KR Maritime Cyber Security

News from KOREAN REGISTER

Vol. 020

December 2019

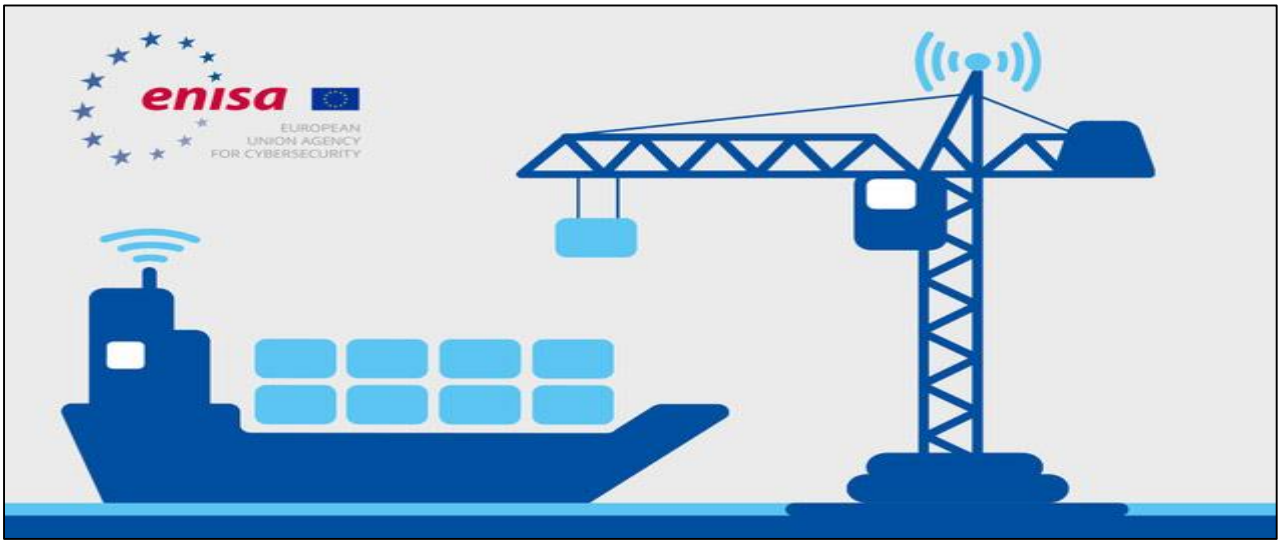
KR and Hyundai LNG shipping sign MOU on cyber security systems

The Korean Register and Hyundai LNG Shipping (HLS) signed a memorandum of understanding (MOU) on 2 December, agreeing to conduct joint research on the application, verification and development of Guidance for maritime cyber security systems. The MOU brings together KR's globally recognized maritime cyber security certification capability and HLS's expertise in cyber security technology. Under the agreement, the two companies will jointly verify cyber security solutions applicable to new ships and will develop risk analysis and design safety evaluations for cyber security systems. The IMO's Resolution of MSC.428(98) adopted at the 98th meeting of the Maritime Safety Committee in June 2017 will increase demand for cyber security risk management from 2021. From this date, Administrations will be obliged to ensure that cyber risks are appropriately addressed in safety management systems no later than the first annual verification of the company's Document of Compliance after January 1, 2021. A ship's cyber security system protects its operational data, the networks that deliver data and the data storage. Demand for cyber security protection has grown in recent years because of the rapid convergence of ship's operational information and communication technologies and the increased exchange of information between ship and ship and ships and land, respectively. KR established its own maritime cyber security certification system last year and provides a cyber security certification services for companies and ships, and cyber security type approval services for networks and automation systems of ships.

ENISA release port cyber security guidelines

ENISA release port cyber security guidelines

The European Union Agency for Cybersecurity (ENISA) has recently issued some port cybersecurity guidelines. Cyber security incidents, such as ransomware attacks on ports, incur significant economic losses, and ports need to ensure cyber security is a top priority in any port digitization development to ensure safety and security and maintain commercial competitiveness. The new ENISA guidelines highlight recommended actions to address cybersecurity threats as ports become ever more digitized. The introduction of the Smart port concept brings particular cyber security challenges because it accelerates the risk exposure of port systems. Ports have traditionally been concerned with physical security and safety, but now they need to integrate cyber security into any global strategy.



