KR Maritime Cyber Security

News from KOREAN REGISTER

Vol. 027

July 2020

KR Cyber security Activities

KR awards cyber security type approval certificate to Suncom

Korean Register (KR, Chairman Lee Hyung-chul) has granted its cyber security type approval certificate to Suncom for tis ship@TAMS on 24 June 2020.

Recently, as digital technology has been applied to ships in earnest, convenience has increased. However, cyber risk exposure has also increased, so the demand for cyber security certification services is increasing. Therefore, KR has provided its own cyber security type approval service based on IEC 62443-4-2 and IEC 61162-460.

Cyber security approval service for ICT equipment includes technical reviews of confidentiality, integrity and availability, which are basic requirements for security, and tests for monitoring capability for responding cyber incident and the capability of backup and recovery.

Ship@TAMS that received type approval is onboard installation equipment developed by Sumcom, that is the shipbuilding & maritime IT venture company and provides integrated management function for anti-virus in conjunction with onshore servers and onboard PC. In addition, it is designed to prevent computer virus infection through the USB security inspection provided by Ship@TAMS even if USB is used for operating technology (OT) such as ECDIS.

Taehoon Koh, President of Suncom, said, “It is meaningful to receive a certificate of type approval from Korean Register, which has excellent certification capability in the world-class. In the future, we will develop technologies related to ship cyber security in preemptive manner and grow into an excellent small and medium-sized enterprises.”

Kaemyoung Park, General Manager of KR cyber certification team, said, “Cyber security is now necessary in the maritime industry.

Like Suncom, which received this type approval, KR will actively support preemptive cyber security activities so that the local shipbuilding & maritime IT small and medium-sized companies can gain a foothold for overseas exports and be recognized for their technical skills.

Maritime Cyberattack up by 400 %

Report: Maritime Cyberattack Up by 400 Percent

Cybersecurity consultancy Naval Dome has reported a 400 percent increase in attempted hacks since February 2020. The primary cause is an increase in malware, ransomware and phishing emails attempting to exploit the COVID-19 pandemic, but Naval Dome says that global travel restrictions, social distancing measures and the economic recession are beginning to cut into companies' self-defense capabilities.

In addition, since OEM technicians have a harder time traveling to service systems on board ships and rigs, they are increasingly making "remote" service calls that require the operator to bypass security protections - creating an opening for a cyberattack.

“Covid-19 social restrictions and border closures have forced OEMs, technicians, and vendors to connect standalone systems to the internet in order to service them,” Naval Dome CEO Itai Sela said. “As budgets are cut and in the absence of service engineers, we are seeing ship and offshore rig staff connecting their OT systems to shoreside networks, at the behest of OEMs, for brief periods of time to carry out diagnostics and upload software updates and patches themselves.“

This means that their IT and OT systems are no longer segregated, and individual endpoints, critical systems and components may be vulnerable, Naval Dome warned. Some of these are legacy systems which have no security update patches and are even more susceptible to cyber attack. “The increase in OEM personnel working remotely on home networks and personal PCs, which are not well protected, adds to the problem," said Sela

During the first three months of 2020, attacks targeting home workers increased tenfold. Security software company McAfee has reported that that between January and April, cloud-based cyberattacks on all businesses increase by 630 percent.

“Our philosophy is that all systems must be protected using a risk ranking. If it is, then the entire platform is protected from both internal and external attack vectors. If only the network is protected, then whatever enters the net (such as an unintentional attack from authorized personnel) will infect all connected systems," said Sela.

Ido Ben-Moshe, vice president of business development for Naval Dome, says that remote working and the introduction of remotely controlled, autonomous technologies is likely to take place at a faster pace in a post-coronavirus world. “This will see companies face new cyber security challenges if they fail to implement adequate protective measures,” he said.

Source : The Maritime Executive, JULY 01, 2020

Kinds of Maritime Wireless Communication and Technical Security Vulnerabilities

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 newletter in July 2020 introduces ‘Kinds of Maritime Wireless Communication and Technical Security Vulnerabilities.’

