyber attacks.”

“When port states and coast guards around the world start asking about cyber risk mitigation and resilience – and they already are – our member shipowners can show them a Cyber Insurance policy from The Swedish Club, with specialist cover for maritime cyber-emergency response, physical damage and wreck removal resulting from a cyber attack. We think that is worth a lot for our members and it’s why we want to protect them.” he adds.

The Club has partnered with leading experts in the field to develop this new insurance and tailored the packages to meet the diverse needs of members. The Basic package covers maritime cyber-emergency response, physical damage, and resulting loss of hire and the Basic Plus version offers expanded coverage limits. For those seeking the highest level of coverage, a comprehensive insurance package is available, all at competitive rates. In addition, in the event of an incident

members can take advantage of a 24/7 hotline manned by cyber specialists.

Thorbjörn Emanuelsson, Director of Underwriting, says:

“Cyber threats should not be taken lightly, and these new products will be instrumental in safeguarding members from the financial repercussions of cyber attacks.”

Overall, the maritime industry has been increasingly aware of the importance of cybersecurity. The maritime industry faces various cybersecurity threats, including ransomware attacks, phishing, and other forms of malware. DP World Australia has been a recent target of a cyber attack after a cyber-attack disrupted its facilities, for three days.

# DP World Australia resumes operations at ports after cyber attack

Source : *thenationalenws.com*



Source: *thenationalnews.com*

DP World Australia, part of Dubai's global ports operator DP World, has resumed operations at all its ports across the country on Monday morning, after a cyber attack forced the company to restrict work for three days.

The resumption of operations follows the “successful tests of key systems overnight”, DP World Australia said on Monday. The company expects that approximately 5,000 containers will move out of its four Australian terminals on Monday.

It operates terminals in Melbourne, Sydney, Brisbane and the port city of Fremantle in Western Australia.

“The ongoing investigation and response to protect networks and systems may cause some necessary, temporary disruptions to their services in the coming days,” it said.

“This is a part of an investigation process and resuming normal logistical operations at this scale.”



Dubai-based DP World employs more than 7,000 people in the Asia-Pacific region and has ports and terminals in 18 locations.

It manages almost 40 per cent of the goods flowing in and out of Australia.

“Although port operations have resumed, it does not mean that this incident has concluded,” national cyber security co-ordinator Air Marshal Darren Goldie said on X, the platform previously known as Twitter.

“The Australian government is continuing to work with DP World Australia to support the management of any further consequences, including any ongoing disruption to Australia’s supply chains.

“Investigations into the incident remain ongoing and remediation work is likely to continue for some time,” he said.

The incident follows a similar one at Industrial and Commercial Bank of China, the world's biggest lender, which was hit by a cyber attack on Friday that caused disruption in US Treasury markets and forced traders to conduct transactions using USB sticks.

Cyber security attacks can cause reputational and financial damage to people and companies. The global average for a data breach in 2022 was \$4.35 million, up from \$4.24 million the previous year, according to IBM's Cost of a Data Breach report.

# NorthStandard provides tips to identify phishing emails

*Source : Safety4sea The Editorial Team*

The NorthStandard provides some useful hints and tips on how to identify phishing emails and how to stay safe on the Internet.

The threat around phishing emails remains high. Hackers can quickly identify an opportunity to take advantage of changing circumstances and raise their game around attempts to hack organizations.

Employees within any organization remain its greatest asset, but they can also be its greatest security threat due to their inherent trusting nature. Its far easier to hack a human rather than attacking sophisticated system-based controls that may be in place.

As informed, the number of Phishing emails has increased by approximately 400% globally over the past three years with employees remaining a prime target, predominantly by being tricked into clicking a link, opening a malicious attachment, providing personal or commercial data or unknowingly sending payments to a fraudulent recipient. Phishing emails are effective because they are quick, cheap and easy to send and can reach millions of mailboxes within seconds. One click or response makes it worthwhile for the hackers.

According to the NorthStandard, there are some useful hints and tips to watch out for when receiving an email to help you stop becoming the victim of a successful phishing attack:

- Always assess the context of an email, do you know the sender and were you expecting an email from them or is it completely out of the blue or making an unusual request?
- If your organization utilizes spam filter warnings within the email subject or use warning banners to advise that an email has been sent externally to your organization, be suspicious if the email is portraying to be from a work colleague internally but is marked as external.
- Is the sender hassling you to do something or to take an action? Never feel rushed into taking an action, it's a common tactic to hurry you into making a mistake.



- Is there an incentive to open an attachment? For example, something nice if you comply such as a gift voucher or something nasty if you don't i.e., a fake speeding ticket or fake legal summons using fear in the hope to convince you to click a link or open an attachment.
- Does the domain name/ email address look correct? Hover your mouse over the email address or right mouse click to check the email properties. Does the spelling of the email address look correct or have letters been replaced to fake a domain name such as use of 'rn' to look like an 'm'?
- Is the email addressed to you personally or is it just generic i.e. Dear Sir or Madam? Does its structure look genuine? Many Phishing emails are not personalised, is something just not right? Trust your instinct and report/ always ask for help if unsure.
- An email contains a request for money/change of bank details held on file or to provide personal details. Please be wary of unexpected requests.
- Remember genuine email accounts can also be hacked. Please be wary of the content of an email if the style of a message from a contact that you know suddenly changes i.e., the way they address you or their grammar/ use of language changes or they ask you something odd and unexpected such as clicking a link or opening a strange and unexpected attachment.
- If unsure of the legitimacy of an email portraying to be from a contact, verify its authenticity by contacting them directly via independently verified contact details not from the details displayed within the email just received! Pick up the phone and verify.

