

KR Maritime Cyber Safety News & Report



Vol. 055
Nov. 2022



CONTENTS

KR Activities

- KR, CIRM Conference Cyber Security Presentation
- KR, G-NAOE 2022 Cyber Security Presentation

Maritime Cyber Safety News

- US: Cybersecurity performance goals for critical infrastructure
- USCG: Be aware of typosquatting of port facility websites

Maritime Cyber Security Expert Column

- Secure Development Lifecycle (SDLC) for onboard equipment

Advertisement

- KR Cyber Security Training Tool & E-LEARNING

KR, CIRM Conference Cyber Security Presentation

Editor : LIM Jeoungkyu, Korean Register

Korean Register was invited to the annual conference of Comité International Radio Maritime (CIRM) held in Malta on October 18th to present cyber security trends (IACS UR E26, E27) and technology development status for autonomous ships. (Presentation: Lim Jeoung-kyu, Senior Surveyor)

Through the presentation, the need to respond to cyber security for equipment and equipment companies and ship owners was emphasized, and Korean Register's role and technology as a technical advisor were promoted at the booth. In particular, the training video implemented on a tablet PC received great acclaim as it could be easily used as a tool to increase awareness of maritime cyber security awareness among the employees in the maritime industry, including seafarer.

CIRM is a consultative body composed of 120 companies such as Wartsila, Inmarsat, JRC, and Furuno to research/review issues related to maritime radio communication technology and operation, and is conducting related standardization activities at international organization such as IMO, IEC, and ITU.



KR, G-NAOE 2022 Cyber Security Presentation

Editor : AHN Jongwoo, Korean Register

KR held cyber security announcement at the G-NAOE(Global Conference on Naval Architecture and Ocean Engineering) 2022 from November 8 to 9. G-NAOE is designated as the biennial international conference to provide opportunities for communication and cooperation to actively lead the post-pandemic era with an adaption of 4th industrial revolution technology toward zero-carbon ocean among academia, research industries, classification, and authorities. At the G-NAOE 2022, KR presented the themes ‘A Risk Based Approach of Cyber Secure by Design for Newbuilding Ship’ and ‘Maritime Cyber Security - International Response against cyber attack.’

In the first topic, LIM Jeoungkyu, the senior surveyor, introduced the cyber security guidelines (IACS UR E26, IEC 62443-3-3, IEC 62443-4-1) and proposed a risk-based approach to cyber security by designing new ships to protect IT and OT systems against comprehensive cyber attack. Each system can achieve cyber design security by implementing IACS UR E26, IEC 62443 Security Level requirements based on the level of risk.

In the second topic, AHN Jongwoo, the senior surveyor, introduced the definition of autonomous vessel level presented by IMO, analyzed cyber security guidelines published in the maritime sector, and presented the guide for developing cyber security guidelines for MASS, which are based on IACS UR E26. In the presentation, he said the part of requirements were introduced, but additional requirements will be further identified when research on autonomous ships is conducted in the future.



KR actively participates in domestic and foreign conferences to provide stakeholders such as academia and industry with the latest cybersecurity status and ship cybersecurity projects underway at KR.

US: Cybersecurity performance goals for critical infrastructure

Source : SAFETY4SEA

The US Department of Homeland Security released the Cybersecurity Performance Goals (CPGs), voluntary practices that outline the highest-priority baseline measures businesses and critical infrastructure owners of all sizes can take to protect themselves against cyber threats.

The CPGs were developed by DHS, through the Cybersecurity and Infrastructure Security Agency (CISA), at the direction of the White House. Over the past year, CISA worked with hundreds of public and private sector partners and analyzed years of data to identify the key challenges that leave our nation at unacceptable risk.

By clearly outlining measurable goals based on easily understandable criteria such as cost, complexity, and impact, the CPGs were designed to be applicable to organizations of all sizes.

CISA developed the CPGs in close partnership with organizations across government and the private sector. The resulting CPGs are intended to be implemented in concert with the NIST Cybersecurity Framework. The CPGs prescribe an abridged subset of actions to help organizations prioritize their security investments.

Cybersecurity Performance Goals

1. Account security:

- Detection of Unsuccessful (Automated) Login Attempts;
- Changing Default Passwords;
- Multi-Factor Authentication (MFA);
- Minimum Password Strength;
- Separating User and Privileged Accounts;
- Unique Credentials;
- Revoking Credentials for Departing Employees.

