KR Maritime Cyber Security

News from KOREAN REGISTER

Vol. 019

November 2019

KR Cyber Security Activities

- German 'Cluster for Building Marine Cyber Security Infrastructure‘
- European Maritime Cyber Resilience Forum
- Singapore Shipping company customized cyber security education

[Series news] ④ Role of Satellites in 5G Standard

Understanding Cyber Threats(OWASP Top 10)

Guidelines for Type Approval of Maritime Cyber Security

Explanation of Term

German Maritime Cyber Security Infrastructure Cluster

At the invitation of the German Maritime Cluster Norddeutschland (MCN), the Korean Register (KR) has participated in the "Cluster for Maritime Cyber Security Infrastructure" meeting, held in Bremerhaven, Germany on 30 October. The MCN was founded in 2011 with the goal of promoting and developing cooperation across the North German maritime sector.

KR highlighted the latest trends in maritime cybersecurity, clarifying OCIMF's and RightShip's cybersecurity requirements, as well as introducing KR's latest activities on cybersecurity technology and certification services.

At the same meeting, Dr Siv Hilde Houmb gave a valuable and interesting live demonstration of how ISO27001-based cybersecurity audits work. In 2020, KR will issue new guidelines in response to the IMO Resolution MSC.428 (98). KR will also provide cybersecurity seminars and training for German and other interested shipping companies on the new guidance.

The European Maritime Cyber Resilience Forum

KR attended Digital Ship's European Maritime Cyber Resilience Forum held in London, UK on 31 October to explore the latest maritime cybersecurity trends and technical information from Europe.

The forum was attended by maritime industry experts including MAN Energy Solution, the UK National Cyber Security Association and Beazley.

MAN Energy Solution insisted that partners, as well as owners, seafarers and onshore employees, should all take part in strengthening cybersecurity. Beazley provided an overview of cybersecurity insurance for ships and insurance offered by different companies.

Plymouth University announced that it would establish a new Cyber-SHIP Lab to simulate a ship's bridge system and study the impact simulated cyber-attacks on systems connected to the bridge.

KR Cyber security Activities #3

Customized training for cybersecurity in Singapore

The Korean Register conducted customized training service for cybersecurity awareness on 14-15 November. The attendees included: 37 supervisors of Diamond Ship Management Pte Ltd, Fleet Ship Management Pte Ltd and MSI Ship Management Pte Ltd in Singapore. Following IMO Resolution MSC.428 (98) the training set out to provide trainees with the basic knowledge and means to identify cyber threats, perform cyber risk assessments, implement cyber risk control measures, and detect, respond and recover from cyber incidents. KR asked the attendees for feedback to make sure that the training was informative and practical and included real cyber attack cases and videos to raise awareness of the risks. The trainees cybersecurity capabilities were further strengthened through a cyber risk assessment workshop. KR has provided customized cybersecurity training to help shipbuilders respond to international cybersecurity issues, these have included Songa Shipmanagement, Sansho Korea, and VL Enterprise Plc. Moving forward KR plans to strengthen and enhance its specialized cybersecurity education for shipbuilders, shipyards, and equipment companies.

<Diamond/Fleet SM>

<MSI SM>

Maritime Cyber Security Awareness Training Course Introduction

Maritime Cyber Security Awareness Training

11-15 November, Singapore

Course Introduction and Time Table

Trainer: Jeoungkyu Lim(Korean Register)
Sanghoon Choi(Korean Register)

1 Course Introduction

As Information and Communication Technology (ICT) becomes widely applied to the shipping industry, cyber threats and vulnerabilities related to digitalization, integration and automation of processes and system in shipping have also emerged. According the IMO Resolution MSC.428(98), administrations should ensure that cyber risks are appropriately addressed in existing safety management systems (as defined in the ISM Code) no later than the first annual verification of the company's Document of Compliance after 1 January 2021.

This one day awareness training course provides the trainees with the knowledge and method to respond to the maritime cyber security issues.

