KR Maritime Cyber Safety News & Report

Vol. 056
Dec. 2022

Korean Register
www.krs.co.kr

CONTENTS

- Notice for subscribers -

Due to internal circumstances, KR Maritime Cyber Safety News and Reports will be published quarterly from 2023, so we ask you for understanding.

Allianz: Cyber Risk Trends 2022

Source : SAFETY4SEA

Ransomware remains a top cyber risk for organizations globally while business email compromise incidents are on the rise and will increase further in the 'deep fake' era, says a new report from Allianz Global Corporate & Specialty (AGCS).

At the same time, the war in Ukraine and wider geopolitical tensions are a major concern as hostilities could spill over into cyber space and cause targeted attacks against companies, infrastructure or supply chains.

The insurer's annual review of the cyber risk landscape also highlights the emerging threats posed by the growing reliance on cloud services, an evolving third-party liability landscape that means higher compensation and penalties, as well as the impact of a shortage of cyber security professionals.

Such potential vulnerabilities mean that today a company's cyber security resilience is scrutinized by more parties than ever before, including global investors, meaning many firms now rank it as their major environmental, social, and governance (ESG) risk concern, the report notes.

"The cyber risk landscape doesn't allow for any resting on laurels. Ransomware and phishing scams are as active as ever and on top of that there is the prospect of a hybrid cyber war"

says Scott Sayce, Global Head of Cyber at AGCS and Group Head of the Cyber Centre of Competence.

Around the world, the frequency of ransomware attacks remains high, as do related claims costs. There was a record 623 million attacks in 2021, double that of 2020.

Although frequency reduced by 23% globally during the first half of 2022, the year-to-date total still exceeds that of the full years of 2017, 2018 and 2019, while Europe saw attacks surge over this period.

Ransomware is forecast to cause $30bn in damages to organizations globally by 2023. From an AGCS perspective, the value of ransomware claims the company was involved in together with other insurers, accounted for well over 50% of all cyber claims costs during 2020 and 2021.

Double and Triple extortion now the norm

"The cost of ransomware attacks has increased as criminals have targeted larger companies, critical infrastructure and supply chains. Criminals have honed their tactics to extort more money," Mr. Sayce explains.

"Double and triple extortion attacks are now the norm – besides the encryption of systems, sensitive data is increasingly stolen and used as a leverage for extortion demands to business partners, suppliers or customers"

Ransomware severity is likely to remain a key threat for businesses, fueled by the growing sophistication of gangs and rising inflation, which is reflected in the increased cost of IT and cyber security specialists.

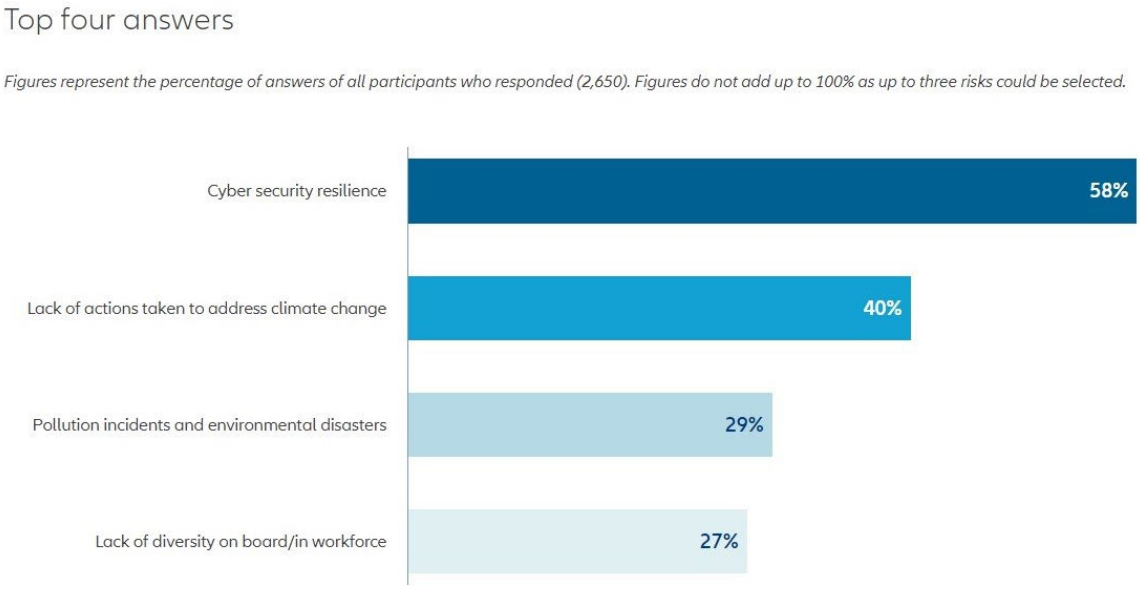
Increasingly, smaller and mid-sized companies which often lack controls and resources to invest in cyber security are being targeted by gangs as larger businesses invest more heavily in security. Gangs are also using a wide range of harrassment techniques, are tailoring their ransom demands to specific companies and are using expert negotiators to maximize returns.