2. Device security:

- Hardware and Software Approval Process;
- Disable Macros by Default;
- Asset Inventory;
- Prohibit Connection of Unauthorized Devices;
- Document Device Configurations.

3. Data security:

- Log Collection;
- Secure Log Storage;
- Strong and Agile Encryption;
- Secure Sensitive Data.

4. Governance and training:

- Organizational Cybersecurity Leadership;
- OT Cybersecurity Leadership;
- Basic Cybersecurity Training;
- OT Cybersecurity Training;
- Improving IT and OT Cybersecurity Relationships.

5. Response and recovery:

- Incident Reporting;
- Incident Response (IR) Plans;
- System Back Ups;
- Document Network Topology.

USCG: Be aware of typosquatting of port facility websites

Source : SAFETY4SEA

Malicious cyber actors continue to spoof U.S. port facility domains using typosquatting techniques in attempts to re-direct users to malicious websites that have similar domain names.

* Typosquatting is a type of social engineering attack which targets internet users who incorrectly type a URL into their web browser rather than using a search engine.

Malicious cyber actors are not directly targeting port facilities, rather, they are targeting individuals who incorrectly type a website address. Misspellings of several U.S. port facility domains have recently been registered, likely for malicious purposes.

These events have been analyzed and investigated, and the following are recommendations for MTS stakeholders:

- 1. Mitigate the Opportunity for Attacks :** Typosquatting Deterrence – Organizations may intentionally register similar domains to their own to deter adversaries from creating typosquatting domains. Other facets of this technique cannot be easily mitigated with preventive controls since it is based on behaviors performed outside of the scope of enterprise defenses and controls.
- 2. Detection Methods :** Consider use of services that may aid in tracking of newly acquired domains, such as WHOIS databases and/or passive DNS. In some cases it may be possible to pivot on known pieces of domain registration information to uncover other infrastructure purchased by the adversary. Consider monitoring for domains created with a similar structure to your own, including under a different TLD.
- 3. Untrusted Traffic :** Treat all traffic transiting your network – especially third-party traffic – as untrusted until it is validated as being legitimate.
- 4. Third Party links :** Avoid clicking on links from third parties. Where possible, enter the correct address of the respective website manually in your browser or open it via your bookmarks.

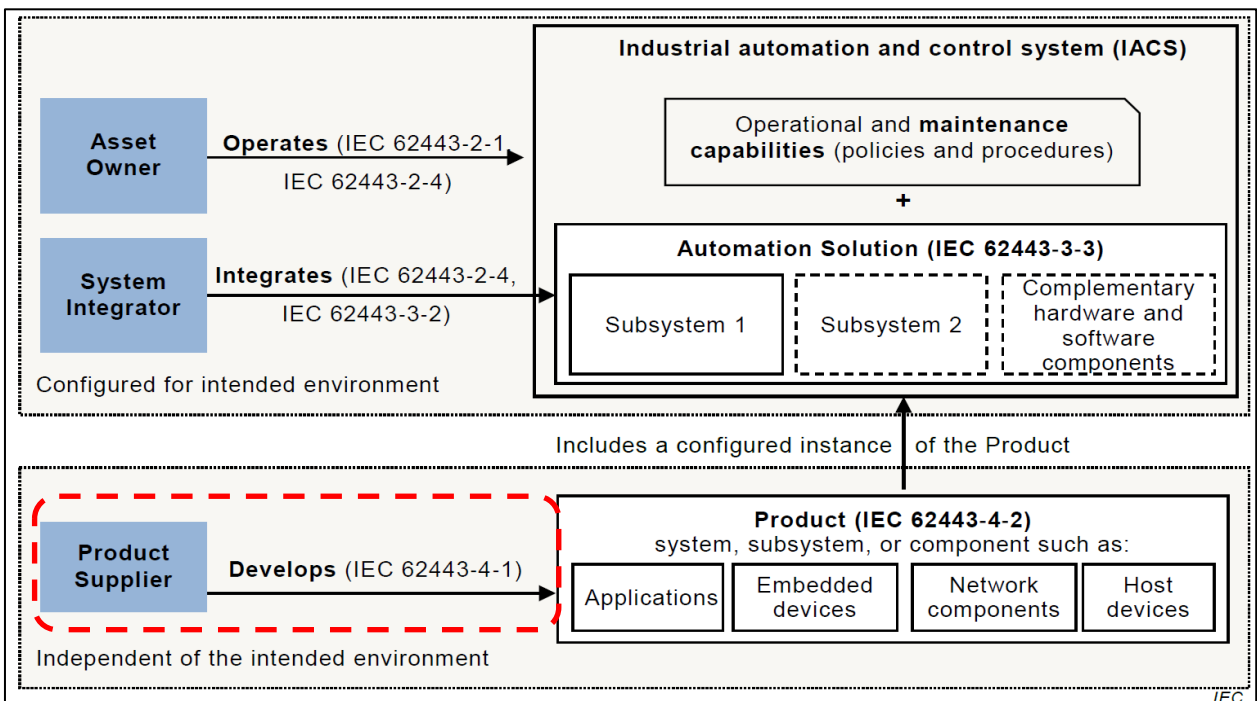
Secure Development Lifecycle (SDLC)

