KR Maritime Cyber Security

News from KOREAN REGISTER

Vol. 028

August 2020

MacNet Strategy Webinar Cyber Security Presentation

MacNet, the Maritime Cluster Networking organisation in Korea (Chairman, Mr LEE Hyung-chul, Chairman of Korean Register) held its 'MacNet 2020 Strategy Webinar (Web + Seminar)' on 15 July 2020.

This webinar, organized by MacNet, and sponsored by the Busan City Government, was held under the theme of 'Strategic Response of the Regulations on De-carbonisation and Cyber Security for the Sustainable Development of the Shipping and Port Industry'. In Session 2, titled 'Current Status and Response of Maritime Cyber Security to Change in a Digital Industrial Environment', Mr SIM, SangGyoo, CTO of Penta Security Systems Inc, presented a paper on 'Cyber Security of Autonomous Ships'; and Mr CHA, YoungKyun, Professor at Korea University, presented a paper on 'Cybersecurity in Digitalization.' The discussion that followed included Mr PARK, Kaemyoung, General manager of KR's Cyber Certification Team.

The presentation by Mr SIM, SangGyoo focused on how to apply cyber security technology that had been developed for self-driving cars, to a ship's external communication and internal systems. Following this, Prof. CHA discussed the changes within the maritime industry resulting from the introduction of ICT (Information and Communication Technology) and cyber security requirements.

Commenting on the session, a MacNet official said, "currently, cyber threats and risks are on the rise due to the introduction of ICT innovations such as Blockchain, Artificial Intelligence (AI), Big data, Digital Platforms, and the Internet of Things (IoT). Because of this, in-depth discussions are being held on how best to respond to cyber security issues in the shipping and port industries".

Maritime Cyber Attack Increase By 900% in Three Years

Cyber-attacks on the Maritime industry's OT systems have increased by 900% over the last three years.

Addressing port and terminal operators during an online forum last week, Robert Rizika, Naval Dome's Boston-based Head of North American Operations, explained that in 2017 there were 50 significant OT hacks reported, increasing to 120 in 2018 and more than 310 last year. He said this year is looking like it will end with more than 500 major cyber security breaches, with substantially more going unreported.

Rizika said that since NotPetya – the virus that resulted in a US$300 million loss for Maersk – "attacks are increasing at an alarming rate" and this year a US-based gas pipeline operator and shipping company MSC have been hit by malware, of which the latter incident shut down the shipowner's Geneva HQ for five days.

last month the OT systems at Iran's Shahid Rajee port were hacked, dozens of cargo ships and oil tankers waiting to offload, while long queues of trucks formed at the entrance to the port stretching for miles, according to Naval Dome. Reports of this attack have gone some way in raising public awareness of the potential wider impact of cyber threats on ports around the world.

In addition, Rizika revealed that a report published by Lloyd's of London indicated that if 15 Asian ports were hacked financial losses would be more than US$110 billion, a significant amount of which would not be recovered through insurance policies, as OT system hacks are not covered.

Going on to explain which parts of the OT system – the network connecting RTGs, STS cranes, traffic control and vessel berthing systems, cargo handling and safety and security systems, etc., – are under threat, Rizika said all of them.

"Unlike the IT infrastructure, there is no "dashboard" for the OT network allowing operators to see the health of all connected systems. Operators rarely know if an attack has taken place, invariably writing up any anomaly as a system error, system failure, or requiring restart.

"What is interesting is that many operators believe they have this protected with traditional cyber security, but the fire walls and software protecting the IT side, do not protect individual systems on the OT network. And The antivirus system would very quickly turn out to be non-essential, impairing and inhibiting system performance." he said.

Where OT networks are thought to be protected, Rizika said they are often inadequate and based on industrial computerised system, operating in a permanent state of disconnection from the network or, alternatively, connected to port systems and the equipment manufacturer's offices overseas via RF radio communication (wi-fi) or a cellular network (via SIM).