## Measures to strengthen smart ship convergence security: Necessity of security guidelines and vulnerability inspection

Source : Researcher Jaedong Jang, Jiyong Choi, Korea Internet & Security Agency(KISA)

Editor : LIM, Jeoungkyu, Korean Register

### Overview

In March 2011, a total of 22 of the world's first 'smart ships' with ship area network (SAN) technology, jointly developed by Hyundai Heavy Industries and the Electronics and Telecommunications Research Institute (ETRI), were delivered to AP Moller, the world's No. 1 shipbuilder in Denmark. It was the first case of applying technology to a ship that integrated 460 types of equipment that were independently managed on the ship using IT, and 12 years later, marine ship technologies that converge information and communication, sensors, and smart technologies are continuously emerging.

As such, the marine ship sector is undergoing a paradigm shift in the safety, reliability, efficiency, and eco-friendliness of existing ships, centered on the development of advanced ICT technologies such as IoT (Internet of Things) and autonomous navigation technology. According to Acute Market Report's autonomous ship market size forecast released in 2017, the smart ship market is expected to grow at a compound annual growth rate of 12.8% from \$5.6 billion in 2016 to reach approximately \$155 billion in 2025.

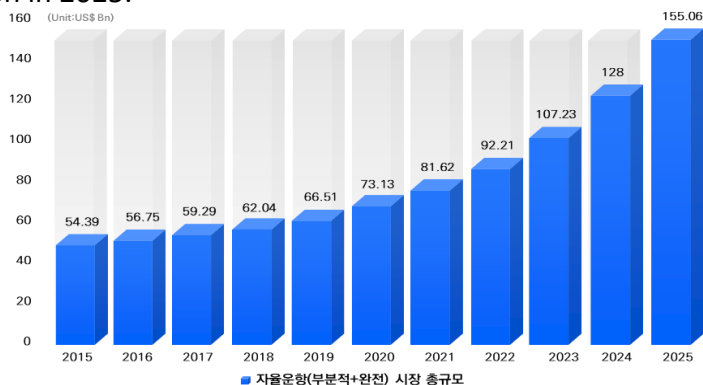


Figure 1 Autonomous ship market size('16~'25)

However, as the smart ship sector is gaining attention as a promising new industry with huge social and economic impact, cybersecurity threats targeting the industry are also increasing. From the hacking of the navigation system of a German shipping line's container vessel in February 2017, which resulted in the loss of control of the navigation system for 10 hours, to the hacking of the management server of a Norwegian classification DNV ship in January 2023, security threats arising from the existing IT environment are being transferred to the maritime and shipbuilding industries.

In this article, we will look at the domestic and international trends in cybersecurity of smart ships, and examine the need for security guidelines and security vulnerability check policies for smart ships through the security enhancement cases of other convergence industries.

## ● Domestic and International Trends in Smart Ship Cybersecurity

Recognizing the dangers of cyber attacks that are spreading across the maritime industry, shipping companies have established guidelines and guidelines for cybersecurity of maritime vessels. Starting with the first cybersecurity guidelines published by the Baltic and International Maritime Council(BIMCO) in 2016, the International Maritime Organization(IMO) approved cyber risk management guidelines in 2017, and the United States Coast Guard(USCG) released cyber risk management practice guidelines in 2020, incorporation of cyber risk ISM into the Rightship inspection vessel questionnaire in 2021, and the release of the International Association of Classification Societies(IACS) Cybersecurity UR E26 and E27 in 2022, the maritime industry is not only recognizing the need for maritime cybersecurity, but is constantly strengthening its measures to manage and respond to cyber risks.

In line with this international trend, Korea has also begun to conduct various studies such as cybersecurity guidelines to respond to security threats in the maritime industry. Korea Classification Society, the only international ship inspection organization in Korea, has been operating the Ship Cybersecurity Response TFT since 2016, laying the foundation for providing core technologies and security solutions for maritime cybersecurity. In 2017, it provided 'cybersecurity certification services' for shipping companies and equipment companies, and also prepared and operated the 'Maritime Cybersecurity Management System Guidelines' to strengthen the cybersecurity of ships and vessels. In addition, the cyber resilience guidelines are being established

to proactively respond to classification inspections mandated by the enactment of IACS UR E26(ship cyber resilience) and E27(equipment system and equipment cyber resilience).

In addition, the Ministry of Oceans and Fisheries enacted the Maritime Cybersafety Management Guidelines on April 21 this year, the first in the transportation sector to define the roles of the government and private sector. The notice stipulates the government's role in preventing damage from possible cybersecurity threats to ships and protecting the lives and safety of the public, as well as matters to be considered when establishing a cybersafety management system for shipping companies. Based on this, the Ministry of Oceans and Fisheries plans to establish and release the 'Maritime Cyber Safety Comprehensive Plan' this year.

As such, maritime cybersecurity guidelines and guidelines have been established and implemented around the world to protect the maritime industry from cybersecurity threats. However, since these guidelines are only recommendations, it is necessary to establish cyber threat prevention and response measures specific to the coastal industry by referring to the guidelines. Therefore, we will look at how to build smart ship security guidelines and support security vulnerability checks based on other industries' convergence security enhancement cases.

