KR Maritime Cyber Security

News from KOREAN REGISTER

Vol. 026

June 2020

KR Cyber Security Activities

- KR signs MOU with SHI to bolster cyber security capabilities
- Cyber Risk Assessment workshop for new shipbuilding project

New security technology applied to Wi-Fi 6

Understanding Cyber Threats(OWASP Top 10 Internet of Things)

Guidelines for Type Approval of Maritime Cyber Security

Explanation of Term

Korean Register signs MOU with SHI to bolster cyber security capabilities of smart ships

Korean Register (KR) has signed a Memorandum of Understanding (MOU) with Samsung Heavy Industries (SHI) to conduct a joint study on “Ship Cyber Security Network Construction and Design Safety Evaluation” at the Marine Engineering Research Center of SHI.

Under the MOU, the two organizations have agreed to evaluate the construction and design safety of cyber security networks applicable to new ships. In addition, they will jointly study technologies that can respond to cyber threats faced by ships, by diagnosing ship cyber security vulnerabilities using the cyber security test beds built by SHI. KR and SHI will work together to enhance and support the application and verification of ship cyber security rules.

“Through this joint study with Samsung Heavy Industries, we will strengthen our ship cyber security certification and technical services capabilities. KR will also continue to increase its cyber security technology leadership in the global maritime market through our cooperation and close working with shipyards,” said Kim Dae-heon, head of KR’s Digital Technology Center.

SHI is recognized for its technological prowess as a result of its cyber security certifications received from major shipping companies based on its proprietary smart ship solution, SVESSEL. It is expected that by combining KR’s world-recognized classification capability and the smart ship technology of Samsung Heavy Industries, the resulting synergies will be extremely beneficial to the shipping industry moving forward.

“We expect to considerably increase the security capabilities of smart ships through our joint study with KR, which is renowned for its cyber security certification technology. In addition, we will continue to deliver ships with the very latest world-class cyber security capabilities for our customers,” Shim Yong-rae, head of the Ship & Marine Research Institute of SHI, added. This is what was approved in the press release.

Cyber Risk Assessment Workshop for Newbuilding Ship Project (LPG Carrier, 84,600 CBM)

KR has delivered the first cyber risk assessment workshop for Hyundai LNG Shipping's newbuilding ship project (LPG carrier, 84,600 CBM) with representatives from Hyundai Heavy Industries (HHI) and Korea Shipbuilding & Marine Engineering (KSOE) attending.

Ship Cyber Risk Assessment is an essential activity to verify the feasibility of the cyber security design of the ship's IT/OT system. The assessment uses possible cyber-attack scenarios and cyber-risk levels to identify cyber-threats and vulnerabilities to ship-critical systems and applies technical security measures (firewalls, IPS/IDS, VPN, Anti-virus, communications and data encryption, etc.) to reduce the risk.

In this workshop, the ISO / IEC 27005, NIST 800-39 cyber risk assessment methodology was applied, along with the concept of Zone & Conduit of IEC 62443 (security certification for industrial automation and control systems), an industry cyber security standard. Based on the standards, the ship's network is subdivided into Remote Zone, Control System Zone, Crew LAN Zone, Bridge Zone, and Wireless Zone to evaluate the level of cyber security boundary protection (e.g. proxy, gateway, router, firewall, one-way gateway, guard and encrypted tunnel).

Moving forward, KR will offer a second cyber risk assessment workshop to Hyundai Heavy Industries (HHI), Korea Shipbuilding & Marine Engineering (KSOE), and shipowners (Hyundai LNG Shipping) and related manufacturers. Through this, it will analyze not only the technical security of the ship but also the administrative and procedural security areas of the shipowner.