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)-1

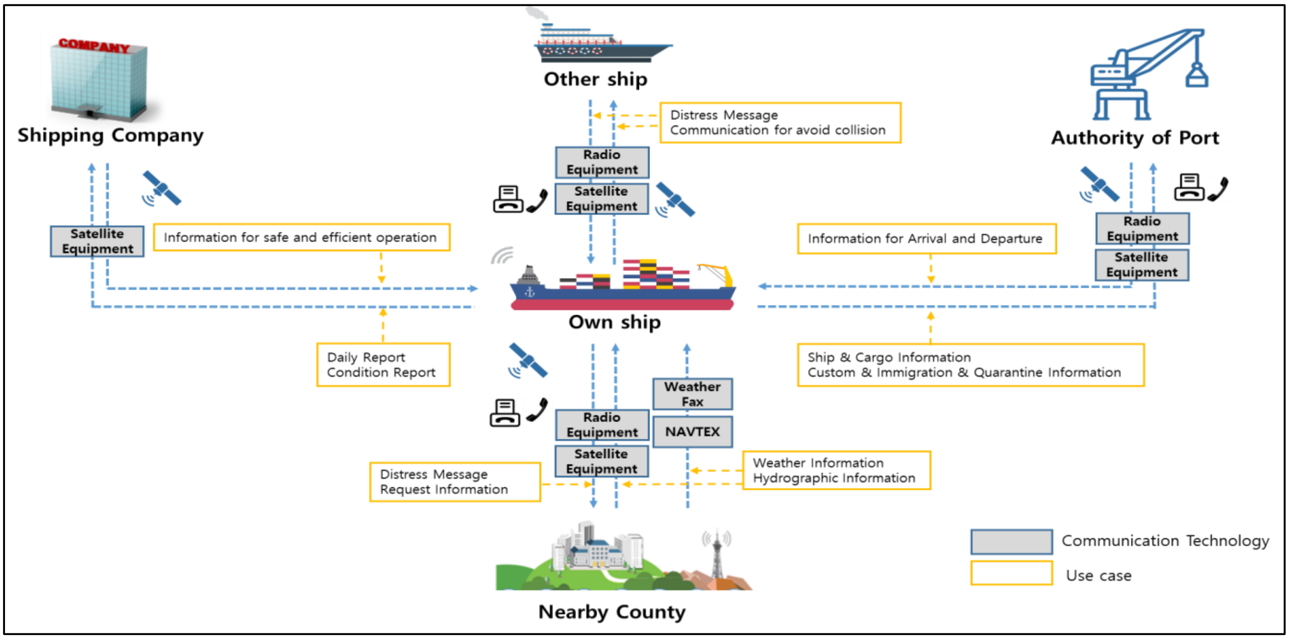
④ New security technology applied to Wi-Fi 6

⑤ Kinds of Maritime Wireless Communication and Technical Security Vulnerabilities

⑥ Security Vulnerabilities and countermeasures of Maritime Wireless Communication

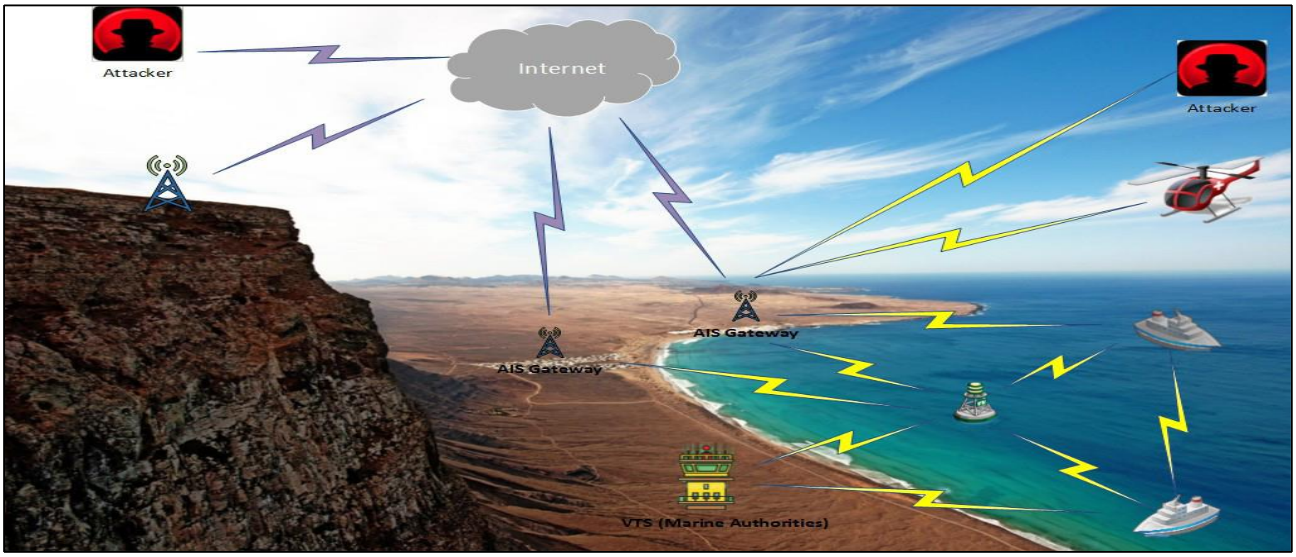
Kinds of Maritime Wireless Communication