### ● Case of Convergence Security in Other Industry(autonomous vehicles)

Similar to the smart ship industry, the automobile industry is also converging various IT technologies with automobiles as ICT technology advances, and security threats that occurred in the existing IT environment are being transferred to the automobile industry. In 2016, a hacking demonstration of a Jeep Cherokee vehicle revealed that vehicles can be hacked by external hackers, and policy and technical activities to protect cars from external hacking began across the automotive industry. In 2021, the EU implemented a regulation that prohibits automakers from selling vehicles without an automotive cybersecurity management system, and China, Japan, and South Korea are also pursuing legislation to mandate cybersecurity in the automotive industry.

Industry organizations such as the Society of Automotive Engineers (SAE) have also established international standards for automotive cybersecurity and are continuously promoting various activities to internalize cybersecurity in the automotive industry. In line with these international trends, large automakers are actively responding to cybersecurity regulations by utilizing their technology and manpower, but it is difficult for small and medium-sized manufacturers and parts companies to respond to regulations on their own due to a lack of cybersecurity-related experts and budgets.

To support this difficult situation, the Korea Internet & Security Agency(KISA) has developed and distributed a security model for autonomous vehicles in the form of guidelines to the industry to improve the cybersecurity level and capabilities of small and medium-sized automobile manufacturers and parts companies. The security model identifies security threats that can occur in vehicles and suggests security technologies that can respond to each security threat and measures to respond to global regulations. In addition, to support companies that have difficulty operating vehicle cybersecurity test tools and facilities that are more expensive than those in the IT industry, KISA has established an autonomous vehicle security living lab equipped with various vehicle security check tools and test environments to conduct security tests on equipment and vehicles developed by companies and compensate for security vulnerabilities.

## ● Autonomous Vehicle Security Model

The autonomous vehicle security model provides a detailed guide for corporate security personnel to apply cybersecurity to their products (vehicles, major parts) and internal systems. Currently, the autonomous vehicle security model is divided into three parts. Part 1 of the autonomous vehicle security model is a guide that presents security enhancement measures for the interior of the car and car services, dividing the internal and external environments into layers, and explains in detail the security threats that may occur in each layer and the countermeasures to them. Through this

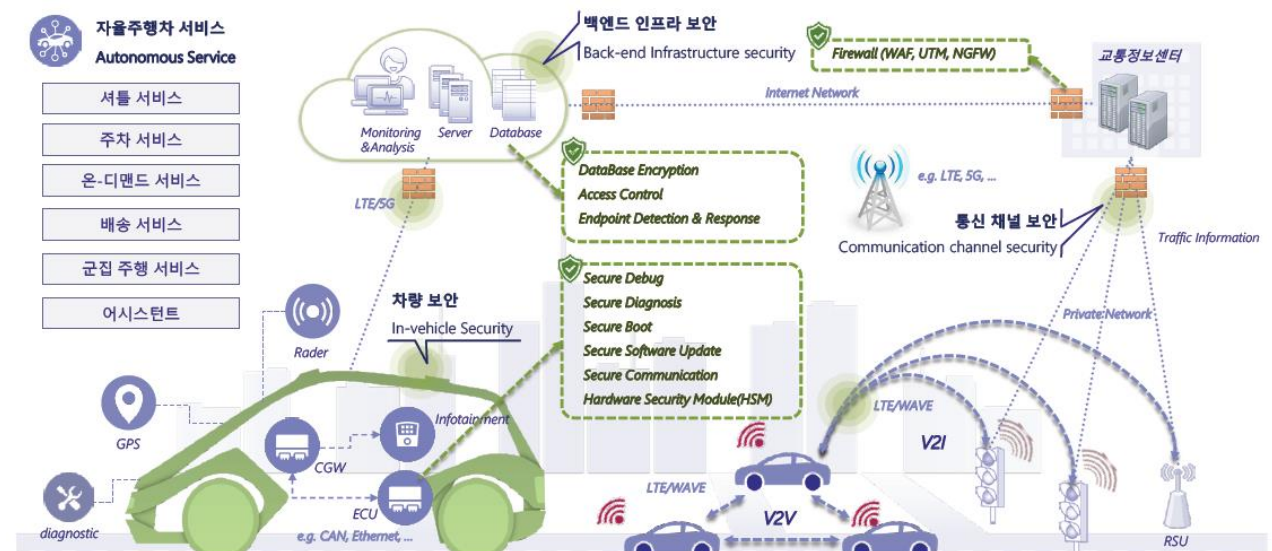


Figure 2 Autonomous Vehicle Cyber Security Solution (Security Model Part1)

<source: KISA "Autonomous Vehicle Security Model Part1<Autonomous Vehicle and Service>", Dec, 2020>

guide, companies in the field can understand the security technologies and countermeasures required for their products. Parts 2 and 3 of the autonomous vehicle security model explain how to establish an internal management system in response to the Cybersecurity Management System (CSMS) and Update Management System (SUMS) regulations, which are European automotive cybersecurity regulations. The security model provides a detailed analysis of the regulatory content so that domestic manufacturers can easily respond to overseas regulations, describes the items that each manufacturer must comply with and the administrative, physical, and technical methods for establishing their own cybersecurity management system, and guides how to submit evidence and deliverables for each process for European regulatory approval.