"Hackers can access the cranes, they can access the storage systems, they can penetrate the core operational systems either through cellular connections, wi-fi, and USB sticks. They can penetrate these systems directly."

Rizika said that as the maritime industry moves towards greater digitalisation and increases the use of networked, autonomous systems, moving more equipment and technologies online, more vulnerabilities, more loopholes, will be created.

"There will be a whole series of new cyber security openings through which people can attack if systems are not properly protected.

"If just one piece of this meticulously-managed operation goes down it will create unprecedented backlog and impact global trade, disrupting operations and infrastructure for weeks if not months, costing tens of millions of dollars in lost revenues."

Naval Dome also predicts that cyber criminals, terrorists and rogue states will at some point begin holding the environment to ransom. "One area we see becoming a major issue is cyber-induced environmental pollution. Think about it: you have all these ships in ports, hackers can easily over-ride systems and valves to initiate leaks and dump hazardous materials, ballast water, fuel oil, etc.," Rizika warned.

Offering advice on the first steps port operators need to take to protect their OT systems, he said a deep understanding of the differences between the two spaces is vital.

"There is a disconnect between IT and OT security. There is no real segregation between the networks. People can come in on the OT side and penetrate the IT side. We are actually seeing this now. Successful IT network hacks have their origins in initial penetration of the OT system."

Source : HELLENIC SHIPPING NEWS, 2020

Security Vulnerabilities and Countermeasures of Maritime Wireless Communication

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 'Security Vulnerabilities and Countermeasures of Maritime Wireless Communication.'

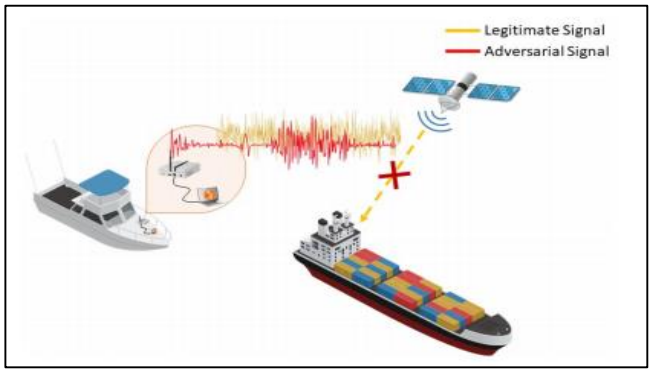
Series news

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

Key security vulnerabilities of maritime wireless communication

1. Global Navigation Satellites System(GNSS)

Ocean going ships are usually fitted with GNSS systems which allow them to know their exact positions by receiving locational information from satellites. To encourage a wide availability, most GNSS systems do not use confidentiality or authentication mechanisms and this makes them easy prey to cyber-attack and particularly to spoofing. In the Black Sea area in June 2017, at least 20 ships were reported to have switched to a manual navigation system due to GNSS spoofing attacks. As concerning, GNSS systems are also highly sensitive to jamming attacks which break down the availability of GNSS by emitting noise at a similar frequency.



< Logic of ship jamming and spoofing attack >

Tech.	Confidentiality	Certification	Availability
GNSS	X	X	X
AIS	X	X	X
SATCOM	X	O	O
CAN-BUS	X	X	O

< Cyber security property of ship communication >

Source :arXiv:2003.01991v1, Vessels Cybersecurity: Issues, Challenges, and the Road Ahead, 4 Mar 2020

2. Satellite Communication

The security levels of satellite communications will vary depending on the supplier but a recent study found an unencrypted connection between the VSAT antenna and the gateway. This means that the use of certain (e.g., POP3 e-mail or HTTP browsing) services could result in personal information being compromised. Similarly, there are many Common Vulnerabilities and Exposures (CVE) that have been identified in relation to GMDSS services. The underlying cause of the vulnerability was found in the thraneLink protocol, a proprietary solution within the SAILOR 6000 communication family. In particular, backdoors have been found where attackers can install unauthenticated firmware updates and malicious software. In addition, an attacker who is aware of the additional protocol-level vulnerabilities in the Mini-C INMARSAT terminal may deactivate the Ship Security Alert System (SSAS) that is used to communicate piracy and terrorist attempts on a ship. Further physical attacks are possible by simply modifying the direction of the VSAT antenna, which may also reject stable satellite communication links.