Currently, maritime wireless communication equipment installed on ships operates independently. Among them, the most widely distributed digital wireless communication equipment is AIS(Automatic Identification System). However, AIS is used to carry out specific services such as tracking for vessels, collision avoidance, search and rescue, accident investigation, etc. VSAT is mainly used for data exchange through the Internet.



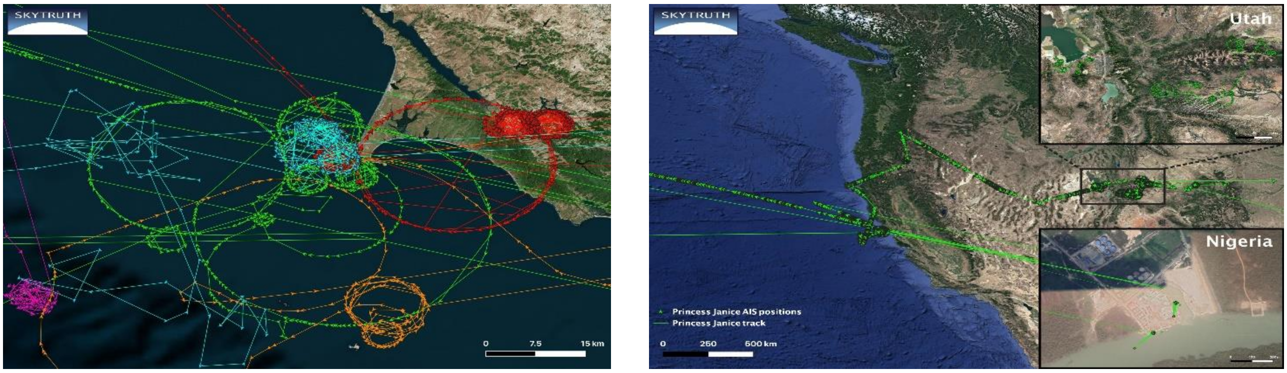
Security Vulnerabilities of AIS

Since 2020, AIS has been supplied to ships and is required to be installed on more than 300 tons of sea-going sea vessels in accordance with IMO SOLAS (river-going, fishing boats, etc. may have different installation regulations for each country) and is expected to be installed on more than 1 million ships worldwide. In 2024, Black Hat, a famous hacking group, introduced the security vulnerability of the AIS at a conference in Singapore.



Source : Blackhat Asia 2014, AIS Exposed understanding Vulnerabilities & Attacks 2.0

According to that introduction, AIS is exposed to a variety of cyber threats, including radio spoofing, hijacking, and GPS spoofing, because the inter-machine authentication and integrity check functions are not designed. In particular, there was an incident in which GPS system of about 290 ships were disabled due to North Korean GPS jamming attack in June 2016. In addition, according to the U.S. private think tank Skytruth recently, It is said that the AIS display found that ships were falsely spinning unlike their actual location. As the result of tracing the vessel, it is a false manifestation of a ship sailing thousands of miles away. From the crew's point of view, these fake AIS signals can cause confusion in determining the ship's route.



Source : https://skytruth.org/blog/

Understanding Cyber Threats(OWASP Top 10 IoT)

OWASP Top 10-Internet of Things(IoT)

The goal of the OWASP Things Internet Project is to help manufacturers, developers, and consumers understand more accurately the security issues associated with the Internet of Things and help users make wiser decisions in terms of security when building, distributing or evaluating IoT technology, according to the OpenWeb Application Security Project (OWASP). IoT)'s cyber threat Top10 and countermeasures are examined.

