# KR Maritime Cyber Safety News & Report

Vol. 054
Oct. 2022

Korean Register
www.krs.co.kr

# CONTENTS

# KR, Cyber Security Training to WILHELMSEN SHIP MANAGEMENT KOREA

*Editor : AHN Jongwoo, Korean Register*

On Oct. 19, KR conducted maritime cyber security training for about 50 land and sea employees of Wilhelmsen Ship Management Korea Co. Ltd. Wilhelmsen Ship Management Korea is a ship management subsidiary of Wilhelmsen, a Norwegian shipping group, and operated more than 40 ships, including Pure Car and Truck Carrier(PCTC).

In the maritime cyber security training held on that day, KR explained the definition of maritime cyber security, international response trends to cyber attacks in the maritime sector, cyber security requirements and response activities. In particular, it was said that cyber security training required by Classification Societies, OCIMF he Ship Inspection Report Programme(SIRE) and RightShip RightShip Inspection Ship Questionnaire(RISQ) can be conducted through magazines, posters, and online training on land and sea. Another major requirement, access control, was explained by examples how to manage accounts/passwords and set screen savor that can be easily done by land/sea employees.

Training was successfully conducted by land/sea employees with high interest, and after training, questions with high interest, and after training, questions and answers were given onboard cyber security training methods.

KR provides customized cyber security training for shipowners, ship managers, Shipyards and equipment companies every year, and also provides online training for customers who have difficulty in face-to-face training.

# Allianz: Best practices to improve IT security

*Editor : AHN Jongwoo, Korean Register*

*Source : SAFETY4SEA*

n a new report, cyber insurer Allianz Global Corporate & Specialty (AGCS) analyzes the latest risk developments around ransomware and outlines how companies can strengthen their defenses with good cyber hygiene and IT security practices.

n the report, AGCS identifies five trends in the ransomware space, although these are constantly evolving and can quickly change in the 'cat and mouse' race between cyber criminals and companies:

1. **The development of 'ransomware as a service' has made it easier for criminals to carry out attacks.** Run like a commercial business, hacker groups such as REvil and Darkside sell or rent their hacking tools to others.
2. **From single to double to triple extortion.** 'Double extortion' tactics are on the rise. Criminals combine the initial encryption of data or systems, or increasingly even their back-ups, with a secondary form of extortion, such as the threat to release sensitive or personal data. In such a scenario, affected companies have to manage the possibility of both a major business interruption and a data breach event, which can significantly increase the final cost of the incident. 'Triple extortion' incidents can combine DDoS attacks, file encryption and data theft – and don't just target one company, but potentially also its customers and business partners.
3. **Supply chain attacks the next big thing:** There are two main types – those that target software/IT services providers and use them to spread the malware (for example, the Kaseya or Solarwinds attacks). Or those that target physical supply chains or critical infrastructure, such as the one which impacted Colonial Pipeline.
4. **Ransom dynamics:** Ransom demands have rocketed over the past 18 months. According to Palo Alto Networks, the average extortion demand in the US was $5.3mn in the first half of 2021, a 518% increase on the 2020 average; the highest demand was $50mn, up from $30mn the previous year. The average amount paid to hackers is around 10 times lower than the average demand, but this general upward trend is alarming.

5. **To pay or not to pay:** Ransom payment is a controversial topic. Law enforcement agencies typically advise against paying extortion demands to not further incentivize attacks.

**Best practices (Partially introduced, follow URL for details)**

**#1 Ransomware identification**

- **Are anti-ransomware toolsets deployed throughout the organization?**
- **Are policies, procedures, access controls methods and communication channels updated frequently to address ransomware threats?**

**#2 Business continuity planning/incident response plan**

- **Are ransomware-specific incident response processes in place?**
- **Is regular user training and awareness conducted on information security, phishing, phone scams and impersonation calls and social engineering attacks?**

**#3 Backups**

- **Are regular backups performed, including frequent backups for critical systems to minimize the impact of the disruption? Are offline back-ups maintained as well?**

**#4 Endpoints**

- **Are endpoint protection (EPP) products and endpoint detection and response (EDR) solutions utilized across the organization on mobile devices, tablets, laptops, desktops etc.?**

**#5 Email, web, office documents security**

- **Are email gateways configured to look for potentially malicious links and programs?**