ENISA port cyber security guidelines : key points

· All stakeholders involved in port operations to define clear governance of port cyber security
· Implement technical cyber security measures, such as network separation, update management, password enforcement, and permission separation
· Cyber security to be included at design stage of port development
· Establish detection and recovery procedures to ensure a rapid response system before cyber attacks affect port operations

Source : https://www.helpnetsecurity.com/2019/11/27/port-cybersecurity/

UK maritime service provider cyber attacks

James Fisher & Sons resent cyber attack

In November, British maritime service provider James Fisher & Sons (JFS) had to close down all of its computer systems following a cyber attack by hackers. The company commissioned an external cybersecurity agency to conduct a forensic investigation of all systems to identify the cause and scope of the attack. A JFS official confirmed that the attack was a Ransomware variant that blocked file access, which led to a 7% drop in the company's share price. A recent study found that the marine sector is very vulnerable to cyber attacks. Too often the systems operations of tankers, container ships, yachts and cruise ships are still using old operating systems such as Windows XP. It is vitally important that companies engaged in maritime business should pay attention to cyber security risk and should take the necessary measures to prevent or mitigate cyber security threats in all circumstances.

Source : https://www.cybersecurity-insiders.com/cyber-attack-on-james-fisher-and-sons/

Image Source : https://safety4sea.com/mexican-oil-company-refuses-to-pay-ransom-to-hackers/

1) James Fisher and Sons is a company founded in 1847 and currently conducts business such as the Port Authority, Renewable Energy Services, Offshore Oil Services, Shipping and other technology businesses such as subsea design and construction.

Ship Cyber Security Vulnerabilities and Countermeasures

Types of ship cyber security vulnerabilities

Ship operators and crews use computers and cyber technology for navigation, communications, cargo, ballast, safety, control and many other purposes. Emergency systems such as security surveillance, fire detection and alarms are increasingly dependent on cyber technology and network designs may be vulnerable to security breaches, uncontrolled access, equipment manufacturers or unknown remote access. Therefore, it is essential for companies to quickly and appropriately address any vulnerabilities identified on land and ships, these could include;

1. An operational system that is no longer supported

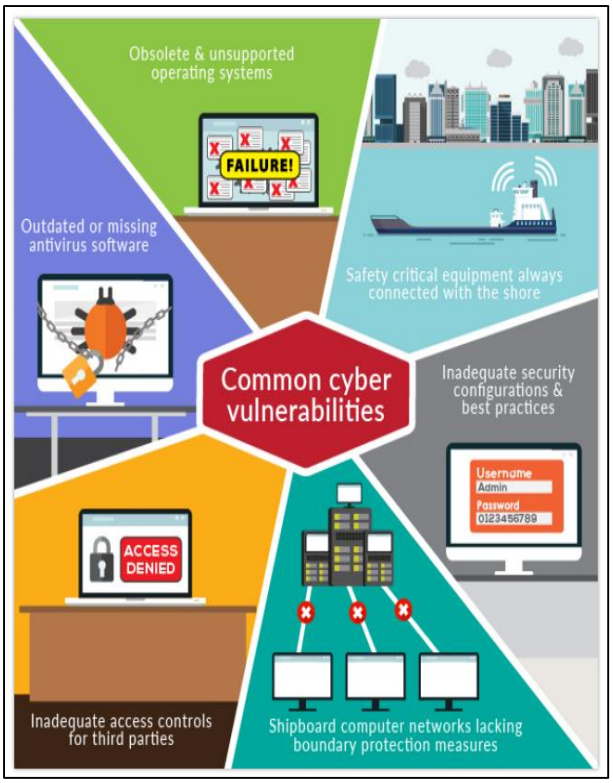
2. An old or missing virus vaccine software and malware prevention program

3. Using inefficient network management, administrator accounts or passwords

4. Missing ship computer networks, border protection measures and network division

5. Always connecting equipment or systems that are important to safety to land

6. Improper access control to third parties, including contractors and service providers



Source: https://safety4sea.com/cm-6-common-cyber-risks-affecting-maritime-industry/

Procedural control and deep defense approach

In order to strengthen the cyber security of a ship, apply the following procedural controls provided by SAFETY4SEA, to improve the appropriate procedures and increase employees' awareness and use of SSP-based physical security, network protection, intrusion detection, software whitelist, access and user control, mobile media and password policies.