New security technology applied to Wi-Fi 6

This series will introduce principles and kinds of wireless network widely used in companies, home, and ships. Also, weakness and countermeasures of wireless network. Therefore, this newsletter in February 2020 introduces 'the kinds of wireless network and communication principle'

Series news

① The principles and kinds of wireless networks

② Technical Security Vulnerabilities and Countermeasures of Wireless LAN (WIFI)-1

③ Technical Security Vulnerabilities and Countermeasures of Wireless LAN (WIFI)-2

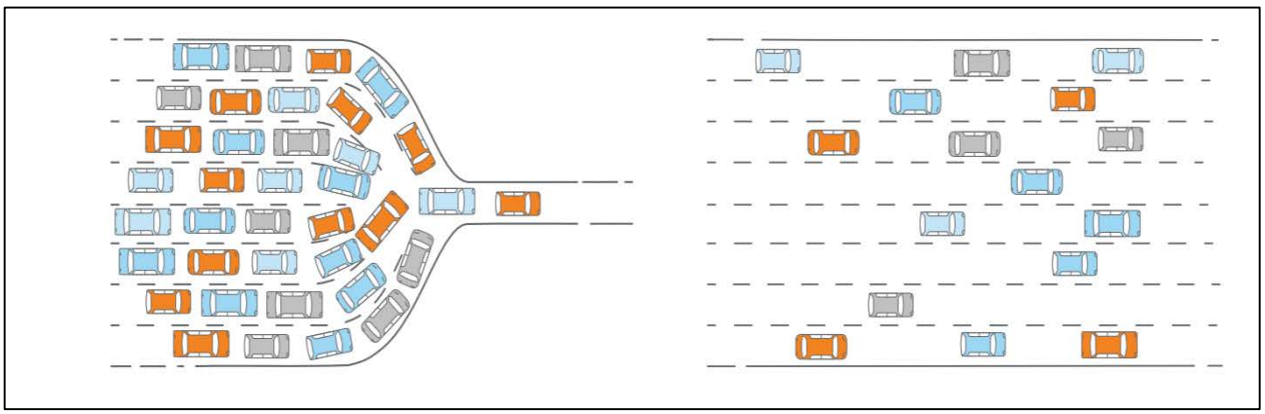
④ **New cyber security technology applied to Wi-Fi 6**

⑤ Technical Security Vulnerabilities and Countermeasures of Other Wireless Networks

⑥ Kinds of maritime wireless communication, technical security vulnerabilities

What is Wi-Fi 6, a new wireless LAN technology?

IN 2018 the IEEE (The Institute of Electrical and Electronics Engineers Standards Association) released the IEEE 802.11ax technical standard which named Wi-Fi 6 by the Wi-Fi Alliance. Wi-Fi 6 has four times the data rate compared to the existing technology (802.11ac) and can use both the 2.4GHz and 5GHz bands. In addition, existing Wi-Fi technology can transmit only one data at a time with OFDM technology, but the OFDMA (orthogonal frequency-division multiple access) technology applied to Wi-Fi 6 means multiple data can be transmitted at the same time. This feature can handle large packets more efficiently, such as streaming HD video, and relatively short packets from IoT devices and voice traffic can be processed more effectively using OFDMA.



Source : 802.11ax(WI-FI 6) introduction, (https://www.arubanetworks.com/ko/products/networking/802-11ax)

Wi-Fi Protected Access 3 (WPA3) technology applied to Wi-Fi 6

The previous newsletter (2020. February to April), covered wireless LAN encryption technology and its vulnerabilities. The WPA3 technology applied to Wi-Fi 6 partially improves the vulnerability of existing WPA2, improving the encryption method and key management technology, and improving security in an open wireless network which is mainly used in public places such as airports. The following table shows the evolution of Wi-Fi security technology

Category	WEP	WPA	WPA2	WPA3
Encryption	RC4	TKIP+RC4	CCMP/AES	GCMP-256
authentication	WEP-Open WEB-Shared	WPA-PSK /Enterprise	WPA2-Personal /Enterprise	WPA3-Personal /Enterprise
Key management	none	4 way-Handshake	4 way-Handshake	ECDH / ECDSA

<The evolution of Wi-Fi security technology>

KRACK attack refers to an attack that does not expose the encryption key itself, but artificially induces a reset of the encryption key in the WIFI network to find out the initial vector used for encryption and to decrypt, falsify, and then forge data.