**#6 Segmentation**

- **Are physical, logical segregations maintained within the network, including the cloud environment?**

**#7 Mergers and acquisitions**

- **Are regular security audits conducted on newly-integrated entities to ensure evaluation of security controls?**

<Source: https://safety4sea.com/allianz-best-practices-to-improve-it-security/ >

# Ship Integrated Security Monitoring Measure

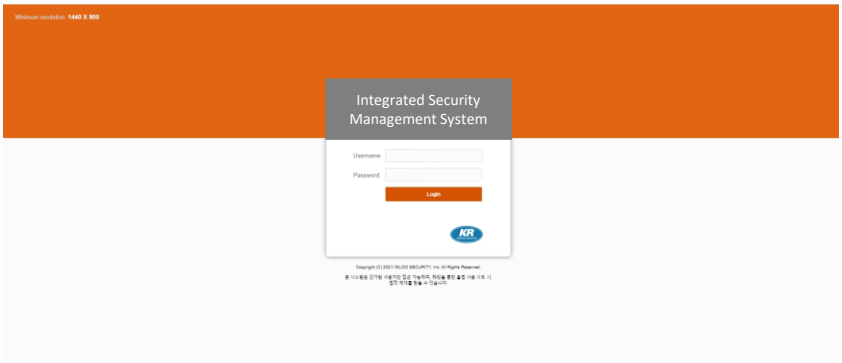
*Editor : Senior Manager Changsik Lee, IGLOO Corporation*

## Introduction

Among the cyber security trends in the maritime sector this year, the most important one is IACS UR(Unified Requirements) E26 Cyber resilience of ships and E27 Cyber resilience of on-board systems and equipment, published on April. These URs are to be s to be uniformly implemented by IACS Societies on ships contracted for construction on or after 1 January 2024, which means that cyber security is no longer an option for shipbuilding and marine industry, but requirements. Therefore, classification survey will be conducted to confirm that new cyber security UR has been reflected on the ships to which these UR are applied. In this column, I'd like to introduce 'the ships integrated security management system' technology that can meet the requirement for 'Network Operation Monitoring' among the requirements of UR E26.

## Ship Integrated Security Management System

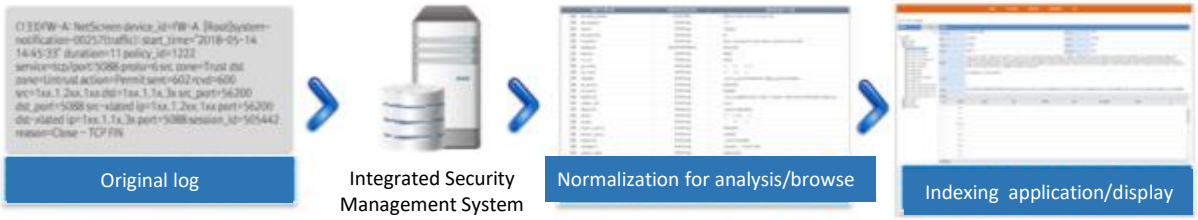
As the OT in charge of controlling ship operation and the IT connected to the external network are closely connected, products and technologies that can monitor and analyze IT and OT centrally are required. The ship integrated security management system is a SIEM(Security Information & Event Management) product capable of identifying, detecting and analyzing abnormal situations covering IT and OT.



On-shore SIEM products are products that can be operated and monitored directly by security experts and detect cyber threats through various correlation analysis, which is far from being operated by non-experts. Therefore, the ship integrated security management system should be configured so that IT non-experts such as crews can easily recognize abnormalities in cyber threats, asset status, etc. when monitoring, and anyone can conveniently monitor.