2 Time Table

Time	Category	Details	Trainer
09:00 - 09:50	Maritime cyber security overview	• Introduction • International response in maritime industry • KR cyber security activities	JK Lim
10:00 - 10:50	Administrative security	• Cyber security management system • Maritime cyber security organization • Human security • TMSA Element 13 : Maritime Security	JK Lim
11:00 - 11:50	Cyber Asset / Cyber Threat	• Cyber asset management overview • Identify asset • Asset criticality • Maritime Cyber threat • Threat list	SH Choi
12:00 - 13:00	Lunch Break		
13:00 - 13:50	Physical security	• Purpose and method of physical security • KR Server room physical security • Physical security by risk assessment	JK Lim
14:00 - 14:50	Technical security	• Network security • Vulnerability analysis • PC security vulnerability analysis	SH Choi
15:00 - 15:50	Understanding of maritime cyber security risk assessment	• Understanding of maritime cyber security and risk assessment • KR cyber security risk process • Application cases	JK Lim
16:00 - 17:00	Workshop	• Hands-on	SH Choi

[Series news] ④

Role of Satellite in 5G Standard

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

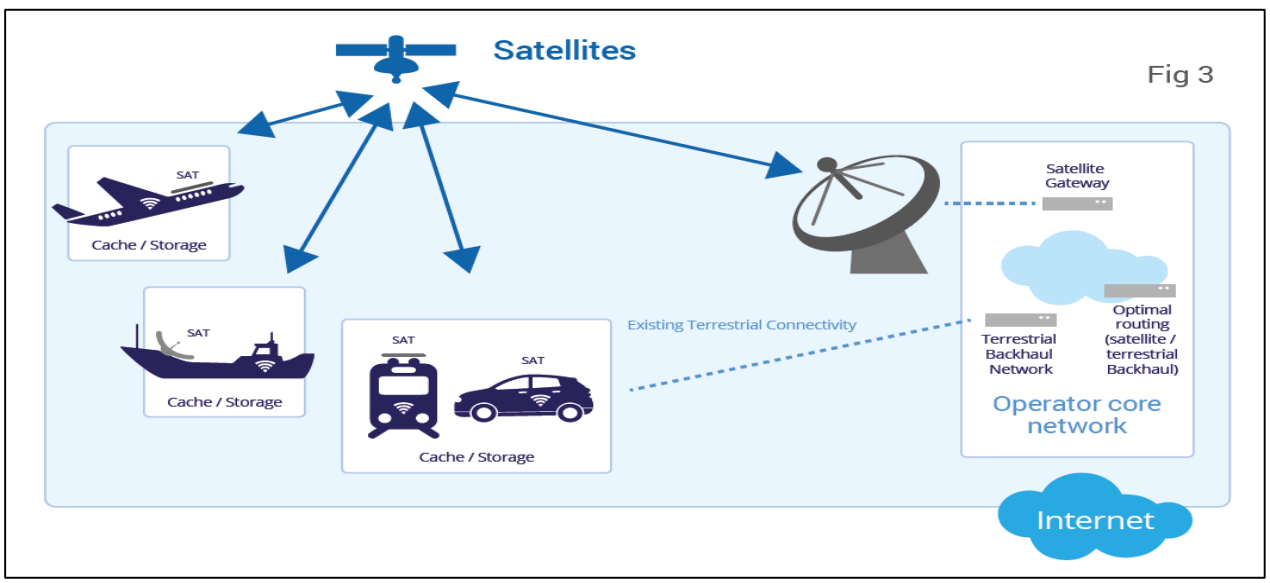
③ **Comparison between LTE centralized network and 5G distributed network**

④ **Role of satellites in G standards**

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

The Role of Satellite in the 5G Standard

At the moment, 3G and LTE standards are designed around communication between ground stations and terrestrial terminals. But, in the 3rd Generation Partnership Project (3GPP), 5G is being standardized for use in non-terrestrial networks, including satellites, drones, HAPS, and aircraft. KR is designing 5G standards and related components. In other words, the satellite is a non-terrestrial 5G base station and the land-based station will be similar in form. This will expand 5G connectivity across islands, seas and desert areas, that cannot be covered by ground stations alone.