### ● Autonomous Vehicle Security Living Lab

The Autonomous Vehicle Security Living Lab was established at the Korea Advanced Institute of Automotive Technology in Saemangeum, Gunsan, Jeollabuk-do, to support companies that have difficulty operating security tests and facilities on their own. The Saemangeum area, where the Security Living Lab is built, is a specialized industrial complex where more than 90% of medium and large-sized commercial vehicles in Korea are produced, and the autonomous vehicle security living lab provides immediate support for companies that lack cybersecurity capabilities in the industrial field.

The Security Living Lab is equipped with test environments and inspection tools for various security tests to support the security requirements required by international regulations and standards. The test environment is a HIL (Hardware in the Loop) system that links a virtual simulation environment with a real vehicle so that security tests can be conducted indoors, and various parts can be tested by combining the virtual environment with the linked vehicle. We also support test vehicles to conduct various security tests in the real field through a driving test center with controlled road conditions. As for the inspection tools, various security tools are introduced and operated to enable various tests such as fuzzing tests and functional tests required by international regulations and standards, and various test procedures and cases are provided in manuals according to the requirements of international regulations. In addition, the autonomous vehicle security living lab provides inspection tools and test procedures to test the stability and security of autonomous driving sensors (radar, lidar, ultrasound, camera, GPS) and external



communication (V2X-WAVE, V2X-Cellular) devices for vehicles.

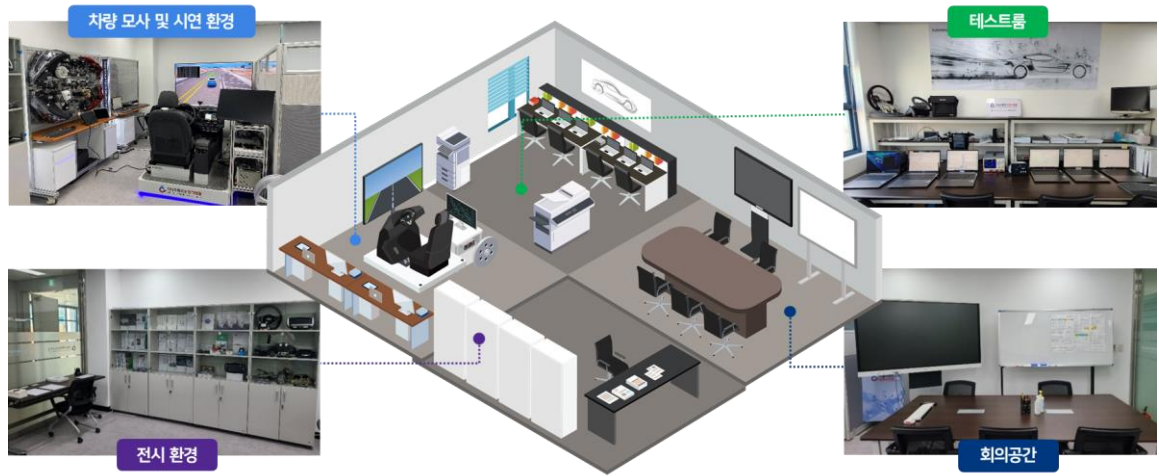


Figure. 3 Autonomous Vehicle Security Living-Lab

## ● Concluding the article...

As ICT technology converges with the maritime and shipbuilding industries, various security issues that occurred in the existing IT environment are rapidly being transferred to the smart ship field. As in the previous case, hacking attacks targeting the maritime and shipbuilding industries continue to increase, and the IMO and the IACS are implementing regulations to respond to cybersecurity threats. The BIMCO and the Digital Container Shipping Association(DCSA) have also published ship cybersecurity guidelines, requiring ships to have a cybersecurity management system in place. However, if the pace of these regulations is implemented without taking into account the adaptability of the industry, it is expected to cause significant disruption for companies with relatively weak cybersecurity capabilities, such as automotive industry case. In order to strengthen the cybersecurity responsiveness of domestic companies to these international regulations and standards, it is necessary to develop a smart ship security model, build a testbed, and provide security consulting for the maritime industry as in the case of other convergence industries. And expect the domestic maritime and shipbuilding industries to develop into a stepping stone to lead global maritime cybersecurity through such proactive security measures.

## ● Reference

1. 'Cyber Security Trends for Maritime Ships', Prof. Seo, Jung Taek in Gachon University, Weakly Technology Trends 2057, 2022.08.03., Institute of Information & Communications Technology Planning & Evaluation (IITP)
2. edaily, 2011.03.25., (<https://www.edaily.co.kr/news/read?newsId=02233686596186600>)
3. Boan News, 2022.03.07., (<https://www.boannews.com/media/view.asp?idx=105264&kind=2>)
4. BBC News Korea, 2021.05.12., (<https://www.bbc.com/korean/international-57073544>)
5. Autonomous Vehicle Security Model PART1 : Autonomous Vehicle and Service, 2020.12, KISA
6. Autonomous Vehicle Security Model PART2 : Cyber Security Management System, 2021.12 , KISA
7. Autonomous Vehicle Security Model PART3 : Software Update Management System, 2022.12, KISA
8. YONHAP NEWS, 2020.12.09., (<https://www.yna.co.kr/view/AKR20201209073600017>)
9. ZDNET Korea, 2021.05.12., (<https://zdnet.co.kr/view/?no=20210512154852>)

# Introduction to risk management-based cybersecurity framework

Source : Jaeyeon Lee, Cyber Battlefield Team of Hanwha Systems  
 Editor : LIM, Jeoungkyu, Korean Register

## Overview

As UR E26, the international regulation of International Association of Classification Societies (IACS), begins in July 2024, preparations for the application and certification of cybersecurity solutions for ships are in full swing. Now, in order to strengthen cyber resilience during the life cycle (design, construction, commissioning, and operation), ships must be certified at the basic ship inspection that they have policies for management of the ship's CBS(Computer based system) and recovery. Although this regulation requirements based on the minimum goals for ship cybersecurity[1], and the requirements are gradually becoming more specific through revisions to regulatory documents[2], risk management-based cybersecurity requirements are still ambiguous regulation that is not standardized.