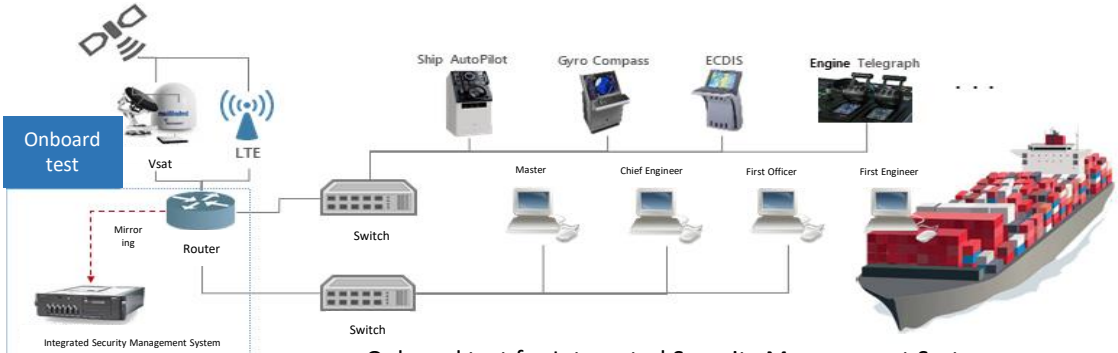
## Security log(event) gathering : Gathering threat information from various security devices

The difference between the integrated security management system and the existing SIEM products is that it is configured with OT sensor equipment. The OT sensor collects and analyzes network packets that are communicated by setting the SPAN function of router/switch equipment so that network operation is not affected. The analyzed data is collected from the module of the integrated security management system and displayed in the dashboard UI along with the data collected from other security equipment. An important component of the system is the ability to collect logs. It is possible to link data with various equipment regardless of the type of equipment, and the collected data is normalized and applied immediately without separate development.




< Log linked stage >

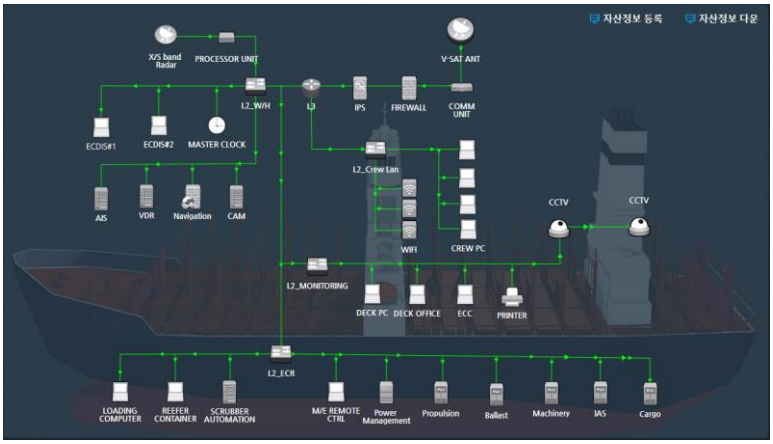
It was confirmed that this function had no problem in collecting and displaying the ship's network communication data in onboard test.




< Onboard test for Integrated Security Management System >

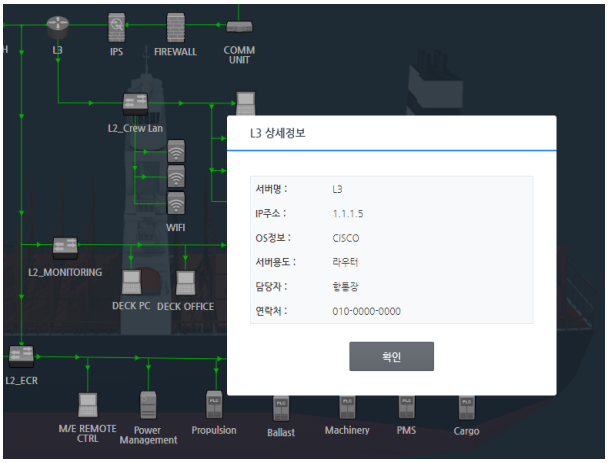
## IT/OT Asset Management : Integrated management of identified / defined asset information

The ship integrated security management system can describe the network environment in the ship with a network topology function. It provides a function that allows crews to easily check registered asset information by registering important asset information and linking it with the UI.

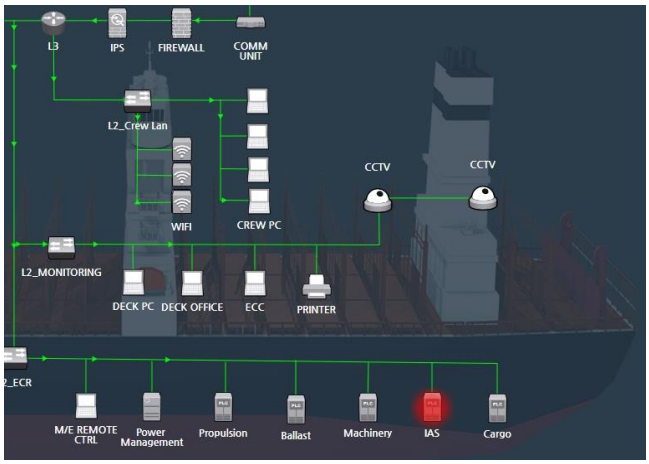



< Ship Network Environment Configuration >

In the event of a network communication/system failure of a registered asset, it is expressed as a highlight function to provide a monitoring function so that even non-IT experts can easily recognize the abnormality.