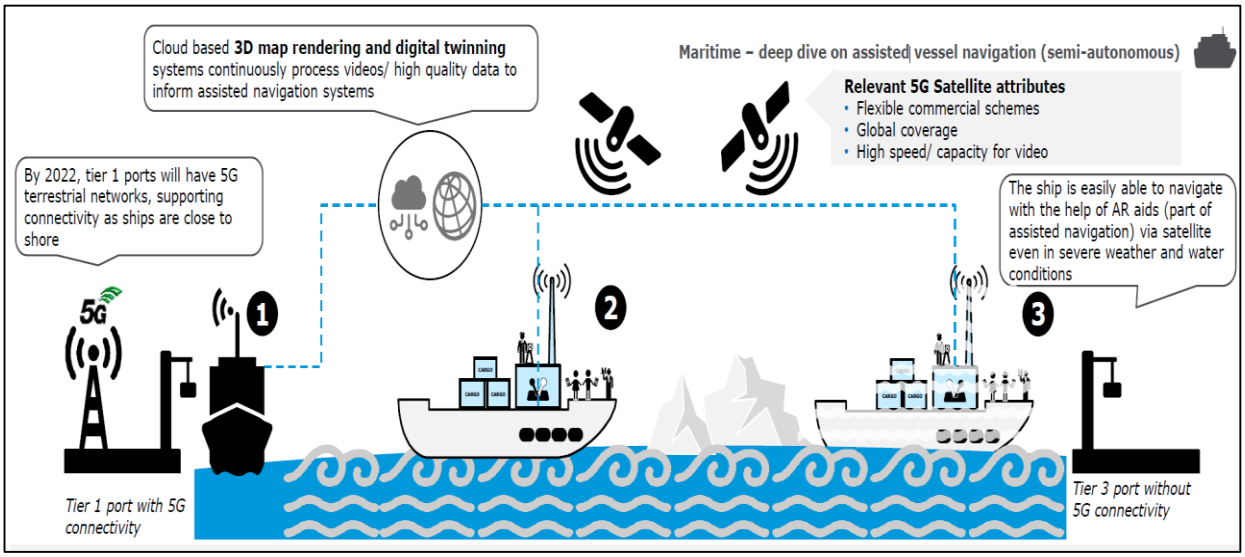


Source : EESA, Satellite for 5G –Tomorrow's connected World 5G Satellite Initiative (S45G)Presentation

Impact of 5G satellites on the maritime industry

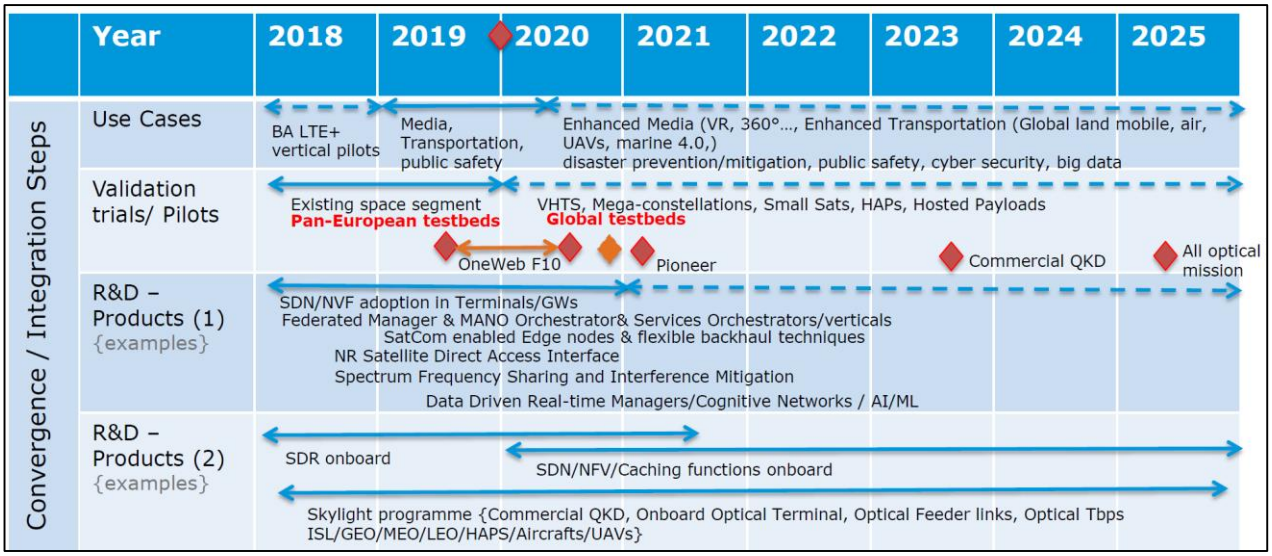
Ships still use satellites to support VSAT and Inmarsat voice and data communication. But, once 5G satellites are gradually integrated and commercialized, high-quality voice and data communications and cybersecurity will be available at a lower price point.