As shown in the table below, the WPA3 security technology elements can be summarized.

Technical element	Description	Technical element
WPA3 Function	192bit Security Suite	192bit Elliptic Curve Encryption
	SAE / 4 Way-Handshake	Simultaneous identity authentication, KRACK res ponse
	Easy Connect	Simplifying the pairing process
	Wi-Fi CERTIFIED Enhanced Open	OWE-based open network encryption
WPA3 mode	WPA3-Personal Mode	– Individual users mode – Forward Security – Traffic protection in case of password exposure
	WPA3-Enterprise Mode	– Enterprise mode – GCMP-256 encryption – HMAC-SHA384 key – 384bit ECDH, ECDSA key authentication – BIP-GMAC-256 f

<WPA3's security technology>

Understanding Guideline for Type Approval of Maritime Cyber Security

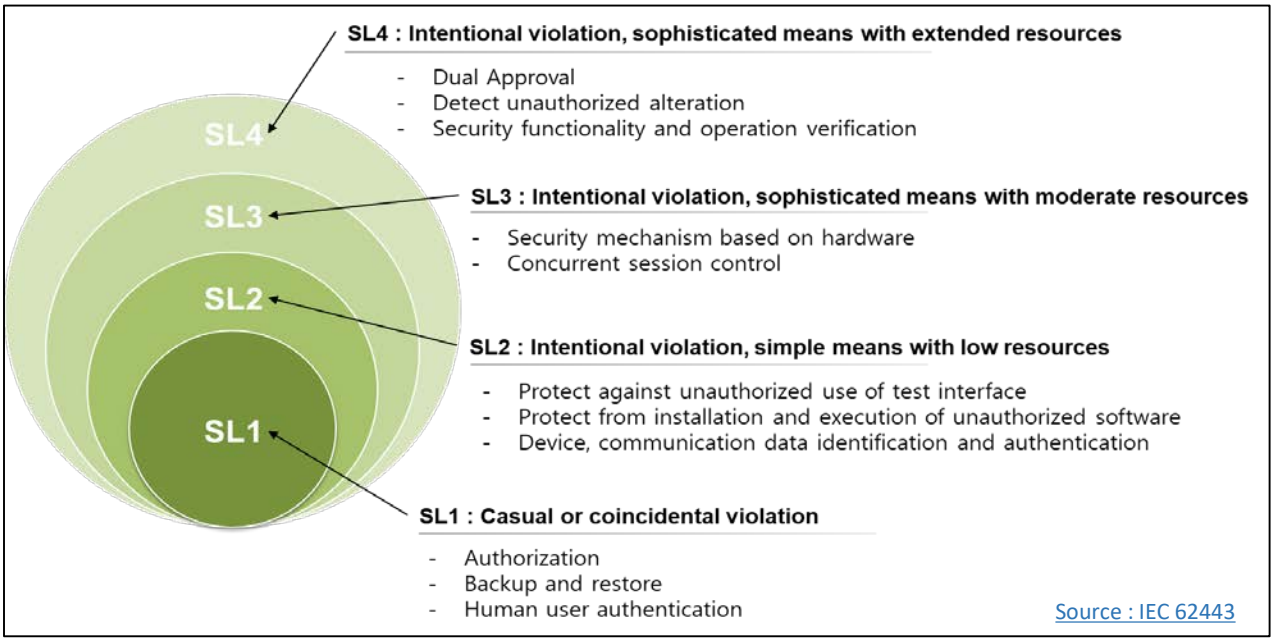
Type approval is to certify for the manufacturers of equipment for marine use that equipment comply with the provisions for the type approved products in the Guidance, where deemed satisfactory by the Society as the results of carrying out the examination, tests and inspection specified in the Guidance before installation on board. The cyber security type approval has been developed based on international standards such as ISA 62443 4-2, IEC 61162-460, and inspect cyber security level and function of cyber systems including remote access equipment, integrated control and monitoring systems on board the ship. The security requirements and their levels are verified on 12 categories and 124 requirements.