Security measures

Security issues	Security measures
GNSS Spoofing	Cross-Technology Location Estimation (GNSS, SATCOM)
Electronic Warfare	Anti-jamming Protocols
Non-Standardized SATCOM Protocols	Standardization Efforts
AIS Spoofing	Software Security Frameworks
Bridge System Assessment	Standardized Security Assessment Procedures
Malware Attacks	Containerization
Automatic Safety Systems	Wireless Sensing and ML
Wired Communication Protocols Security	Physical Security Strategies, Access Control

< Key security issues and security measures of ship wireless communication >

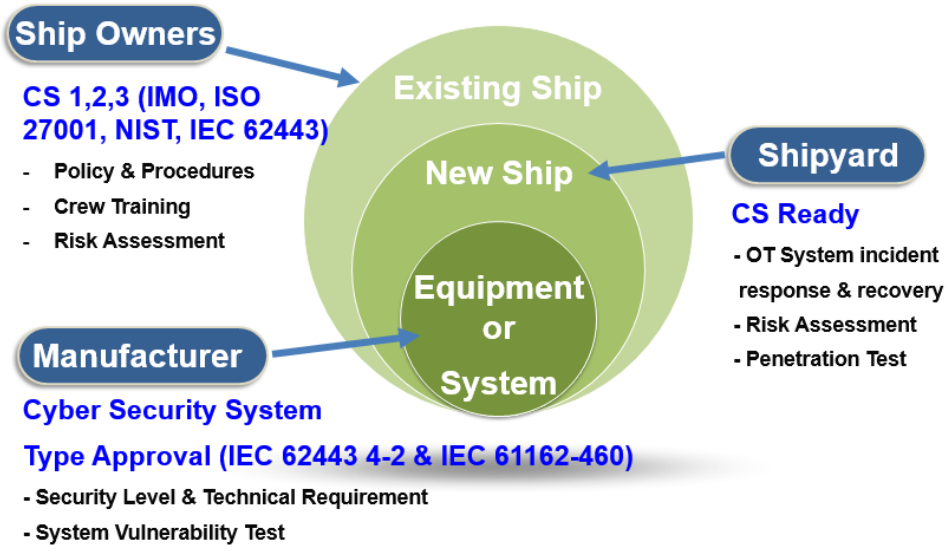
Key security issues related to wireless communication in ships and the resulting security measures are summarized in table 2. However, whilst these security measures may be the most effective currently, as maritime wireless communication technology continues to advance, the design of cyber security measures will need to be updated regularly.

Understanding of Cyber Security Notation (CS Ready) for New ship

KR Cyber Security Certification System

KR Maritime Cyber Security Certification applies to the company or the ship with cyber security management system (CSMS). When the company/the ship pass the survey for certification(document review and on-site survey), KR issues cyber security compliance certificates to the company/the existing ship, and cyber security notation (CS-Ready) to the new ship. Cyber security compliance for the company/the existing ship is divided to 3 levels (CS1, CS2 and CS3) in accordance with cyber security maturity, and consists of 35 survey areas and 144 survey items.