Editor : CHOI Sanghoon, Korean Register

IACS(International Association of Classification Societies) issue UR(Unified Requirements) E27 in April of this year and it includes requirements for cyber resilience of on-board systems and equipment. Among these requirements, there are SDLC(Secure Development Lifecycle) requirements that manufacturers of systems and equipment should apply throughout the entire product life cycle from development to maintenance.

The secure development life cycle is defined in international standard IEC 62443-4-1, which are applied to cyber security of OT systems and covers the process for secure development of products, that is, the requirements for procedures.

As shown in the figure below, the functional requirements of cyber security for systems and devices are respectively covered in IEC 62443-3-3 and IEC 62443-4-2 while the SLDC requirements for the manufacturer's product development process are covered by IEC 62443-4-1. In this regards, UR E27 refers to 7 requirement for SDLC.



< Example scope of product life-cycle (source : IEC 62443-4-1)>

According to UR E27, seven security development lifecycle requirements for manufacturers supplying onboard systems and equipment are as follows.

1. Procedures and technical controls to protect private keys used for code signing

Procedures and technical controls should be in place to protect private keys used for code signing from unauthorized access or alteration. And there should be a QA process for testing updates prior to release.

2. Procedures for providing product security update guide documents

Guidance documents should include product version numbers, instructions on how to apply a patch and its impact, and how to verify that a patch has been applied.

3. Procedures for providing documentation to ensure dependent component/OS security updates

A process should be adopted to ensure that documentation for dependent components or operating system security updates is available to users and should be specified for compatibility with the product.

4. Procedures for ensuring availability of security updates for products

A process should be adopted to ensure that security updates for all supported products and product versions are available to users in a way that makes it easy to verify that security patch is authentic.

5. Procedures for generating documentation outlining a security-in-depth strategy to support installation, operation and maintenance.

The defense-in-depth strategy should include the security features and roles implemented by the product, the threats considered and the product's user mitigation strategy for known security risks.

6. Procedure for providing external environment guidance for products

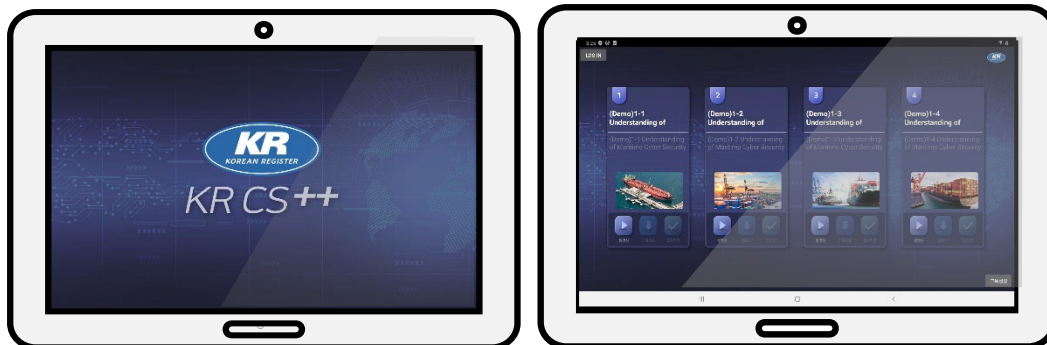
A process for user documentation describing the security-in-depth measures required in the external environment in which the product is used should be adopted.

7. Procedure for providing guidance to ensure product security during installation/maintenance

Examples of contents should be precautions when integrating with other systems, guidelines and recommendations for regular security maintenance activities, etc.

KR CS++

KR Maritime 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) 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