< Detailed information of the asset >

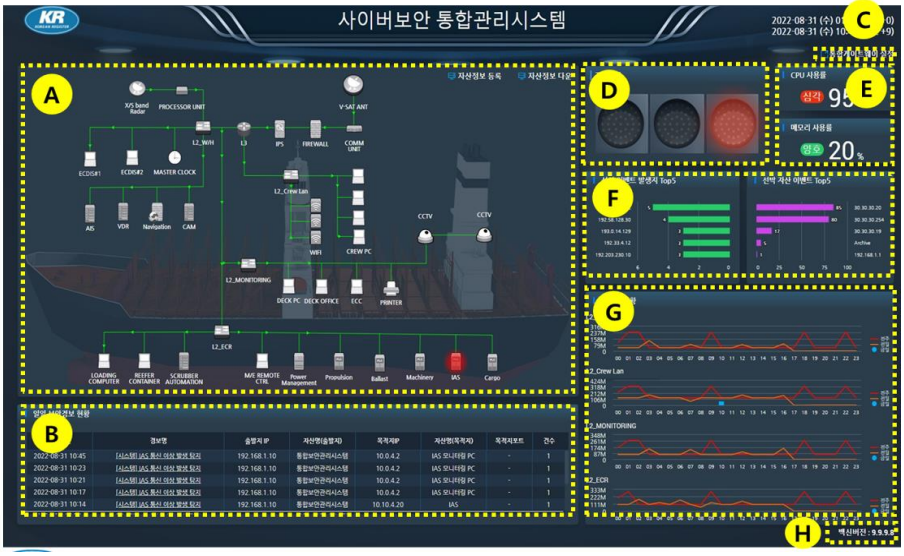



< Highlight function of the asset at abnormal situation >

## Integrated Dashboard : Provides integrated operational screens through visualization of alarm events

The ship integrated security management system UI is configured to enable comprehensive real-time monitoring of emergency notifications, security threats, and system/network status information. Unlike the existing emergency notification function on land, it was reorganized into three stages in the form of traffic lights familiar to operation on ships. Depending on the risk of a predefined security policy, security threats are automatically changed to dangerous

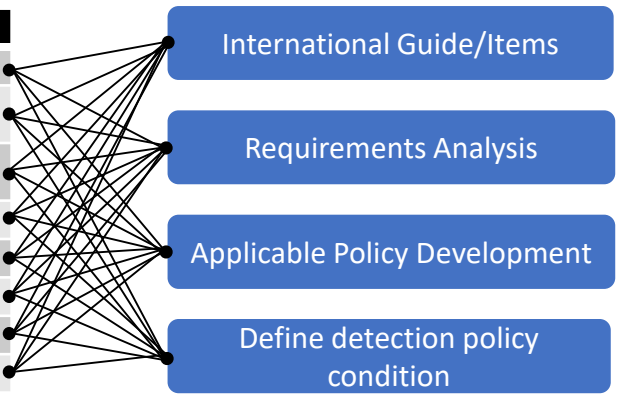
(yellow) and high (red) when they occur, and are configured to be easily recognized by the stakeholders. It also displays the status of system resources and network traffic so that important resource information on the ship can be checked in real time.




A. Network topology map
B. Daily security alarm status
C. Integrated gateway configuration
D. Emergency alarm
E. System status
F. Origin of threat event Top 5
G. Traffic status
H. Anti-virus program engine info.