< Composition of KR Cyber Security Type Approval Guidelines >

Section 1 General	Section 5 Data Confidentiality	Section 9 Software Application Requirements
Sections 2 Identification and Authentication	Section 6 Restricted Data Flow	Section 10 Embedded Device Requirements
Section 3 Use Control	Section 7 Timely Response to Events	Section 11 Host Device Requirements
Section 4 System Integrity	Section 8 Resource Availability	Section 12 Network Device Requirements

Source : http://www.krs.co.kr/KRRules/KRRules2019/data/data_other/ENGLISH/gc31e000.pdf

Understanding Security Level (SL)



Source : IEC 62443

Lack of Secure Update Mechanism

Unauthorized software and firmware updates are a major threat vector for IoT cyber-attacks. IoT breaches can have physical consequences that result in loss of data and also introduce substantial legal liability and erode brand reputation. The table is the example of security measures for a “lack of security update mechanism” that ENISA recommends.

Domain	Security measure	Referred standards
IT security administration IT security architecture Identity and access management IT security maintenance	Ensure the device software/firmware, its configuration and its applications have the ability to update Over-The-Air (OTA), that the update server is secure, that the update file is transmitted via a secure connection, that it does not contain sensitive data (e.g. hardcoded credentials), and that it is signed by an authorised trust entity and encrypted using accepted encryption methods, and that the update package has its digital signature, signing certificate and signing certificate chain, verified by the device before the update process begins. Failing to build in OTA update capabilities will leave devices exposed to threats and vulnerabilities for the entirety of their lifetimes	・ISO27001 A12. Operations security ・NIST SP 800-53 - SI-7 Software, Firmware, And Information Integrity ・NIST Framework for Improving Critical Infrastructure Cybersecurity ・OWASP I9. Internet of Things Top Ten ・U.S. Department of Homeland Security - Strategic Principles For Securing The Internet Of Things (IoT) ・Cloud Security Alliance (CSA) - Future-proofing the Connected World: 13 Steps to DevelopingSecure IoT Products ・IoT Security Foundation (IoTSF) ・GSM Association (GSMA) ・IoT Security Guidelines- Atlantic Council (Brent Scowcroft Center On International Security) - Smart Homes and the Internet of Things- Online Trust Alliance (OTA) ・IoT Trust Framework and Trust Framework Resource Guide ・BITAG (Broadband Internet Technical Advisory Group) ・Internet of Things (IoT) Security andPrivacy Recommendations Technical Working Group Report ・ARMOUR (Large-Scale Experiments of IoT Security Trust) ・AT&T Cybersecurity Insights ・Exploring IoT Security Volume 2 ・Symantec - An Internet of Things Reference Architecture ・- Symantec - Internet Security Threat Report (ISTR) ・Microsoft - Cybersecurity Policy For The Internet Of Things Etc.
IT security architecture	Offer an automatic firmware update mechanism. Devices should be configured to check for the existence of firmware updates at frequent intervals. Automatic firmware updates should be enabled by default. A device may offer an option to disable automatic firmware updates and require authentication for it.	
IT security architecture	Backward compatibility of firmware updates. Automatic firmware updates should not change network protocol interfaces in any way that is incompatible with previous versions. Updates and patches should not modify user-configured preferences, security, and/or privacy settings without user notification. Users should have the ability to approve, authorise or reject updates.	