In this article, in order to understand risk management-based cybersecurity design, NIST's Cyber Security Framework and RMF (Risk Management Framework) is introduced in addition to UR E26. Through this, it is a guideline that is commonly applied to risk management-based cybersecurity design not only for ships, but also for finance, national important facilities, and national defense, and provides information to understand ship cyber resilience and UR E26 through application cases in other domains.



Fig 1 Cyber risk management-based framework and regulations

## ● Domestic and International Trends in Smart Ship Cybersecurity

Cyber resilience, defined in the UR E26 regulation, refers to the ability to reduce and mitigate the occurrence of cyber incidents resulting from disruption or damage to operational technology (OT) used for the safe operation of ships [3]. Here, the keywords “reduce and mitigate” can be seen as the core of cyber resilience. If all cyber threats that occur are “completely eliminated,” the cyber safety of the ship will naturally increase, but this activity should not have a serious impact on the achievement of the ship’s operational purpose and safe operation. Conversely, even if a cyber threat occurs, if it does not have a serious impact on the safe operation of the ship, response and recovery priorities may be lowered.

The UR E26 regulation consists of 5 requirements and 17 detailed requirements, but from a cyber risk management perspective, the 5 requirements can be interpreted into 5 risk management stages. In Step 1, managing the CBS inventory is basic for safe operation of the ship. To identify which CBS are important among these, a Cyber Risk Assessment based on Confidentiality-Integrity-Availability must be performed to prioritize CBS for threats.

Step 2, Protect, must be protected hierarchically by dividing it into network and CBS. ‘Security zone setting’, ‘network protection safety devices’, ‘network access control’, ‘wireless communication’, and ‘remote access control’ are related to network protection, and ‘protection from malicious

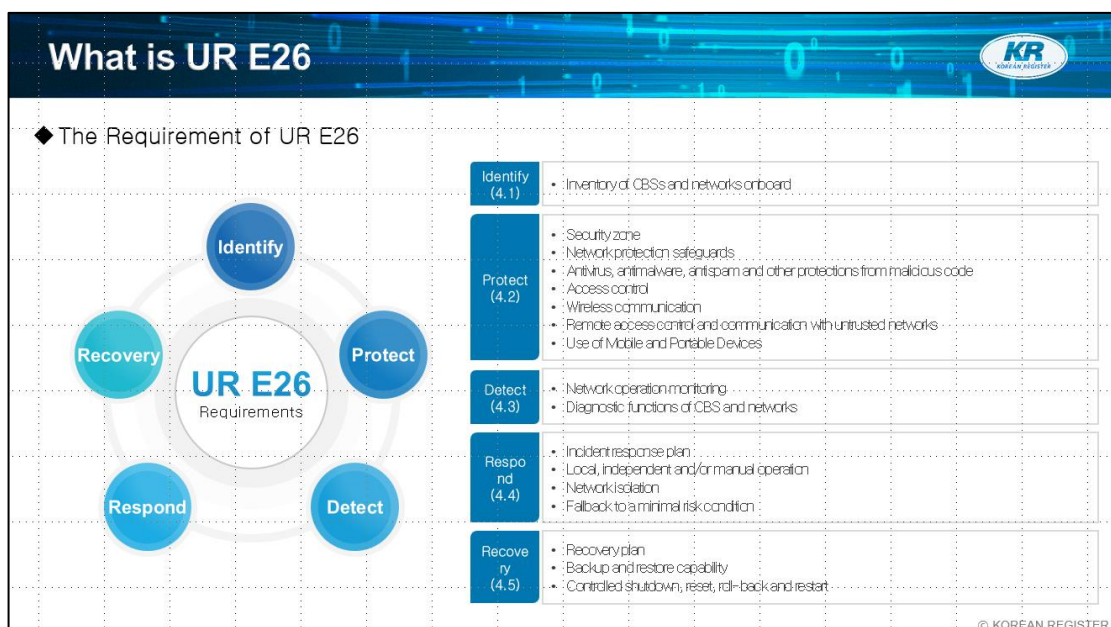


Fig 2 IACS UR E26 Requirements [4]

code' and 'CBS access' 'Control', 'Use of mobile and portable devices' are protected items for CBS. If cybersecurity solutions cannot be technically applied to all CBSs, cyber risks must be mitigated through physical and managerial measures.

Step 3 detect requires monitoring the operating network and monitoring the status of the CBS and network to check whether cyber threats have occurred or are operating in a normal state. Since condition monitoring must be done using limited ship resources, monitoring items, condition monitoring cycle, reporting information, etc. must be determined according to the CBS priority-based management policy.

In Step 4 Respond, and Step 5 Recovery, response and recovery policies must be established based on the results of the cyber risk assessment performed in Step 1 [3]. While steps 1 to 3 focused on technical functions, UR E26 regulations also require response and recovery to document policy. In the response phase, incident response plans, local/manual operation plans, network isolation, return to minimum risk, etc. are all policies that cannot be written without a sufficient understanding of the ship's CBS and network, and ship operations.