As such, the ship integrated security management system aims to prepare a system optimized for maritime cyber security in consideration of the necessity of ships and sailors. The cyber threat detection policy was also applied by analyzing the requirements of the international maritime guidelines and developing a detection policy applicable to ships.

| No. | Guidelines | Name |
|---|---|---|
| 1 | Guidance of Maritime Cyber Security | Korean Register |
| 2 | The Guidelines on Cyber Security Onboard Ships | BIMCO |
| 3 | Guidelines on maritime cyber risk management | IMO |
| 4 | Rec. 166 | IACS |
| 5 | UR E26 | IACS |
| 6 | UR E27 | IACS |
| 7 | IEC 62443 3-3 | IEC |
| 8 | IEC 62443 4-2 | IEC |




< Cyber Threat Detection Policy>

The system for ship monitoring needs to be lightweight in consideration of the physical and network limitations of the ship, and the product is being reflected in the first half of next year. The process of reflecting the characteristics of these ships will lay the foundation for cyber security of ships in the future and establish an integrated security system that can preemptively respond to cyber threats.

# 5G`s Effects and Cyber Threats on the Maritime

*Editor : YOO Jinho, Korean Register*

## series news

① What is 5G?

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

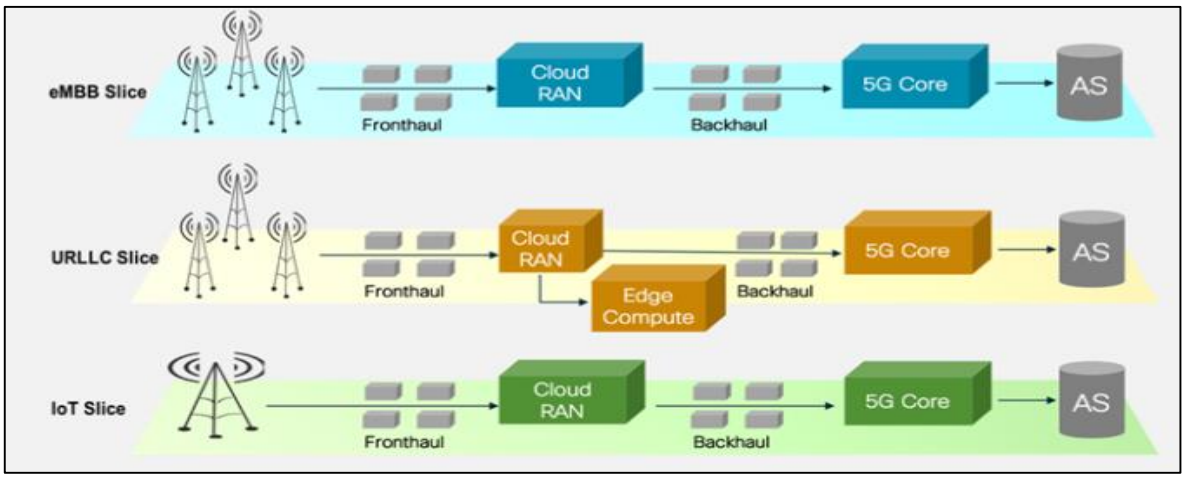
③ Comparison between LTE centralized network and 5G distributed network