As worldwide research on autonomous navigation ships (MASS) continues, 5G communications will play an increasingly important role in strengthening connectivity and cybersecurity



Source : EESA, Satellite for 5G –Tomorrow's connected World 5G Satellite Initiative (S45G)Presentation

According to the European Space Agency's (ESA) plan for 5G satellite implementation, trials are expected to be completed by 2020 and a case will be developed for 5G usage for Marine 4.0, by 2025. As a result existing offshore businesses, such as shipping companies and the equipment industry will need to prepare for the development of new digital services from the 5G satellite once they are available.



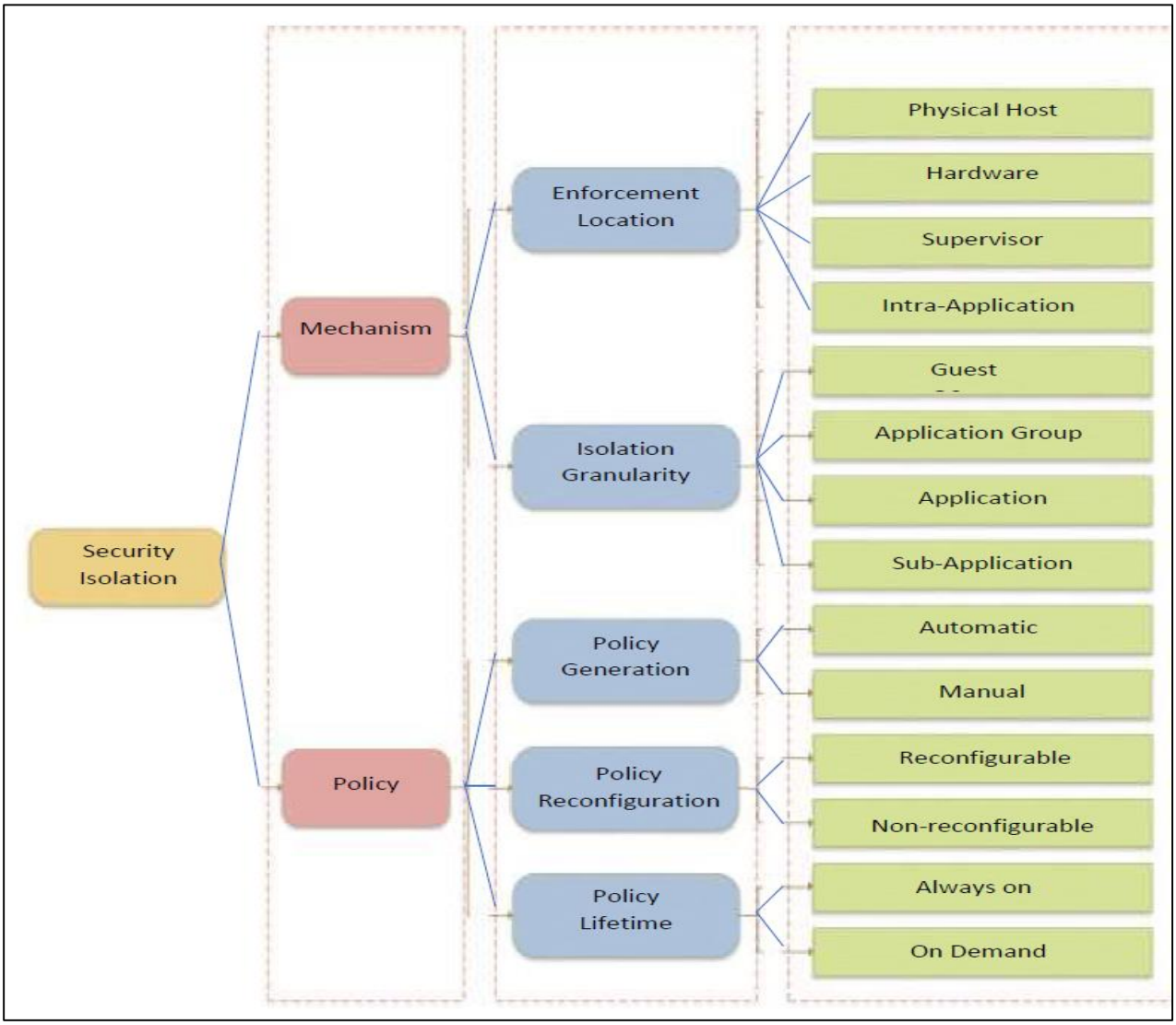
Source : EESA, Satellite for 5G –Tomorrow's connected World 5G Satellite Initiative (S45G)Presentation