Use of insecure or outdated components

Use of outdated software components or insecure libraries in the code could allow the device to be compromised. Thus, developers or manufactures of IoT device should meet the following requirements.

1. All software components in consumer IoT devices should be securely updateable
2. The consumer should be informed by the appropriate entity, such as the manufacturer or service provider, that an update is required.
3. When software components are updateable, updates shall be timely.
4. When software components are updateable, an end-of-life policy shall be published for devices that explicitly states the minimum length of time for which a device will receive software updates and the reasons for the length of the support period.
5. When software components are updateable, the need for each update should be made clear to consumers and an update should be easy to implement.
6. When software components are updateable, updates should, where possible, maintain the basic functioning of the device, which can be critical to remain available during an update.
7. When software components are updateable, the provenance of software updates should be assured and security patches should be delivered over a secure channel.
8. For constrained devices that cannot have their software updated, the product should be isolable and the hardware replaceable.
9. For constrained devices that cannot have their software updated, the rationale for the absence of software updates, the period of hardware replacement support and an end-of-life policy should be published in an accessible way that is clear and transparent to the consumer.

Source : ETSI TS 103 645 v1.1.1

Guideline for Type Approval of Maritime Cyber Security

Understanding Guideline for Type Approval of Maritime Cyber Security

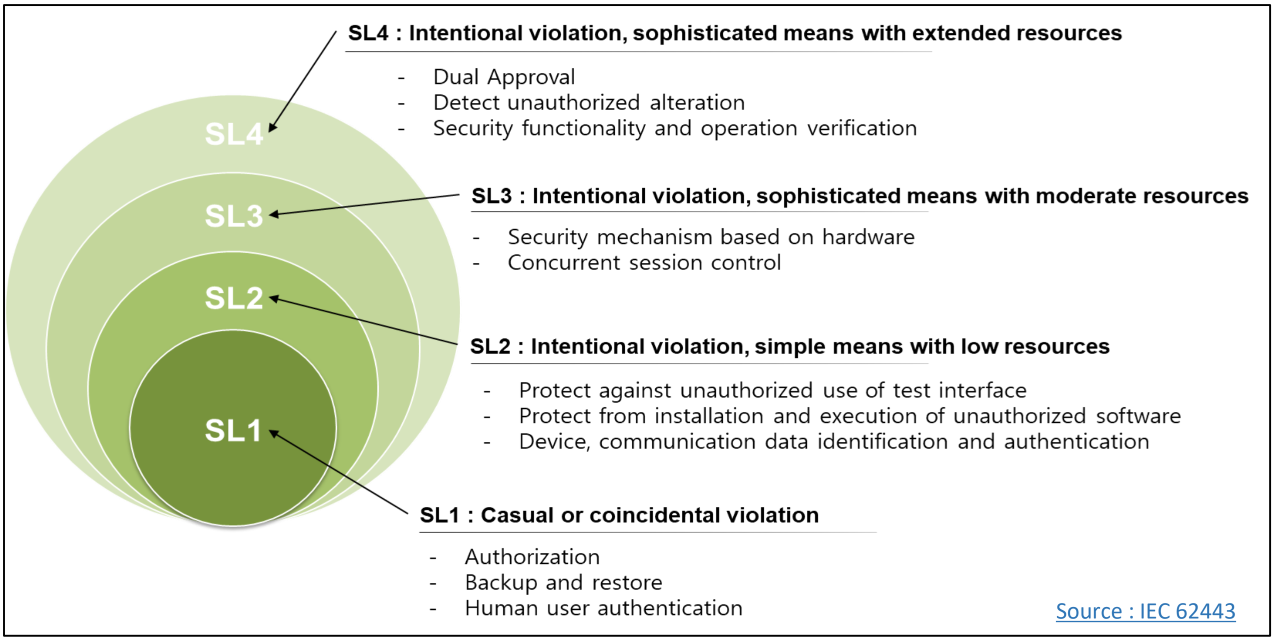
Type approval is to certify for the manufacturers of equipment for marine use that equipment comply with the provisions for the type approved products in the Guidance, where deemed satisfactory by the Society as the results of carrying out the examination, tests and inspection specified in the Guidance 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)