④ Role of wireless backhaul technology and 5G satellites in 5G standards

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

## 5G network structure and network slicing

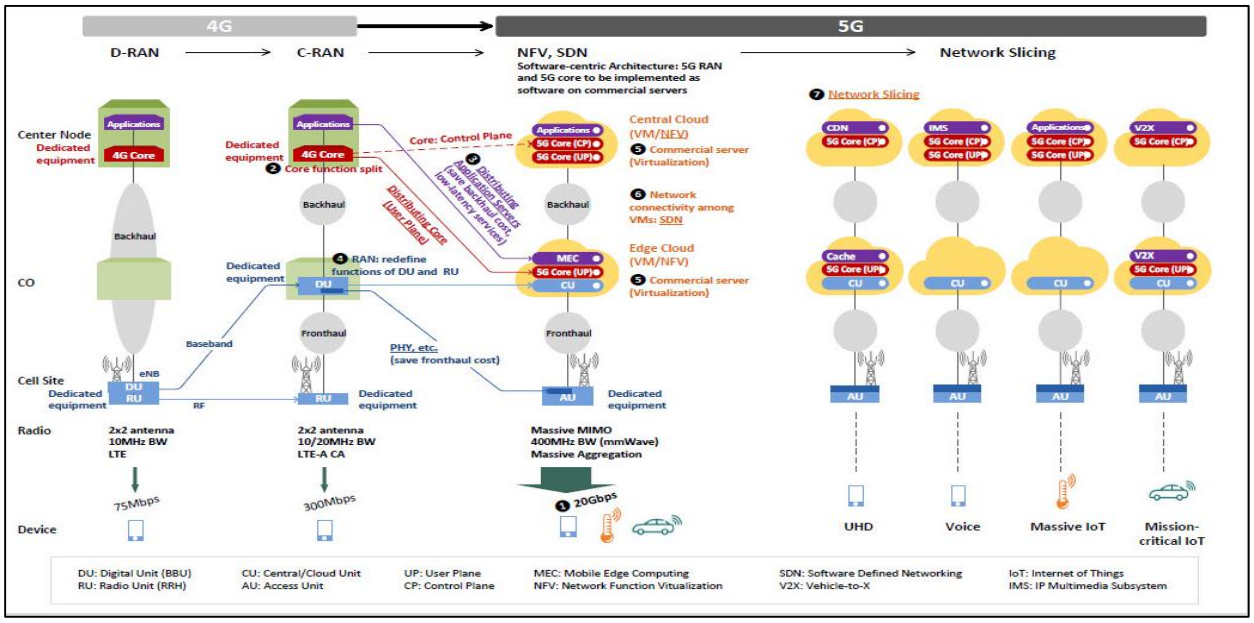
As explained in the August newsletter, 5G has a service-based architecture based on the requirements of each industry. In addition, the separation of CP/UP (Control Plane/User Plane) functions and the modularization of network function (NF) are the main features. The advantages of the 5G network structure are that it can modularize the network functions required by each service such as ships, IoT devices, automobiles, factories, etc., and virtualize them into the optimized network. In this way, a virtual dedicated network technology is called a network slicing technology to divide one physical network into multiple logical networks to guarantee communication performance by service group.




Source : https://www.netmanias.com/en/?m=view&id=blog&no=13311&kw=E2E+Network+Slicing&page=1

## 5G network structure and network slicing (Continue Page)

In other words, as HDD is partitioned into C and D, it virtualizes the network and provides a dedicated network specialized for the service for various services with different characteristics. For example, in order to respond immediately to the risks that occur on the road, the network associated with autonomous vehicles is most important to perform ultra-low latency of 1 ms. On the other hand, water companies related to Smart City are important for ultra-capacity connection performance that can transmit small amounts of data at the same time on thousands of devices, even though the speed is somewhat slow. So, Is it 5G phone network, 5G Massive IoT network, 5G mission-critical IoT network separately? It is the network slicing technology that reduces the cost by creating several logical networks on one physical delusion.