Procedural control	Detailed content
#1 Education and Recognition	▪ Internal cyber threats are significant and should not be underestimated, even employees can be careless, and data can be mishandled. ▪ Training and awareness should be adjusted to the level appropriate for the onboard personnel, including captains, officers, crew and coastal staff who support the management and operation of the ship.
# 2 Upgrade and software maintenance	▪ Hardware or software that producers or software developers no longer support cannot be updated to address potential vulnerabilities. For this reason, using hardware and software that is no longer supported should be carefully evaluated by the company as part of its cyber risk assessment. * Note: Procedures to update software in a timely manner are needed in relation to ship type, internet connection speed, and sea time
# 3 Update anti-virus and anti-malware tools	▪ Continuous updates are required to detect and process malware using software tools. Updates should be distributed to the ship in time and set up procedurally so that all related computers on the ship are updated.
# 5 Administrator authority use	▪ Administrator privileges allow system configuration settings and full access to all data and must be provided only to properly educated employees who use that privilege to log into the system. ▪ User accounts should be removed when no longer in use and should not be passed from one user to the next using a generic user name
# 6 Physical and mobile media control	▪ A clear policy for the use of mobile media devices is essential; media devices should not be used to transmit information between systems that are generally not controlled and systems that are controlled. If there is no medium device such as software maintenance, then there should be a procedure to check whether any malware is present in the mobile media device.
# 7 Discarding equipment containing data	▪ Equipment that is no longer used may contain commercially sensitive confidential data. The company should have a procedure to dispose of the equipment so that any data is also properly disposed of in the unused equipment and it's not possible to access important information
# 8 Receiving support from coastal and emergency planning	▪ In case of a cyber attack, a ship must be able to receive technical support; this support and any related procedures must be available on all ships.

[Series News] ⑤

Application of 5G for Maritime Digitization

This series will deal with a core infrastructure related to the 4th industrial revolution, the positive ripple effect of 5G on the marine industry, and the cyber threat accordingly. Therefore, this newsletter, Sep. 2019, introduces '5G network structure and network slicing technology.

series news

① What is 5G?

② 5G Network architecture - Network Slicing, and Affects on the maritime Industry

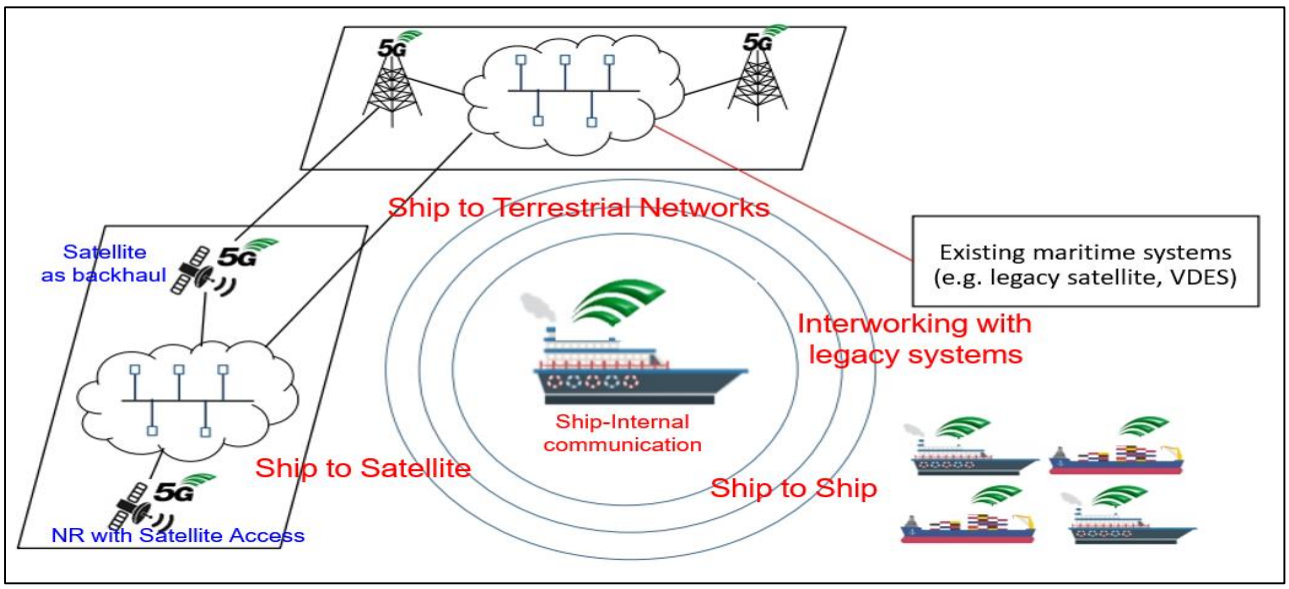
③ Comparison between LTE centralized network and 5G distributed network