Level 5 already requires policies for planning, backup, and controlled system reset and restart to restore the CBS to an operational state for safe operation of the ship after a cyber incident occurs. In stages 4 and 5, it is especially important to conduct a ship risk assessment through collaboration between ship experts and cybersecurity experts, and the policy established as

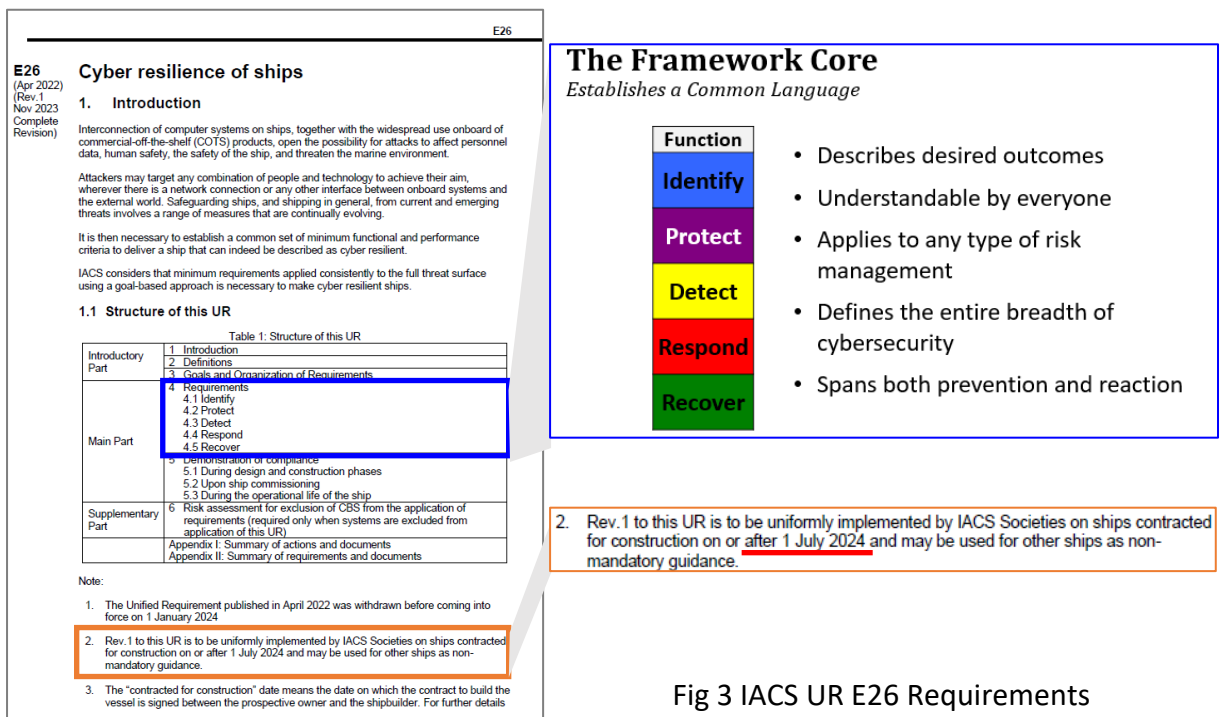


Fig 3 IACS UR E26 Requirements

a result must be documented and submitted at the time of basic inspection, so a ship cyber security solution that satisfies UR E26.

This is considered the biggest reason why it cannot be easily developed. This is because existing enterprise-based cybersecurity solutions are not optimized for the ship environment, and because ships have little experience applying cybersecurity solutions, they face difficulties in installation and operation. However, starting in 2024, ships equipped with the solution are certified, technical and management experience is accumulated, and the system becomes standardized, and ship cybersecurity technology is expected to quickly stabilize.

## ● NIST Cyber Security Framework

The NIST Cyber Security Framework (CSF), a guideline for mitigating cybersecurity risks, was released in version 1.0 in 2014 and version 1.1 in 2018, and is currently in the process of collecting opinions for version 2.0. The framework was initially developed to focus on industries essential to national and economic security, including energy, finance, telecommunications, and the defense industrial base, but has since expanded to include large and small businesses and organizations across all industry sectors, as well as federal, state, and local governments. It is being used so widely that it has been evaluated as having proven to be flexible enough to be voluntarily adopted [5].

Version 1.1 has 5 functions, 23 categories, and 108 subcategories, and is based on risk assessment [6]. Risk assessment (ID.RA) is included in the identification step and guides you to perform a risk assessment that takes into account the organization's operations.

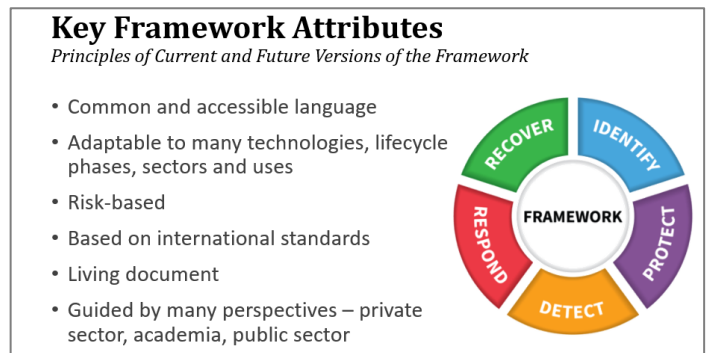


Fig 4 NIST Cyber Security Framework[6]

As one of the profiles of CSF version 1.0, in January 2023, the U.S. Coast Guard released the Maritime Cybersecurity Assessment and Annex Guide (MCAAG) [7]. Cybersecurity vulnerabilities were voluntarily identified and facility protection was defined based on CSF. The scope of cybersecurity management was defined to include ships and port facilities, and cybersecurity levels were divided into three levels to facilitate the application of cybersecurity technology in each phase.