Source : ENISA, Baseline Security Recommendations for IoT, NOVEMBER 2017

Understanding Guidelines for Type Approval of Maritime Cyber Security

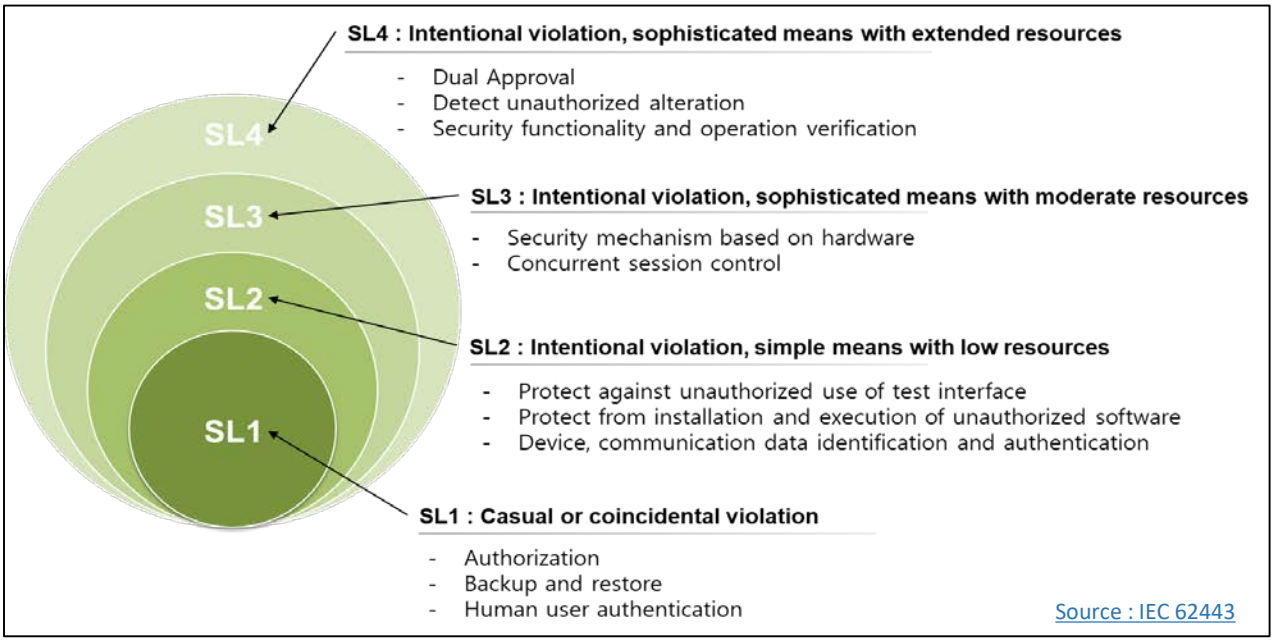
Type approval is to certify for the manufacturers of equipment for marine use that equipment comply with the provisions for the type approved products in the Guidance, where deemed satisfactory by the Society as the results of carrying out the examination, tests and inspection specified in the Guidance before installation on board. The cyber security type approval has been developed based on international standards such as ISA 62443 4-2, IEC 61162-460, and inspect cyber security level and function of cyber systems including remote access equipment, integrated control and monitoring systems on board the ship. The security requirements and their levels are verified on 12 categories and 124 requirements.

< Composition of KR Cyber Security Type Approval Guidelines >

Section 1 General	Section 5 Data Confidentiality	Section 9 Software Application Requirements
Sections 2 Identification and Authentication	Section 6 Restricted Data Flow	Section 10 Embedded Device Requirements
Section 3 Use Control	Section 7 Timely Response to Events	Section 11 Host Device Requirements
Section 4 System Integrity	Section 8 Resource Availability	Section 12 Network Device Requirements

Source : http://www.krs.co.kr/KRRules/KRRules2019/data/data_other/ENGLISH/gc31e000.pdf

Understanding Security Level (SL)