- **CS1, CS2, CS3** : Requirements of CSMS for the existing ship **(Shipping company)**
- **CS Ready** : Requirements for establishing integrated cyber security system of new ship **(Shipbuilder)**
- **CS Type Approval** : Requirements of cyber security function of equipment system **(Equipment company)**

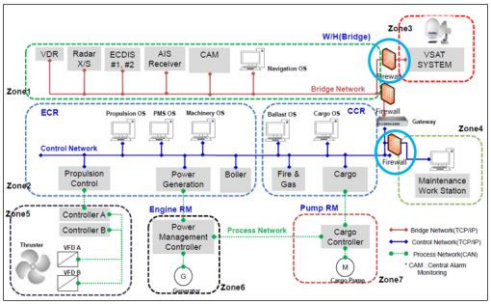


Need of Cyber Security Notation (CS Ready) for New Ship

As the marine business environment changes, Advanced automation and integrated control system is equipped in ships, and remote access, control and maintenance of the system in ships became possible from the land, which resulted increase of ship cyber risks. Therefore it is very important for maritime safety that construction and verification of an integrated system preventing and responding cyber incidents from the stage of ship building. KR gives 'CS Ready' notation to the new ship with cyber security system. In this newsletter, the requirements will be introduced.

[CS Ready] Main Activity : Document review(ship network, etc.)

Cybersecurity design validation is reviewed through document review on ship network configuration chart, asset list, system functional requirements specification, incident response & recovery manuals, etc. List and details of document to be submitted are founded on the following page.



< Ship network configuration chart >

[CS Ready] Main Activity : Cyber risk assessment

Cyber risk assessment is the essential element that verifies the validity of the cybersecurity design of ship IT/OT systems. possible cyber attack scenarios, cyber risk levels and technical security measures (firewall, IPS/IDS, VPN, Anti-virus, communication and data encryption, etc.) to reduce risk are identified by identifying cyber threats and vulnerabilities to key systems.

< Cyber risk assessment workshop >

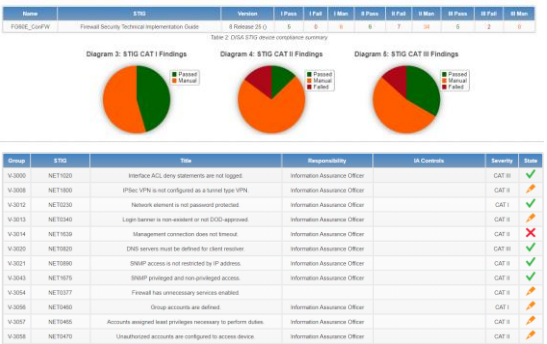
[CS Ready] Main Activity : Factory Acceptance Test & Onboard Test

It can be confirmed by on-site survey that the security capabilities of the ship cyber security system are properly implemented. Cyber security for individual systems is verified through Factory Acceptance Test(FAT), and cyber security of integrated systems such as remote access of ships on land and control of external communication interface is verified through onboard test

< Cyber security FAT >

[CS Ready] Main Activity : Vulnerability diagnosis and pen. test

Vulnerability diagnosis or penetration test can be used as a way to conduct on-site verification on cybersecurity capabilities identified through documentation review. Using various automation tools, security vulnerabilities such as PC, server, DBMS, network, web and application, malware, and cryptographic communication methods can be easily diagnosed and dealt with.



< Network vulnerability diagnosis Tool >

CS Ready Notation Document List
[Guidance for Maritime Cyber Security System Ch.2 Sec.3)

Shipbuilder who applies the CS Ready notation for the new ship should submit the following