④ Role of satellites in G standards

⑤ **The private network reference model in 5G standard for effective use in ships and ports**

A study on the application of 5G standard for smart shipping

The communication environment at sea is fundamentally different from the communication environment on the land due to reflection and scattering. Mobile communication technologies such as LTE and 5G are also based on a land communication environment, and they need to be applied to the marine environment as soon as possible. Marine users want to apply 5G to the marine environment, particularly for the digitization of marine fisheries, and for smart ports and autonomous ships. So, in order to apply 5G to the marine environment, how can this be done, and what additional research and 3GPP standardization work is needed.

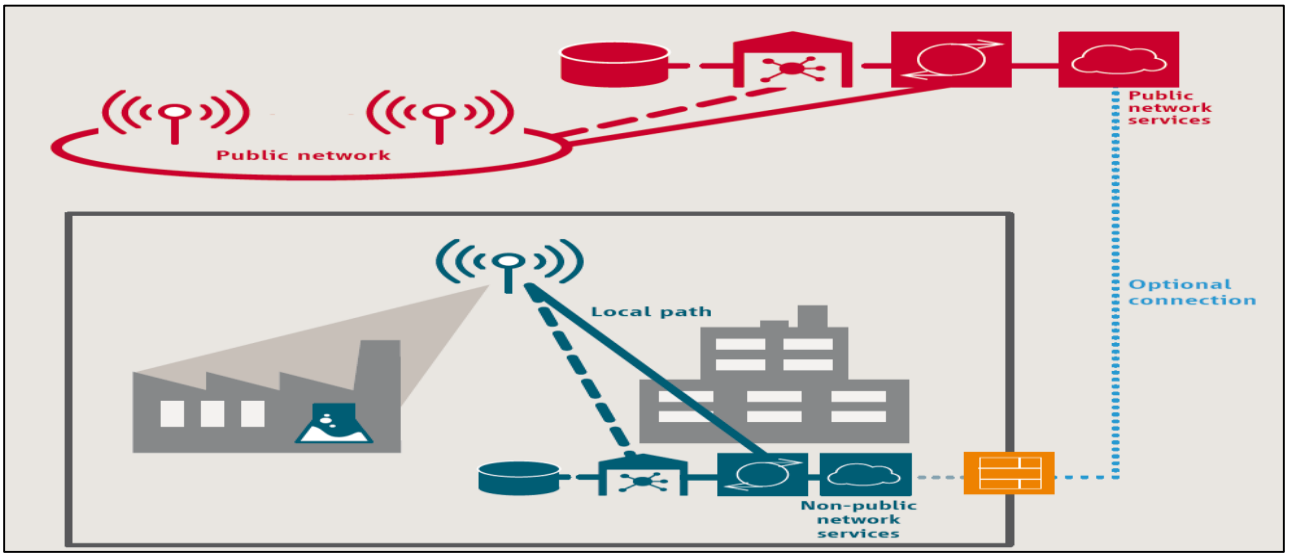


Source : KR-Synctechno, APMC 2019-Update of 5G standardization in 3GPP