Mitigating cybersecurity threats on IoT devices using 5G technology

5G is integrating technology for wired networks as well as satellites. Therefore, based on the model applied to mitigate cybersecurity threats in the 5G standard, KR will introduce it as a reference model to address cyber threats in ships and companies.

For ships, the security isolation of IT and OT systems is necessary. To achieve this, 5G applied the following model. Security isolation issues can generally be configured in two ways, depending on the threat model. The technical mechanism addresses the need for security isolation. The design subcategories considered are enforcement location and isolation granularity; another method is to apply policy design.

Cybersecurity is an important factor to be considered in the ship design stage. Cybersecurity threat can be reduced by policy design, without affecting the system by installing of a heavy cybersecurity solution in the OT system.



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

Understanding Cyber Threats(OWASP Top 10)

Understanding cyber threats

A cyber threat is any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, or the nation state through unauthorized access to an information system, causing destruction, disclosure, modification of information, and/or denial of service (source: NIST SP: 800-128). Cyber threats need to be categorized periodically to identify the vulnerabilities of assets, and the potential impact on that asset.

KR Guidance for Maritime Cyber Security System requirement(CS1)

204.1 Risk Management : External environmental factors affecting the environments of internal information technology and operational technology should be identified and cataloged as threats.

OWASP Top 10

The Open Web Application Security Project (OWASP) is an open source web application security project, researching web exposure, malicious files and scripts, and security vulnerabilities. The OWASP Top 10, which is frequently referred to, highlights the top web application vulnerabilities, it was published in 2004, 2007 , 2010, 2013 and 2017. In this newsletter we will analyze the **'A10 : 2017 – Insufficient Logging&Monotoring'**

OWASP Top 10 - 2013	→	OWASP Top 10 - 2017
A1 – Injection	→	A1:2017-Injection
A2 – Broken Authentication and Session Management	→	A2:2017-Broken Authentication
A3 – Cross-Site Scripting (XSS)	↘	A3:2017-Sensitive Data Exposure
A4 – Insecure Direct Object References [Merged+A7]	U	A4:2017-XML External Entities (XXE) [NEW]
A5 – Security Misconfiguration	↘	A5:2017-Broken Access Control [Merged]
A6 – Sensitive Data Exposure	↗	A6:2017-Security Misconfiguration
A7 – Missing Function Level Access Contr [Merged+A4]	U	A7:2017-Cross-Site Scripting (XSS)
A8 – Cross-Site Request Forgery (CSRF)	☒	A8:2017-Insecure Deserialization [NEW, Community]
A9 – Using Components with Known Vulnerabilities	→	A9:2017-Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards	☒	A10:2017-Insufficient Logging&Monitoring [NEW,Comm.]

Source : OWASP Top 10 Project

OWASP Top 10 'A10 : 2017 - Insufficient logging and monitoring'

Insufficient logging and monitoring can occur at any time. Auditable events such as logins, login failures, and critical transactions are not logged. Warnings and errors do not generate log messages, are inappropriate or unclear. Application and API logs of suspicious activity may not be monitored, and logs may only be stored locally. Therefore, an automated process is needed to inform a user of when certain alerts are triggered or for where certain alert thresholds are reached so that appropriate action can be taken (e.g. SIEM).