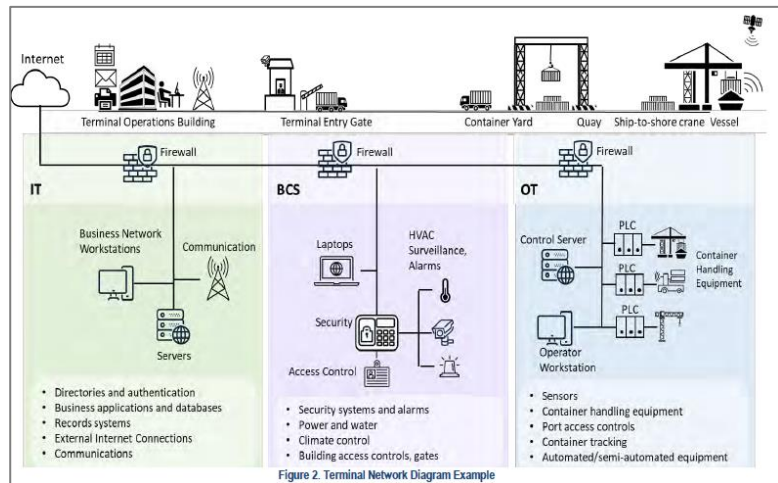
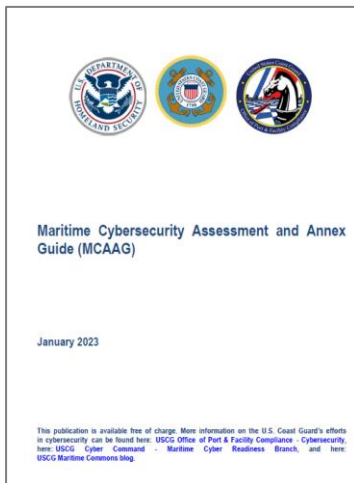


Fig 5 Maritime Cybersecurity Assessment And Annex Guide(MCAAG)

## ● RMF(Risk Management Framework)

The U.S. federal government has defined the framework for risk management guidelines that protect computers and networks as RMF (Risk Management Framework), and is using a systematic and structured risk management process that includes the system development life cycle [8]. RMF is continuously being researched and updated not only in the defense field but also in fields related to finance, corporate networks, and AI, and in revision 2, it consists of a total of 7 stages (preparation, classification, selection, implementation, evaluation, authorization, and monitoring).

1. Prepare: essential activities that an organization must prepare for risk management
2. Categorize: classifies system and information based on impact analysis
3. Select: protect Your System with Security requirement set
4. Implement: describe and document how the control will be implemented and deployed
5. Assess: evaluation to check functional implementation against requirements
6. Authorize: approval for system operation based on risk-based decisions
7. Monitoring: continuous monitoring of risks to the system

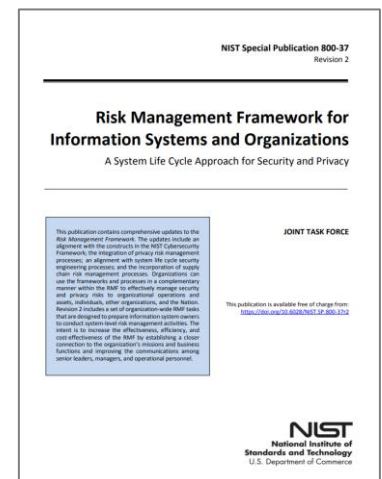


Fig 6. NIST RMF Rev2 [9]

The RMF process detects and responds to risks early from an organizational perspective, and enables overall management of future recurrence prevention and risk mitigation. In the case of

national defense, defense against cyber threats is carried out through the application of RMF processes and technologies, and it includes more requirements and management processes than the NIST Cyber Security Framework introduced in the previous chapter.