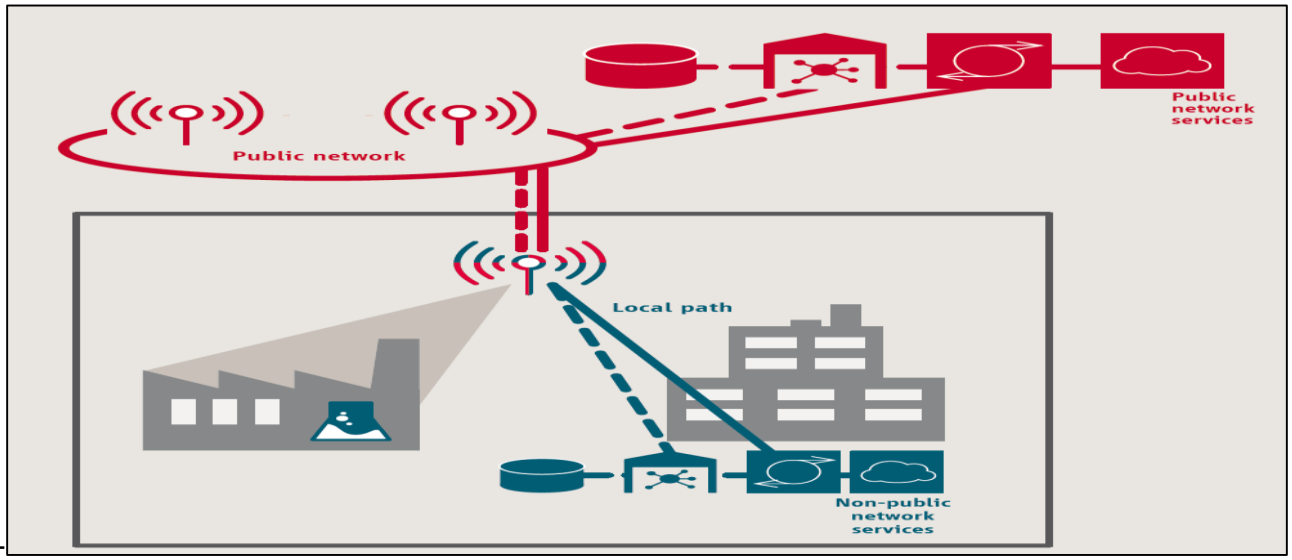
Reference to introduce a 5G private network to a ship's internal network

To enhance the smartness of a ship, the internal network needs to be improved. To control OT equipment in vessels such as autonomous ship ships, it is worth referring to the private network concept in the smart factory field of the existing 5G standard. The 5G standard is separated into a User Plane for Data Exchange, a switch, and a Control Plane for Router Control. In order to control OT equipment in ships, performance criteria such as delay speed, reliability, and stability are important, and performance such as communication capacity is necessary to monitor the situation onboard with CCTV on land. Therefore, efficient communication is necessary for each service scenario on the ship, and this concept can be used as a reference model for the smartness of the ship, such as on an autonomous ship.

