

KR Maritime Cyber Safety News & Report



Vol. 050
June. 2022



CONTENTS

KR Activities

- KORMARIME CONFERENCE 2022, Presentation of "Maritime Cybersecurity Trends"

Maritime Cyber Safety News

- IACS issued recommendation on incorporating cyber risk management into SMS
- USCG on cyber security awareness and action

Cyber Security Expert Column

- COONTEC Co., Ltd. : Ship Supply Chain Security Management Plan

Advertisement

- KR Cyber Security Training Tool & E-LEARNING



Maritime Cybersecurity Trends - IACS UR KORARINE CONFERENCE 2022

By Ahn, Jong-woo, Senior Surveyor, Korean Register

Ahn Jong-woo, Senior Surveyor, made a presentation on maritime cybersecurity trends at the KORMARINE Conference 2022 held at Songdo Convensia in Incheon on June 22, 2022.

In this session, He gave a detailed introduction to UR E26 and E27, the Unified Requirements (UR) related to ship cyber security, which were newly published in April 2022 by the International Association of Classification Societies (IACS). It was introduced that cyber security is no longer an option in the shipbuilding and offshore industry, but a mandatory rule from ships contracted for construction in January 24, when the common rules took effect. The KR announced that it would carry out verification work for the new UR through cooperation with domestic shipyards and shipbuilding equipment manufacturers before the effective date of this UR. On the other hand, KORMARINE Conference 2022 was held as an online and offline hybrid, and about 300 people attended the site, and it is said that about 500 people participated in live online broadcast in real time.



IACS Publication News

Recommendation on incorporating cyber risk management into Safety Management Systems

* Detailed analysis of this recommendation will be published from the July, 2022 issue

The IACS issued a recommendation on incorporating cyber risk management into safety management system(SMS) in May 2022. This Recommendation proposes a methodology for the stakeholders of ships in operation to achieve cyber risk assessment, and states that ship cyber risk assessment according to this methodology is not mandatory. Detailed information can be found on the IACS website.

. (<https://iacs.org.uk/publications>)

No. 171
(May 2022)

Recommendation on incorporating cyber risk management into Safety Management Systems

1 Foreword

IMO has decided that cyber security shall be handled in accordance with the existing objectives and functional requirements of the ISM Code. Companies (DOC holders) should use their existing Safety Management Systems (and SMS measures) to assess risks and implement safeguards and otherwise handle cyber security.

IMO defines risk as: "The combination of the frequency and the severity of the consequence." (MSC-MEPC 2/Circ.12/Rev.2). In other words, risk has two components: likelihood of occurrence and severity of the consequences.

The goal of this Recommendation is to focus only on risk assessment and risk management.

It is important to utilize the opportunity to strengthen the overview of IT and OT critical systems on board and to use risk assessments to implement appropriate safeguards and implement measures likely to lower risk to an acceptable level.

Implementing efficient measures needed for maritime cyber risk management in safety management systems is paramount, and will be helped by this recommendation. Readers are invited to turn to the following documents which describe in a simple and complete way all the rules and good practices to use in order to effectively manage the field of embedded cyber security.

- MSC-FAL 1/Circ.3 "Guidelines on maritime cyber risk management"
- "The Guidelines on Cyber Security onboard ships" produced and supported by BIMCO, Chamber of Shipping of America, Digital Containership Association, International Association of Dry Cargo Shipowners (INTERCARGO), InterManager, International Association of Independent Tanker Owners (INTERTANKO), International Chamber of Shipping (ICS), International Union of Marine Insurance (IUMI), Oil Companies International Marine Forum (OCIMF), Superyacht Builders Association (Sybass) and World Shipping Council (WSC)
- BIMCO "Cyber Security Workbook for on board ship use"

These guidelines provide high-level recommendations for maritime cyber risk management that can be incorporated into existing risk management processes and are complementary to the safety and security management practices established by this International Maritime Organization.

2 Introduction

2.1 Purpose of the recommendation

2.1.1 Risk analysis is one of the foundations of any risk management. Cyber security risk management is no exception. Therefore the main purpose of this document is to propose a method to guide stakeholders on the achievement of a cyber risk assessment for ships in service.



Maritime Cybersecurity News Scrap

USCG on cyber security awareness and action

Source : www.hstoday.us

The U.S Coast Guard Assistant Commandant for Prevention Policy has published [Marine Safety Information Bulletin 02-22](#) “Cybersecurity Awareness and Action”. The Coast Guard continues to monitor world events and their potential impact on the Marine Transportation System (MTS).