Logs should back up and synchronize with other servers. The attacker should not be able to clear all logs after hacking the server. Review the system and verify that all the important actions have been recorded. The verification should include logins, important transactions, and password changes for future forensics.

Scenario#1

The open-source project forum software run by a small team was hacked into a flaw in the software; attackers removed the internal source code store, which included the following version and all the forum contents. Although source codes could be recovered, the absence of monitoring, logging, or warnings caused much greater disadvantages

Source : hackeone.blogspot.com

Scenario#2

An attacker scans to find a user using a common password. You can use this password to steal all accounts. For all other uses, this scan leaves only one false login record. A few days later, you can repeat this task with a different password.

Source : hackeone.blogspot.com

Is the Application Vulnerable?

Insufficient logging, detection, monitoring and active response occurs any time:

- Auditable events, such as logins, failed logins, and high-value transactions are not logged.
- Warnings and errors generate no, inadequate, or unclear log messages.
- Logs of applications and APIs are not monitored for suspicious activity.
- Logs are only stored locally.
- Appropriate alerting thresholds and response escalation processes are not in place or effective.
- Penetration testing and scans by DAST tools (such as OWASP ZAP) do not trigger alerts.
- The application is unable to detect, escalate, or alert for active attacks in real time or near real time.

You are vulnerable to information leakage if you make logging and alerting events visible to a user or an attacker (see **A3:2017-Sensitive Information Exposure**).

How to Prevent

As per the risk of the data stored or processed by the application:

- Ensure all login, access control failures, and server-side input validation failures can be logged with sufficient user context to identify suspicious or malicious accounts, and held for sufficient time to allow delayed forensic analysis.
- Ensure that logs are generated in a format that can be easily consumed by a centralized log management solutions.
- Ensure high-value transactions have an audit trail with integrity controls to prevent tampering or deletion, such as append-only database tables or similar.
- Establish effective monitoring and alerting such that suspicious activities are detected and responded to in a timely fashion.
- Establish or adopt an incident response and recovery plan, such as NIST 800-61 rev 2 or later.

There are commercial and open source application protection frameworks such as OWASP AppSensor, web application firewalls such as ModSecurity with the OWASP ModSecurity Core Rule Set, and log correlation software with custom dashboards and alerting.

Source : OWASP Top 10 - 2017

Guideline for Type Approval of Maritime Cyber Security

Understanding Guideline for Type Approval of Maritime Cyber Security

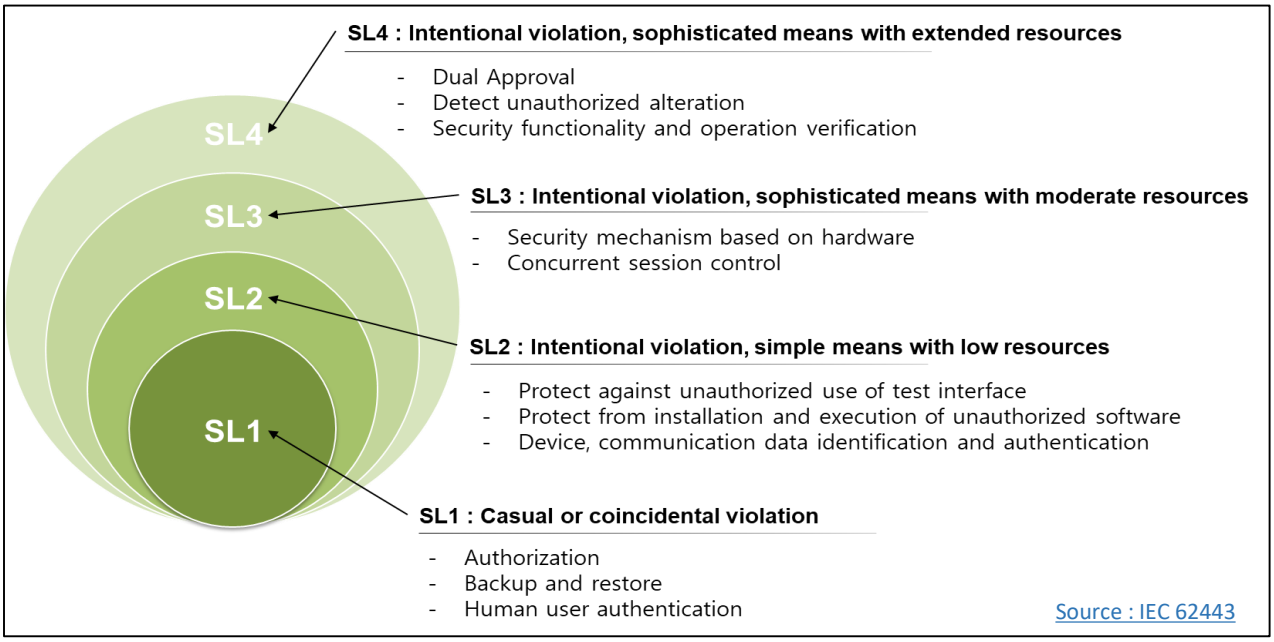
Type approval is to certify for the manufacturers of equipment for marine use that equipment comply with the provisions for the type approved products in the Guidance, where deemed satisfactory by the Society as the results of carrying out the examination, tests and inspection specified in the Guidance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