SL4 : Intentional violation, sophisticated means with extended resources

- Dual Approval
- Detect unauthorized alteration
- Security functionality and operation verification

SL3 : Intentional violation, sophisticated means with moderate resources

- Security mechanism based on hardware
- Concurrent session control

SL2 : Intentional violation, simple means with low resources

- Protect against unauthorized use of test interface
- Protect from installation and execution of unauthorized software
- Device, communication data identification and authentication

SL1 : Casual or coincidental violation

- Authorization
- Backup and restore
- Human user authentication

Source : IEC 62443

KR Type Approval of Maritime Cybersecurity Inspection Items

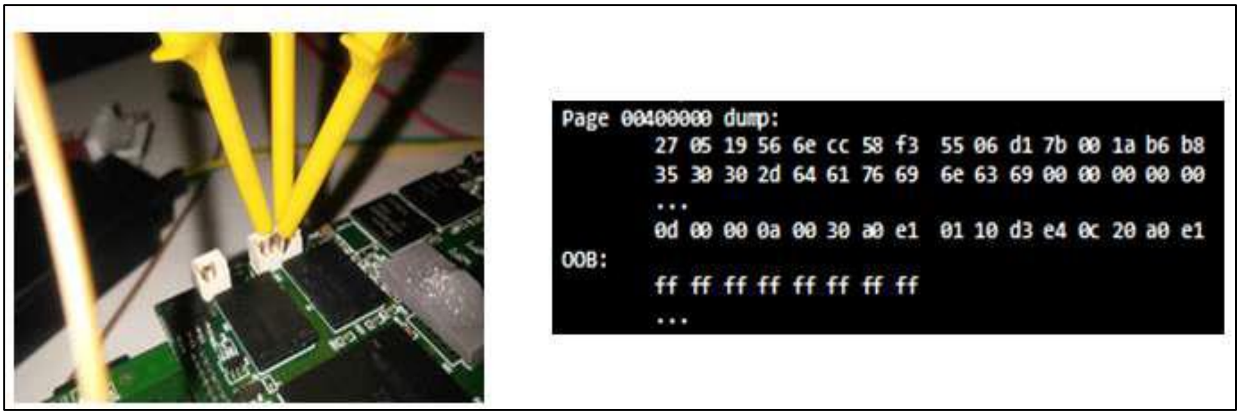
Embedded Device Requirements

- Use of physical diagnostic and test interfaces (1002)

1. Embedded devices should protect against unauthorized use of the physical factory diagnostic and test interface(s). (SL 2)
2. Embedded devices should provide active monitoring of the device's diagnostic and test interface(s) and generate an audit log entry when attempts to access these interface(s) are detected. (SL 3,4)

Security of physical diagnostic and test interfaces

For embedded equipment such as PLC, separated physical PORTs cab be used for system maintenance or firmware updates. An example of this is the Point Test Action Group (JTAG) Port, which can be exploited for external attacks.



```
Page 00400000 dump:
        27 05 19 56 6e cc 58 f3  55 06 d1 7b 00 1a b6 b8
        35 30 30 2d 64 61 76 69  6e 63 69 00 00 00 00 00
        ...
        0d 00 00 0a 00 30 a0 e1  01 10 d3 e4 0c 20 a0 e1
OOB:
        ff ff ff ff ff ff ff ff
        ...
```

<Examples of physical attacks on exposed ports>

To meet SL2 rating of cyber security type approval, prevention function of unauthorized use of physical ports that may be subject to such attacks should be provided. Examples of unauthorized use of physical factory diagnostics and test interfaces include the use of these ports only during the first stage of development and the removal of those ports after product launch. This is the most complete method, but depending on the product, the use of that port may be required after launch, and in such cases, access restrictions may be provided to meet the requirements. For the JTAG Port, access restriction functions can be implemented using the program tools provided by the chip manufacturer. To meet SL3 and 4, it is required to provide active monitoring of the diagnostic and test interfaces and to record any attempt to access them. If access restriction functions are implemented, rather than port removal, to prevent unauthorized use, access records may be recorded in the log, etc. to meet the requirements.