Document	Details
Asset List	▪ **List-up of all the equipment for the system** - OS / firmware, software and version information - Hardware model and version - Port Information (USB, LAN, WiFi, Serial, etc.) - Physical location - VLANs and IP / MAC address - Anti-Virus program
Network Configuration	▪ **Ship overall system architecture drawings (logical and physical)** - Asset and Zone Definition (Based on IEC 62443 3-3 Zone & Conduit) - Perimeter protection devices (gateways, routers, firewalls, VPNs) - Data flow (unidirectional, bidirectional) - VLANs and IP addresses
System functional requirements / user manuals	▪ **Security Design Philosophy** - Cyber system / cyber security equipment configuration and function - Security configuration, functions and settings (firewall, DMZ, etc.) - Network equipment (switch, etc.) functions and settings - Cyber incident detection / function (IPS, IDS, SIEM) - Remote and wireless connection policy - Communication and data encryption policy - Software maintenance policy - Cyber incident recovery Policy - Password management, malware detection (anti-virus), etc. ▪ **Software Functional Manual / Specifications / User Manual** - Interface method / mechanism between other systems - I / O List (Control / Monitoring) - Protocol information
Asset vulnerability analysis results	▪ **Technical Security vulnerability analysis results** - Server, Security equipment, Network equipment, PC, DBMS, etc
Cyber Risk Assessment Report	▪ **Cyber Security Threat List** - Spoofing, Sniffing, Brute Force Attack, etc. ▪ **Cyber asset assessment(Confidentiality, Integrity, Availability)** ▪ **Cyber security risk acceptance criteria** ▪ **Cyber security risk identification and action plan** - Safeguard identification and action - Identify Inherent Risk and Residual Risk
Software registry and quality plan	▪ **Software Quality Management Plan** ▪ **Software inventory management (includes change management)** - Software name and publisher - Installation date, version number - Maintenance type (local / remote) - Account Type (Normal / Only) - Access control list with read, write, and execute permissions - IP / Port, License number
Incident response and recovery manual	▪ **Cyber Incident Response and Recovery Manual** - Cyber incident list - Cyber incident detection display and alarm, impact - Cyber incident response and recovery policy / flowchart - Automatic and manual recovery
Cyber security test procedures	▪ **Factory Test Procedure** ▪ **Onboard Test Procedure**

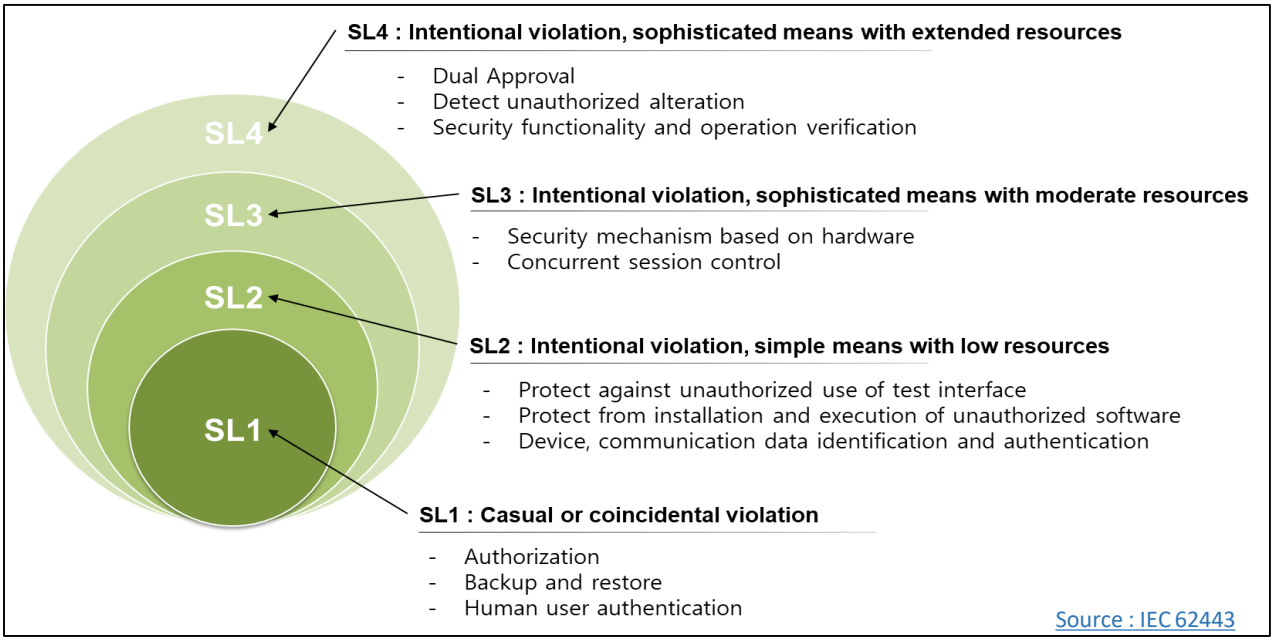
Guideline for Type Approval of Maritime Cyber Security

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.