Use of cryptography (503)

If cryptography is required, the component should use cryptographic security mechanisms according to internationally recognized and proven security practices and recommendations. (SL1,2,3,4)

Guidelines for Encryption Application

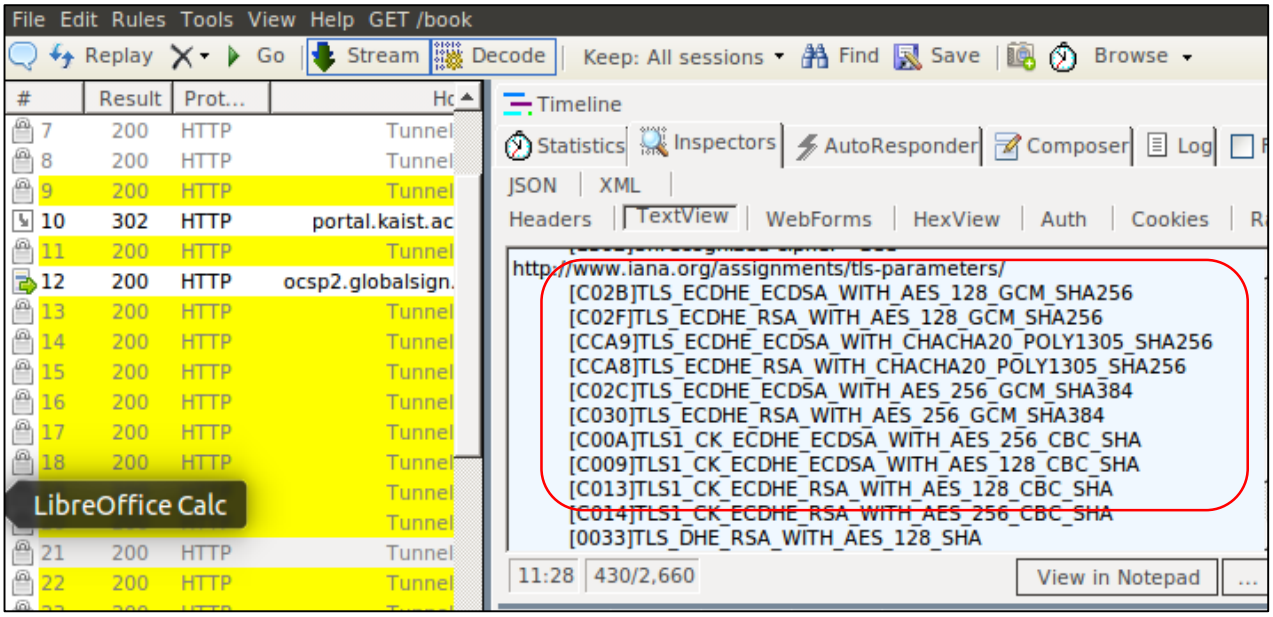
Encryption means cryptographic transformation of data into a form that conceals the data's original meaning to prevent it from being known or used. (Source: NIST SP: 800-82).

Encryption is a good way to protect confidentiality of saving important data, internal / external communication data and backup. But the algorithms proved as vulnerable should not be used.