CISA’s [“Shields Up” website](#) remains the primary location for information and recommendations for adapting a heightened cybersecurity posture, and we highly encourage all MTS stakeholders to visit the site regularly for updates and reminders.

The Coast Guard fully supports this guidance and stands ready with our partner agencies to respond to these reports. Considering the heightened risk, stakeholders should closely monitor their computer systems, telecommunications systems, and networks for suspicious activity and breaches of security and, when in doubt, report to the National Response Center (NRC). Maritime Transportation Security Act (MTSA) regulated vessels and facilities *are required*, and other MTS stakeholders are encouraged, to report breaches of security or suspicious activity to the NRC at 1-800-424-8802. [The CG-5P Policy Letter 08-16, Reporting Suspicious Activity and Breaches of Security](#) provides additional guidance on the reporting of cyber incidents.

The Coast Guard continues to review policies, procedures, and guidance to address the evolving nature of cyber risk management. The Coast Guard published [Navigation and Vessel Inspection Circular \(NVIC\) 01-20: Guidelines for Addressing Cyber Risks at Maritime Transportation Security Act \(MTSA\) Regulated Facilities](#), as well as a [Vessel Cyber Risk Management Work Instruction](#), to assist stakeholders in incorporating cybersecurity into facility and vessel security assessments and plans. Additionally, in ports across the country, Area Maritime Security Committees (AMSC) serve as a key resource for local, state, federal and private entities to engage on information sharing, best practices, and port safety and security. We will continue to leverage these committees to address cyber risks in the MTS.



Cybersecurity expert column

Management of Ship Supply Chain Security

By Bang Joon-hyuk, CEO, Coontec Co., LTD

● Cybersecurity Threats in the Shipping Industry

Innovative technologies are being implemented as ICT technology is introduced in traditional industrial fields such as manufacturing and automobiles. The ship industry is no exception. With the introduction of ICT technology in the ship industry, new technologies such as smart ships, autonomous ships, and fully autonomous ships are developing. As advanced information and communication technologies are being combined, software and network systems that are the basis of advanced technologies are becoming more complicated, and as a result, various cyber risks targeting the ship industry are increasing.

● Importance of Supply Chain Security Management

In the event of a cyber attack on a ship, it can lead to a major accident that goes beyond simple confidential data capture. Since marine accidents are generally considered to be about six times more dangerous than road traffic accidents, it is important to check the function of ships as well as check security to prevent such marine accidents in advance.

Cybersecurity threats that can lead to ship accidents are occurring in various fields in the IT and OT fields. In the case of IT security, it is directly related to supply chain security depending on the complexity of each component and software constituting the ship. Supply chain attack is a concept that contrasts with direct attacks on specific companies and institutions and refers to types of attacks that penetrate the internal assets of a company through various suppliers such as external partners and partners with relatively poor security management. Such supply chain attacks are on the rise as the supply chain, which receives each product and software from various global suppliers and releases one completed product, becomes more complex.

● Importance of Supply Chain Security Management (Cont.)

As mentioned above, as ICT is applied to ship-related technologies, software supply chains are becoming more complex and diversified, so ship supply chain security management is also important. However, since it is impossible to manually identify and manage all the components of the software that make up the ship, it is essential to create an SBOM for effective software management and to utilize an automated platform that can check for software and vulnerabilities based on that SBOM.



● Process for Ship Supply Chain Security Management

- ① Analyze the software components that make up the ship
- ② Creating a SBOM(Software Bill of Materials) for each component
- ③ SBOM-based open source security management with open source management tools
- ④ Binary analysis tool checks for binary vulnerabilities to components
- ⑤ Continuous monitoring and inspection of the entire SBOM