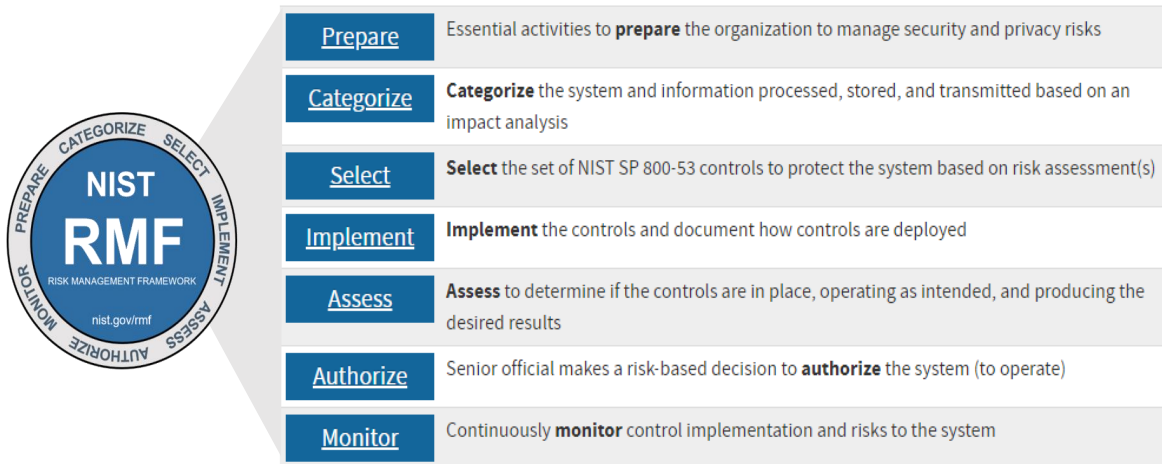


Fig 7. NIST RMF v2.0 7 Steps

## ● Closing

As systems within ships become increasingly integrated and digitized, and remote control and connectivity with networks gradually increase, the cyber safety of ships can be guaranteed by only applying piecemeal technologies, such as controlling external networks or detecting and removing specific malicious codes. In preparation for the rapid increase in human and material damage caused by cyber threats in ships and ports, and the maritime sector, the IACS has announced cybersecurity requirements as mandatory requirement for ships since 2024. UR E26 and E27 requirements are not limited to the application of cybersecurity technology within ships, but also include the organization's cybersecurity policy through risk management, so all stakeholders in the maritime sector, including shipping companies, ship owners, shipyards, and equipment companies, You need to understand their cybersecurity.

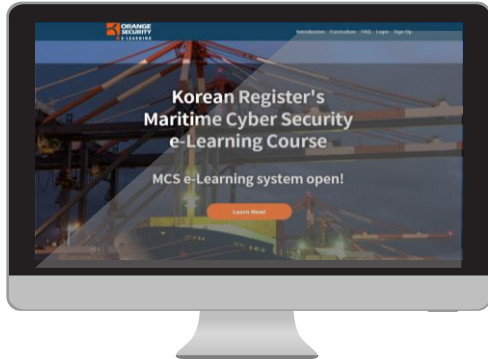
In this paper, we introduced NIST CSF and RMF, which are the basis of UR E26 and 27 regulations, to improve understanding of cybersecurity and risk management and to strengthen maritime cyber safety. Since the scope of application for maritime cybersecurity is reflected not only in the private sector but also in government policies, it is expected that cyber safety in the maritime sector will continue to be strengthened in the future.

## ● References

1. <https://iacs.org.uk/news/iacs-adopts-new-requirements-on-cyber-safety/>
2. <https://iacs.org.uk/resolutions/unified-requirements/ur-e>
3. Cyber Resilience of Ships, IACS UR E26 Rev1 Nov 2023 Complete Revision.
4. [https://www.krs.co.kr/kor/BBS/BF\\_View.aspx](https://www.krs.co.kr/kor/BBS/BF_View.aspx)
5. <https://www.nist.gov/news-events/news/2018/04/nist-releases-version-11-its-popular-cybersecurity-framework>
6. <https://www.nist.gov/cyberframework/framework>
7. <https://www.dco.uscg.mil/Our-Organization/Assistant-Commandant-for-Prevention-Policy-CG-5P/Inspections-Compliance-CG-5PC-/Office-of-Port-Facility-Compliance/Domestic-Ports-Division/cybersecurity/>
8. <https://csrc.nist.gov/projects/risk-management/about-rmf>
9. <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf>

## Online Training

# KR Maritime Cybersecurity e-Learning Center training course



Q&A : <https://edu.orangecq.com/>

KR reorganized the cyber security e-learning training in cooperation with Orange Security, who is a maritime cyber security specialist. Through this reorganization of e-learning training, KR becomes to provide customized training for each customer.

New curriculum consists of Maritime cyber security Awareness, cyber security Practical Management, cyber security Officers and cyber security Type Approval. Maritime cyber security Awareness is a course to raise awareness of maritime cyber security for employees including crews, which includes two modules - Understanding of Maritime Cyber Security and Practice of Maritime Cyber Security. cyber security Practical Management is a course for ship officers and engineers, which includes KR Remote Cyber Survey as well as Maritime cyber security Awareness course. cyber security Officers is for the person in charge of managing cyber security system and responding classification cyber security survey. This course consists of Administrative Security, Cyber Asset, Threat and Technical Security, Understanding of Maritime Cyber Security Risk Assessment with all modules in cyber security Practical Management. Finally, KR Cyber Security Type Approval is a course for equipment company and provides introduction of international standard related to requirements of cyber security for equipment and materials required for obtaining KR cyber security type approval.

KR CS++

## KR Cybersecurity training tool



No.	Titles
1	Understanding of Maritime Cyber Security
2	Practice of Maritime Cyber Security
3	Administrative Security
4	Cyber Asset, Threat and Technical Security
5	KR Cyber Security Type Approval
6	Understanding of Maritime Cyber Security Risk Assessment
7	KR Remote Cyber Survey

KR launched KR CS++, maritime cybersecurity training tool.

KR CS++ was produced in USB type and tablet type for effective cybersecurity training of seafarers in an environment where cybersecurity training is difficult due to the unstable Internet environment on ships. In addition, KR is striving for customer satisfaction by providing various types of services.

Currently, the same service is provided through cybersecurity e-learning education.



*Providing the best services, Creating a better world*

Cyber Certification Team, Korean Register  
(46762) 36, Myeongji ocean city 9-ro, Gangseo-gu, Busan Republic of Korea  
Tel +82 70 8799 8595  
Fax +82 70 8799 8594  
[www.krs.co.kr](http://www.krs.co.kr)

Copyright © 2023 ALL RIGHTS RESERVED BY KOREAN REGISTER