The minimum requirements for encryption are as follows.

1. The algorithms (MD5,SHA-0, SHA-1, DES, 3DES) that are proved to be vulnerable should not be used.
2. In case of using asymmetric key, key length to be more than 2048 bit and encrypted with RSA or higher.
3. In case of using symmetrical key, key length to be more than 256 bits and encrypted with AES or higher.

'Use of cryptography' is common requirements for security level 1 to 4, and manufacturers of equipment who would like to apply cyber security type approval of Korean Register required to prove that the encryption algorithm the system/equipment used is not vulnerable.



<Examples of encryption confirmation using FIDDLER, one of the encryption diagnostic tools>

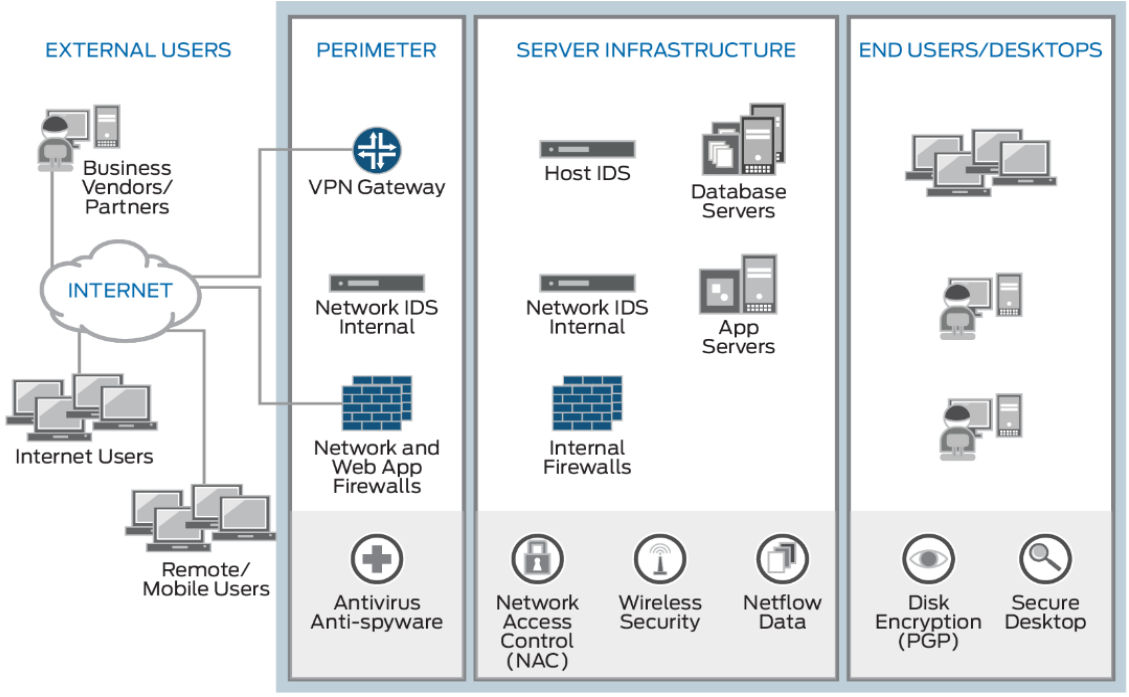
Explanation of Term

SIEM

Security Information and Event Management (SIEM) software collects, stores, and analyzes logs from the perimeter to the end-user. Threats can be monitored in real-time, for rapid attack detection, prevention, and response along with comprehensive security reporting and compliance management.

SIEM software logs event records from sources across the network, enabling long-term analysis of security events. Real-time reporting provides a comprehensive defence for your organization's IT security.

Source : https://www.juniper.net



Cryptography

- Hash function (non-decryption): A cryptographic technique that receives arbitrary length information and outputs a fixed-length ciphertext (hash value), so that the encrypted information cannot be decrypted. Secure password management is possible because the original user password is not known from the stored passphrase (hash value) (e.g. SHA-512).

- Block encryption algorithm (decryption possible): It divides the input value (social security number, account number), into a particular block size and encrypts each block, using a secret key that is only shared between the sender and receiver (e.g. AES 256).

Source : KISA, cryptographic implementation guide