Source : https://www.netmanias.com/en/?m=view&id=oneshot&no=8393

## What is the impact of 5G on the marine industry?

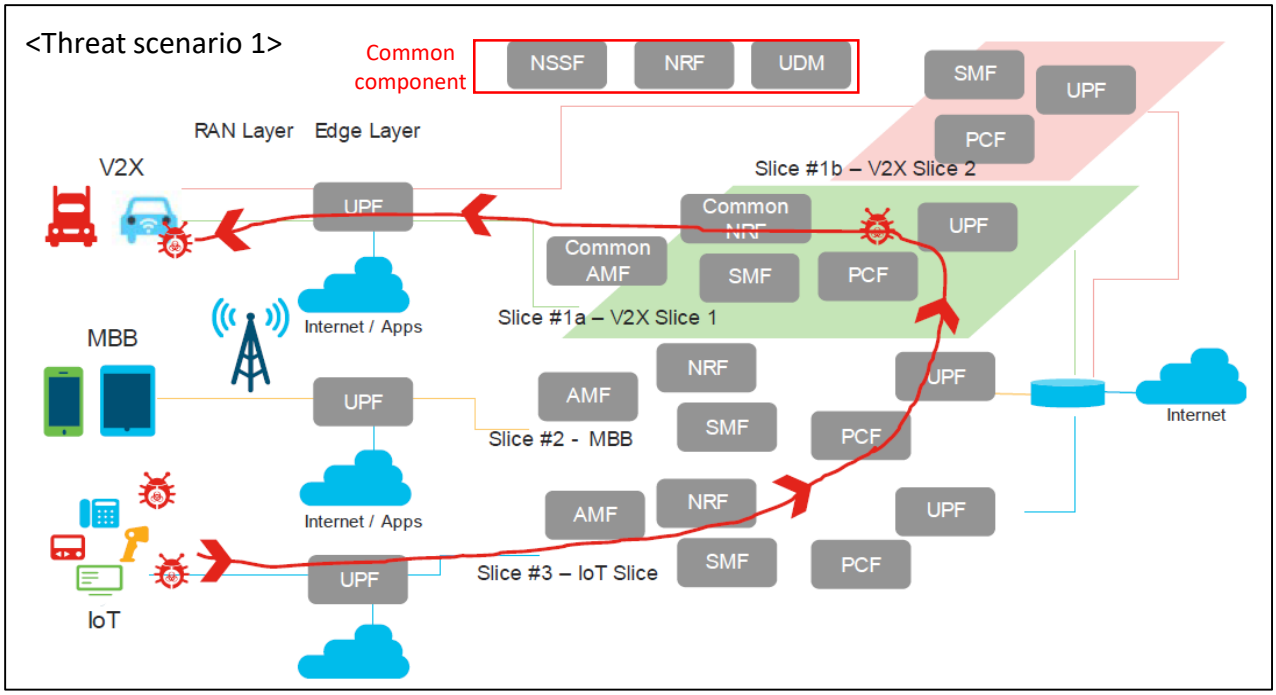
In June 2019, the IMO Maritime Safety Commission 101st meeting approved the provisional guidelines for the test operation of Maritime Autonomous Surface Ship (MASS), and the marine industry has been conducting research for the automation and digitalization of existing marine related industries such as MASS, smart port. For the digitalization of the existing marine industry, the development of communication infrastructure is one of the key factors, and international standardization research is also underway to apply 5G. 5G international standardization is carried out in 3GPP. In other words, if the 5G network slicing structure

## What is the impact of 5G on the marine industry? (Continue Page)

defines the requirements of the marine environment-specific Maritime slice and technology development is carried out, the marine industry is expected to emerge commercial technologies and solutions.

## 5G Cyber Risk Factors - Threat Factors of 5G Network Slicing Structures

5G makes networks very flexible. They can provide exactly what is required because NFs can be established and removed on a per-need basis and used simultaneously by multiple different slices. Also, network Operations, Administration and Management (OAM) can be simplified and made more flexible. Service providers can utilize automated tools to provide the network services with the predefined redundancy, capacity and other capabilities. Generally, some of these tools and capabilities have been available in the network prior to 5G.




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

There are common resources and components shared between all the slices, such as the NSSF (Network Slice Selection Function). The rest of the slices may have individual resources assigned, such as AMF, SMF, PCF layers that are dedicated functions catering to specific slices. the attack could be multi-factored by allowing the malware to have the ability to deplete the resources of the slice, therefore causing DoS (Denial of Service) to the actual subscriber. An attacker may also exhaust resources common to multiple slices, causing denial of service or