Source : IEC 62443

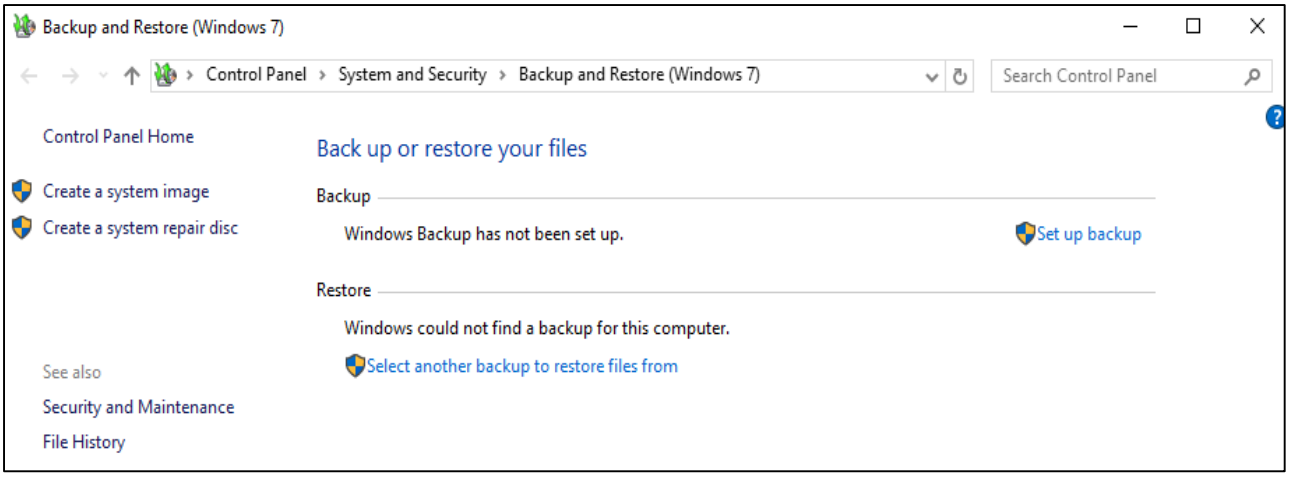
KR Type Approval of Maritime Cyber Security Inspection Items

System backup (803)

1. Components should provide the capability to participate in system level backup operations in order to safeguard the component state (user- and system-level information). The backup process should not affect the normal component operations. Components should provide an authorization enforcement mechanism for all users based on their assigned responsibilities and least privilege. (SL 1)
2. Components should provide the capability to validate the integrity of backed up information prior to the initiation of a restore of that information. (SL 2,3,4)

Requirement for Back-up

Backup is a copy of files and programs made to facilitate recovery if necessary (Source NIST SP 800-34r1) and it is an essential function for recovery, in case of system failure or misconfiguration. To meet the SL1 requirement, backup functions should be provided and the backup process should not affect the normal operations. If OT system cannot guarantee normal operations during the backup process then it can cause a problem with the availability of OT systems and cause a serious problem. In cases where it is difficult to provide these functions in the system, providing a redundancy of the system can be another solution. To meet SL 2, 3 and 4, a function to verify the integrity of backup should be provided. Integrity means protecting the accuracy and completeness of assets. In case the integrity of backup file is broken (eg. It has been unable to recover the system as a result of the backup file being falsified or damaged), a function is required to inform the user of the status before recovery. This is because if the system is restored with falsified or damaged files, the system could be abused for hacking or the system may not work properly and cause serious problems.



<Example of backup function>

Explanation of Term

OFDMA(Orthogonal Frequency Division Multiplexing Access)

- Multiple interorthogonal carriers are used to modulate and multiplex signals, which can reduce inter-symbolic interference (ISI) by extending the symbolic cycle by the number of subcarriers that direct the high-speed data to a number of subcarriers in parallel. Nevertheless, if the ghost is severe, a guard interval longer than the maximum period of the reflective wave is placed between the symbols to remove interference. Therefore, OFDM is capable of high-speed data transmission in a highly ghosted channel environment, single-frequency network (SFN) configuration with the use of guard interval, and easy application of multi-input multiple-output (MIMO) or adaptive modulation and coding (AMC) technologies. However, due to the relatively large Peak to Average Ratio (PAR), power efficiency is reduced. [TTA]

OTA(Over-the-air programming)

- OTA is designed to wirelessly distribute updates of new software, firmware, settings and encryption keys to devices such as mobile phones and set-top boxes. Through OTA, we can defend and prevent new types of malicious attacks, reduce costs by being able to update SW without door-to-door repair or USB delivery for SW updates, and update operating systems or SWs like smartphones to easily apply new functions and technologies throughout the life cycle of the device. [Suresoft]