< Factory Automation Service Scenarios in a Disconnected Network >



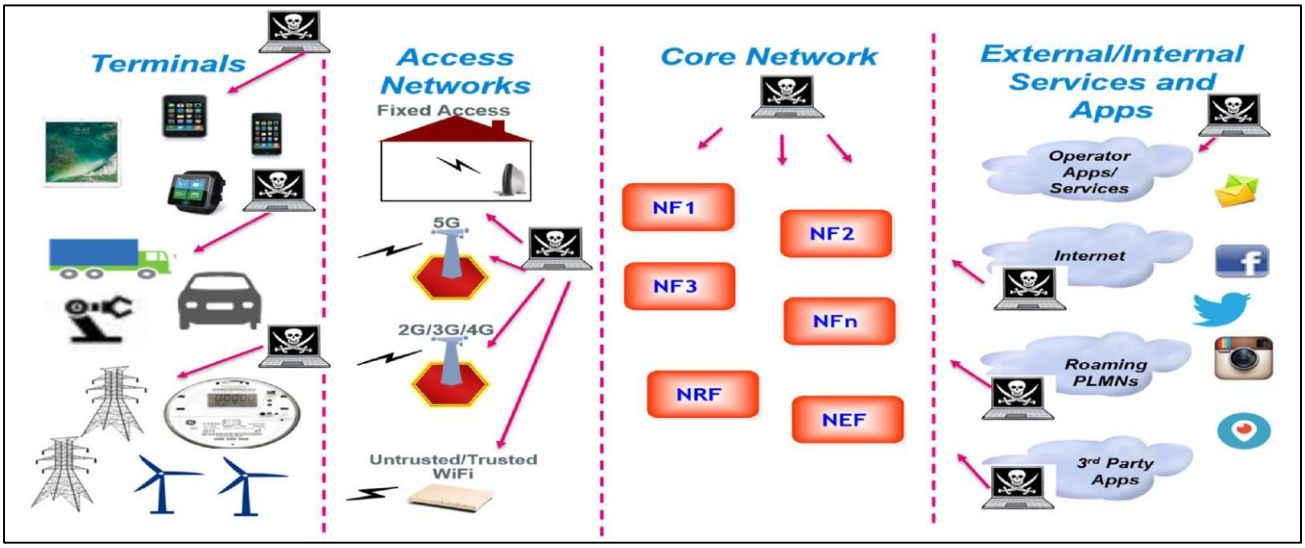
< Factory Automation Service Scenarios for Remote Control and Monitoring >



Source : 5G ACIA, 5G Non-Public Networks for Industrial Scenarios

Cyber threat elements of 5G standards

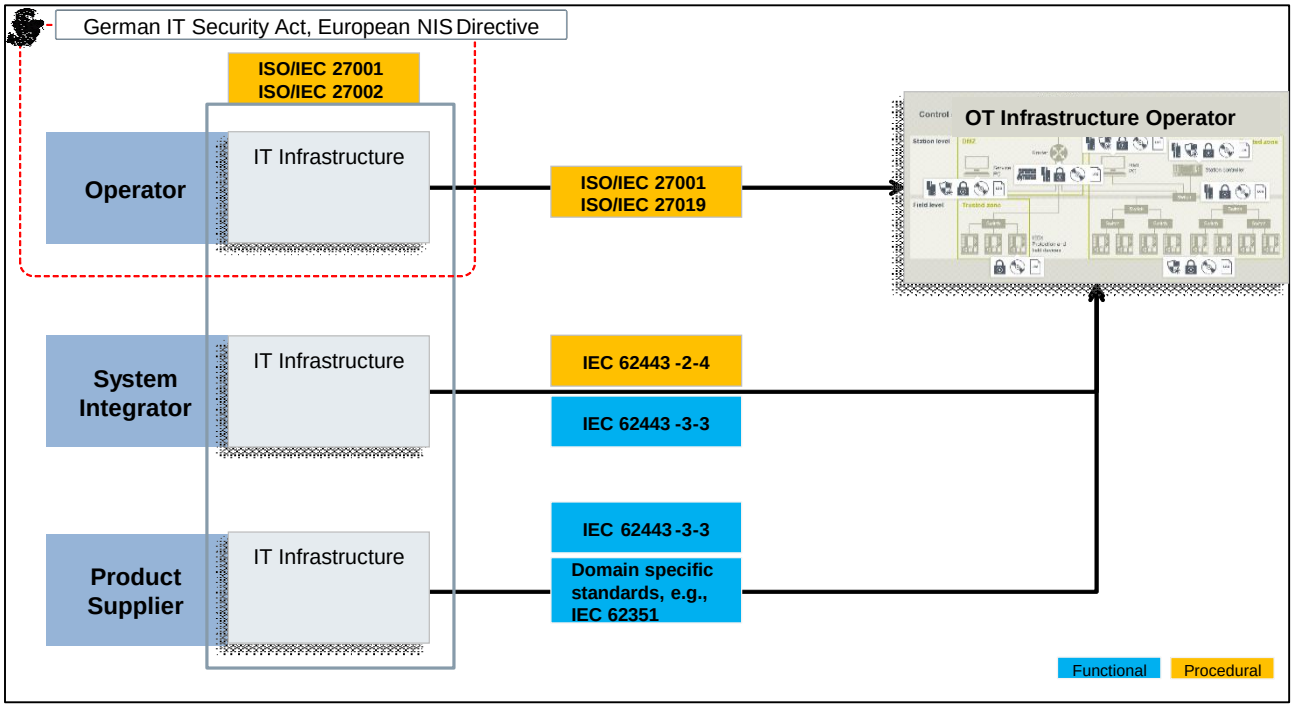
Standards work to mitigate any cyber threats by conducting a risk analysis of each of the various 5G elements and segments, such as the terminals, wireless networks, wired networks, operator hosts, or applications and services, in order to reduce cyber threats. The figure below shows a high-level landscape for 5G threats.