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

Understanding Security Level (SL)



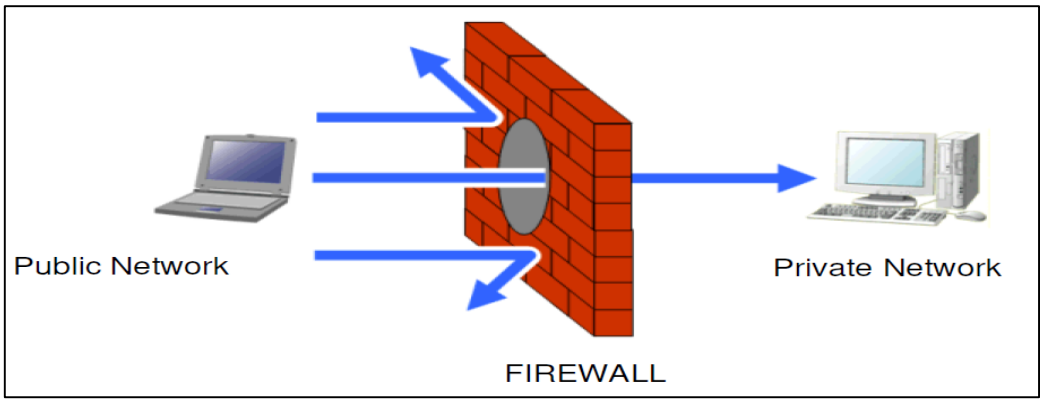
KR Type Approval of Maritime Cybersecurity Inspection Items

Network Device Requirements - Zone boundary protection (1211)

1. A network device at a zone boundary should provide the capability to monitor and control communications at zone boundaries to enforce the compartmentalization defined in the risk-based zones and conduits model. (SL 1)
2. The network component should provide the capability to deny network traffic by default and allow network traffic by exception. (SL 2)
3. The network component should provide the capability to protect against any communication through the system boundary (also termed island mode) (SL 3,4).
4. The network component should provide the capability to protect against any communication through the system boundary when there is an operational failure of the boundary protection mechanisms (also termed fail-close) (SL 3,4).

Security of physical diagnostic and test interfaces

To secure a complex network, an efficient method is to divide the network into zones and maintain security for each zone. To maintain overall security, the boundaries of each zone must also be protected. The concept of Zone & Conduit is the function of dividing each zone and protecting their respective boundaries.



< Examples of zone boundary protection with firewall >

Zone boundary protection using firewalls is a typical example. The basic concept of firewalls can be likened to the door to the house in which we live. Those with keys (allowed IP address) are allowed in, and others (denied IP address) are not. Security is maintained by minimizing access from the outside and only allowing entry to those with a registered IP address, protocols, etc. To protect against attacks from allowed IP addresses (insiders) additional IDS (Intrusion Detection Systems) or IPS (Intrusion Prevention Systems) are installed.

Explanation of Term

Maritime Cluster Networking in Korean (MacNet)

- Founded in November 2015 to create an ecosystem where the marine industry, government, academia and research institutes share technologies and information through networking and mutual cooperation, MacNet operates as a consultative body comprising 49 related organizations including shipbuilding, shipping, port, equipment, shipping and finance. In November 2019, it was re-launched as the Maritime Cluster Networking (MacNet).
- MacNet's mission is to operate a network of industry, government and academia, to give practitioners a voice in the development of the Korean Government's maritime industry policy.

Source : MacNet

Spoofing Attack

Hacking method in which an external malicious network intruder randomly configures a website to induce general users to visit, thereby gaining the user's system privileges and then stealing information by exploiting a structural flaw in the Internet protocol TCP/IP. Types of spoofing attacks include ARP spoofing, IP spoofing, DNS spoofing and email spoofing.

Source : Naver