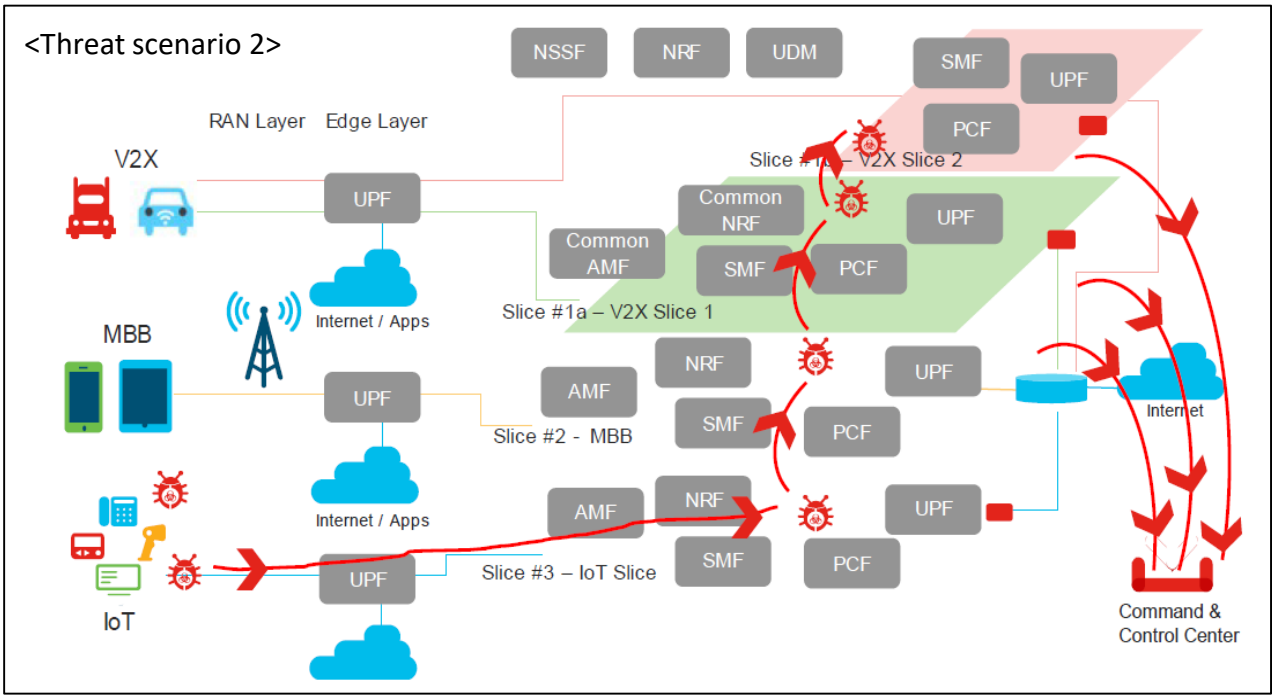
## 5G Cyber Risk Factors - Threat Factors of 5G Network Slicing Structures
(Continue Page)

service degradation in other slices as well. This leads to severe degradation in the offered network services. As a cloud native architecture, 5GC (5G Core) has all the functions virtualized that provide the added flexibility required for network slicing. However, this leads to another threat vector. Side channel attacks, coupled with improper isolation between network slices, leads to data exfiltration. This is critical in sensitive parts of the mobile network such as billing, charging and subscriber authentication layers.

## 5G Cyber Risk Factors - Threat Factors of 5G Network Slicing Structures

As shown in Figure of threat scenario 2, if the slices and the components within the slice are not adequately isolated, the attacker could access other slice components using the infected device or endpoint in another slice. Figure 4.6 shows the infected device allowing the attacker access to the slice resources. Ultimately, the other slices are exposed and data exfiltration proceeds to an external server (a C&C center, for example).

<Threat scenario 2>




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

Once the attacker gathers all the network's information behind the firewall, they could launch an attack on subscribers based on the leaked information. Furthermore, the attacker could use the information for fraudulent financial gains. Network slicing allows operators to offer

## 5G Cyber Risk Factors - Threat Factors of 5G Network Slicing Structures
(Continue Page)

customized services to customers. It is possible for 5G systems, based on operators' policies, to provide standardized APIs to create, modify, delete, monitor, and update the services of network slices. Slice management also contains critical threat vectors if not secured. Additionally, as per 3GPP standards specifications, the management interface between the Network Slice Management Function (NSMF) and the Communication Service Management Function (CSMF) or between Communication Service Provider (CSP) and Communication Service Customer (CSC) is specified.

Furthermore, interfaces are also specified for the operation phase of management aspects of a Network Slice Instance (NSI), supervision, and performance reporting.

# KR CS++


| 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 |

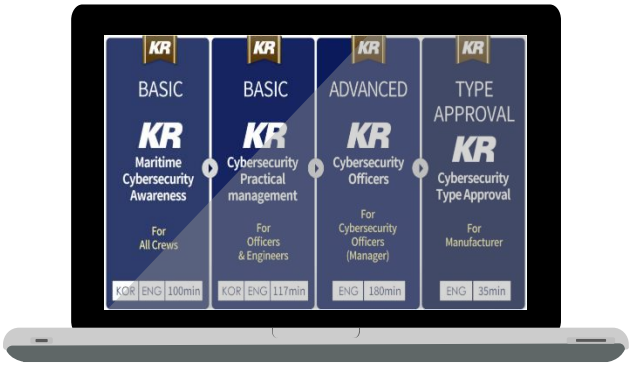
KR launched KR CS++, maritime cybersecurity training tool.

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/](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 ok Korea
Tel +82 70 8799 8595
Fax +82 70 8799 8594
www.krs.co.kr