Source : The Evolution of Security in 5G, 5G America white paper, July 2019

Cyber security frameworks for 5G factory automation standards

The 5G factory automation-related standard uses the framework of the IEC62443 standard; the IEC62443 standard is widely used in OT systems.



Source : 3GPP TR 22.804 V.2.0.0(2018-5)

Guideline for Type Approval of Maritime Cyber Security

Understanding Guideline for Type Approval of Maritime Cyber Security

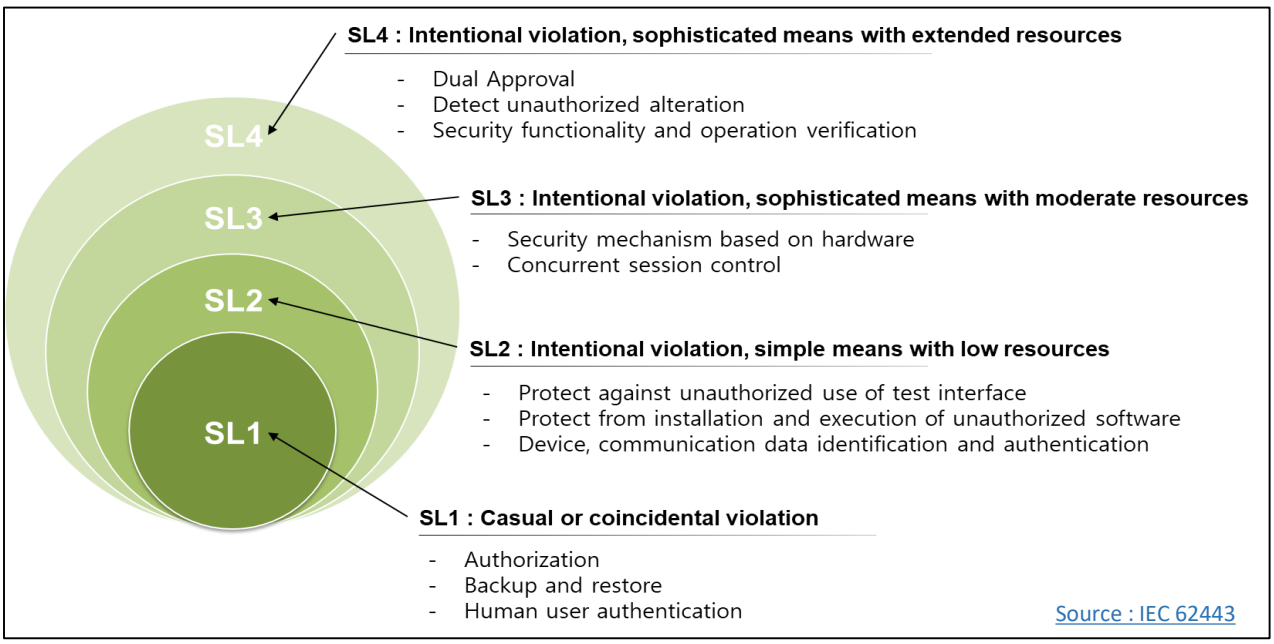
Type approval is to certify for the manufacturers of equipment for marine use that equipment comply with the provisions for the type approved products in the Guidance, where deemed satisfactory by the Society as the results of carrying out the examination, tests and inspection specified in the Guidance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