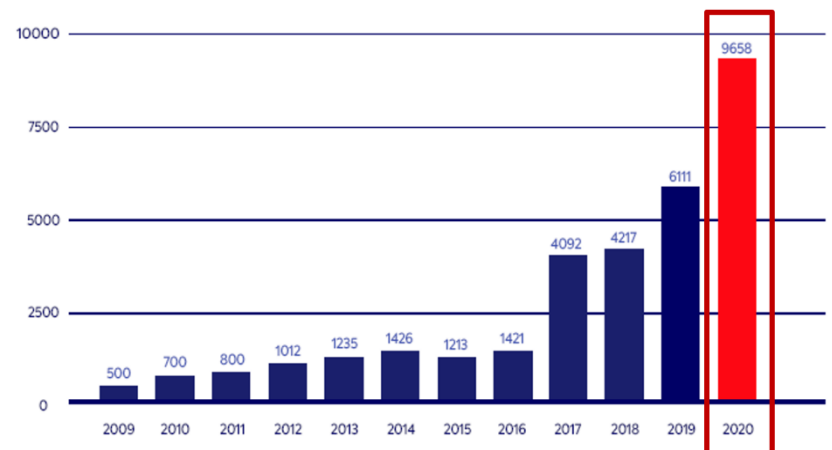
To manage supply chain security in the ship industry, it is essential to fully identify and analyze the software components that make up the various devices used on the ship. This is because, in situations where visibility into components is not secured, it is impossible to evaluate security threats that can threaten the ship itself, as well as to establish necessary checks and countermeasures.

● Process for Ship Supply Chain Security Management (Cont.)

After the analysis of the system software components of the ship has been conducted, the SBOM(Software Bill of Materials) shall be created to manage each component. SBOM provides details of various software-related components such as libraries and modules, which can identify the dependencies between software components, effectively correcting and mitigating security incidents based on SBOM if certain vulnerabilities are found. Through this SBOM, transparency in ship software can be secured and vulnerabilities can be tracked quickly and accurately.

At this time, SBOM should also include information related to open source software, which has recently been rapidly introduced, and it is important to manage vulnerabilities that can be missed by source code analysis through binary analysis tools. Let's learn about open source and binary management, which plays a key role in managing supply chain security.

● Open Source Software Management



<Trend of annual occurrence of open source vulnerabilities>

For the security management of the ship's software supply chain, it is important to thoroughly manage open sources based on SBOM. In the case of open source, which is rapidly increasing in use due to the reduction of time and cost of software development, it is easy to target malicious cyber attacks as the source code is disclosed, and open source vulnerabilities are rapidly increasing.

● Open Source Software Management (Cont.)

Open source is complexly linked to each software component, making it impossible to manually analyze dependencies and usage. In order to strengthen supply chain security by managing open source security, it is essential to accurately analyze each software component and introduce an automated platform that can quickly detect open source security vulnerabilities.

Introducing an automated platform for vulnerability management can quickly detect vulnerabilities in the open source components of the ship and quickly apply appropriate fixes to them, preventing software supply chain attack threats.

- **Enhanced security with binary analysis**

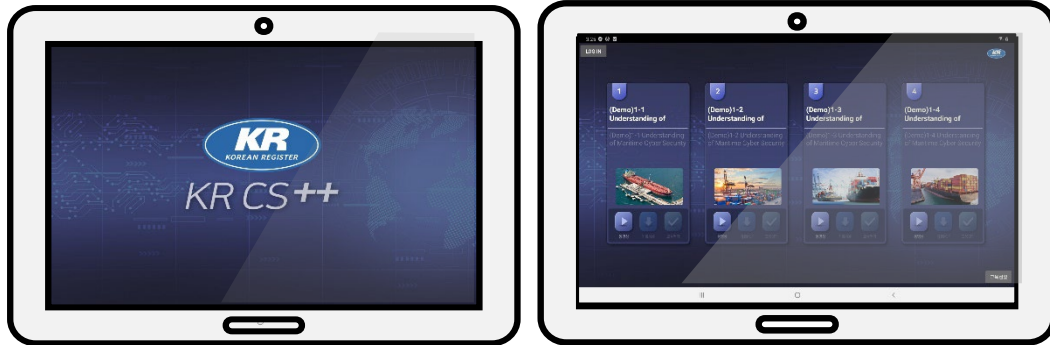
<SBOM management through binary analysis>

In addition to source code-based open source management, the SBOM of the ship can be managed through binary analysis to manage the security hole. When a platform for binary analysis is introduced, it is possible to identify the hardware and software components that make up the vessel, thereby evaluating the actual impact of the vulnerability on the vessel.

As ICT technology being applied to the ship industry is being advanced and diversified, continuous monitoring based on SBOM generated through binary inspection will identify known and unknown vulnerabilities in real time to prevent damage caused by cyber attacks.

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.

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.



Providing the best services, Creating a better world

Cyber Certification Team, Korean Register

46762 부산광역시 강서구 명지오션시티 9로 36 (명지동)

(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

Copyright © 2022 ALL RIGHTS RESERVED BY KOREAN REGISTER