Source : IEC 62443

KR Type Approval of Maritime Cybersecurity Inspection Items

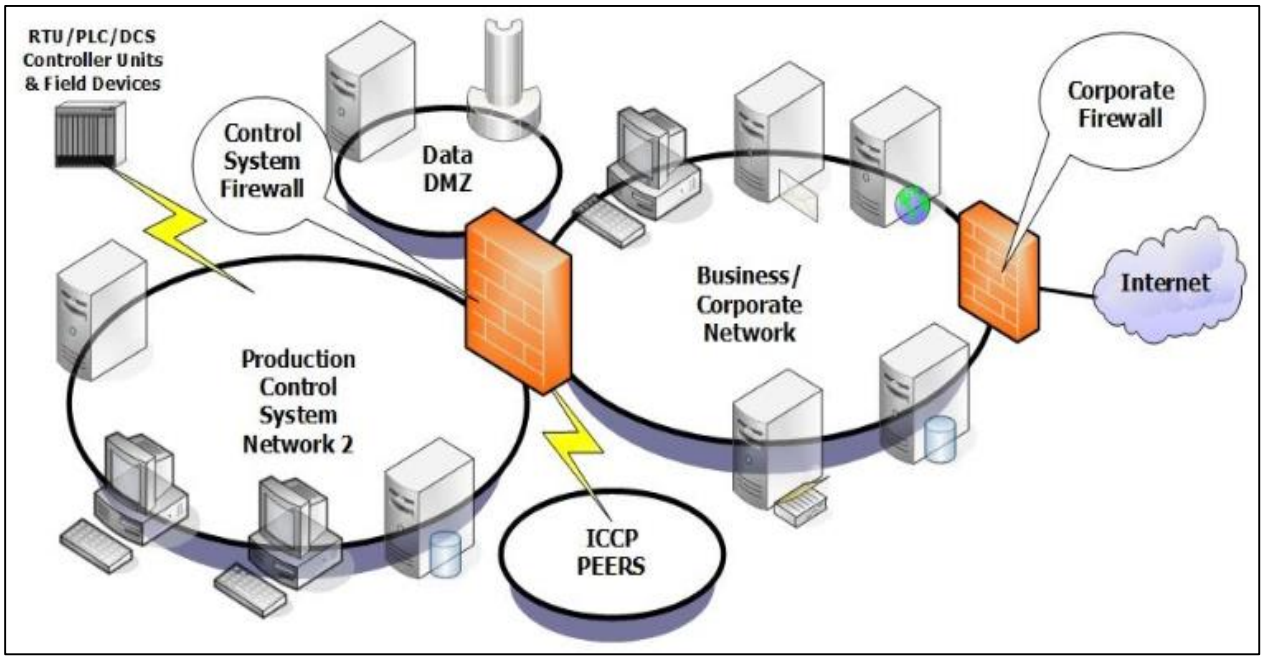
Network segmentation(601)

Components should support a segmented network to support zones and conduits, as needed, to support the broader network architecture based on logical segmentation and criticality.

Guidelines for Network Segmentation

The OT system of the ship must be separated from the IT system, which is possible by physical or logical methods. In the case of a stand-alone system that is not physically connected to the external system, it is safe from external intrusion through the network because it is physically separated from the network. However, the number of smart vessels that support functions such as monitoring and maintenance via remote access from land are increasing, and in this case, a network division function can be implemented through a logical network separation. The subnets should be constructed according to the structure of the OT system, not a single network. A subnet is easy to understand if it is literally creating a subnetwork on a network. Physically, it seems to be all connected to one switch, but through the subnet configuration, there are several logical networks. In addition to subnet configuration, an access control policy should be established by setting a firewall or switch. Transceiver or non-reception of data going network can be restricted through the policy setting, of the allowable policy of the IP address base or the communications port and the safe network can be constituted.

< Example of network configuration considering DMZ between control network and business network>



Source : us-cert.gov

Explanation of Term

Ransomware

Ransomware is a malicious code that encrypts user data (system files, documents, images, videos, etc.) and demands money for recovery. It is a combination of ransom and software, and is a malicious program that changes the system to an unusable state or encrypts data to prevent it from being used and requires money as a hostage

European Union Cyber Security Agency (ENISA)

The European Network and Information Security Agency was established in 2004 to protect the cyber information of the EU. It plays an important role providing information and supporting Member States, European Union institutions, bodies and agencies in their response to computer viruses and incidents of hacking in each country.