Sophisticated scams

Business email compromise (BEC) attacks continue to rise, facilitated by growing digitalization and availability of data, the shift to remote working and, increasingly, 'deep fake' technology and virtual conferencing.

BEC scams totalled $43bn globally from 2016 to 2021 according to the FBI, with a 65% spike in scams between July 2019 and December 2021 alone. Attacks are becoming more sophisticated and targeted with criminals now using virtual meeting platforms to trick employees to transfer funds or share sensitive information.

Increasingly, these attacks are enabled by artificial intelligence enabling 'deep fake 'audio or videos that mimic senior executives. Last year, a bank employee from the United Arab Emirates made a $35mn transfer after being misled by the cloned voice of a company.



The threat of cyber war

The war in Ukraine and wider geopolitical tensions are a major factor reshaping the cyber threat landscape as it increases the risk of espionage, sabotage and destructive cyber-attacks against companies with ties to Russia and Ukraine, as well as allies and those in neighboring countries.

State-sponsored cyber acts could potentially target critical infrastructure, supply chains or corporations.

"As yet the war between Russia and Ukraine has not led to a notable uptick in cyber insurance claims, however it does point to a potentially increased risk from nation-states"

Mr. Sayce explains.

Although acts of war are typically excluded from traditional insurance products, the risk of a hybrid cyber war has accelerated efforts in the insurance market to address the issue of war and state-sponsored cyber attacks in wordings and provide clarity of cover for customers.

AGCS identified a number of other trends in the 'Cyber: The changing threat landscape' report including:

- **Hackers zero in on vulnerable supply chains:** Supply chain attacks – whether on critical infrastructure such as the Colonial Pipeline or on cloud services – have emerged as a significant risk. Increasingly, ransomware gangs use the threat of disruption to pressure firms into paying ransoms, with manufacturing companies particularly vulnerable.
- **Cloud outsourcing:** Companies continue to shift their services and data storage on to the cloud, despite growing concerns around security and risk aggregation. By relying on a small number of providers for cloud services or cyber security, society is creating large concentrations around a few single points of failure. It is a common misconception that the outsourcing or cloud vendor will assume full responsibility in the event of an incident.
- **Third-party liability, including fines and penalties,** is becoming more relevant with advances in technology, organizations collecting more information and enforced data privacy regulation. Almost any cyber incident – including double-extortion ransomware – can lead to litigation and demands for compensation from affected parties**.**
- **A shortage of professionals** is hindering efforts to improve cyber security. While there is growing awareness among boards, the number of unfilled cyber security jobs worldwide has grown 350% over the past eight years to 3.5 million estimates show, meaning many companies struggle to hire, impacting their ability to improve their cyber security posture.
- **Cyber security increasingly seen through the ESG lens.** Today, companies' cyber security resilience is scrutinized by far more stakeholder groups than in the past. Increasingly, cyber security considerations are incorporated into the ESG risk-analysis frameworks of data providers, who look into companies' practices to evaluate their preparedness for cyber crime. Making sure a company's cyber processes and policies are understood at the board level and that risk monitoring processes are in place has never been more important.

In response to a more complex risk environment and increasing cyber claims activity, the insurance industry is more diligently assessing companies' cyber risk profiles in a bid to incentivize companies to improve their security and risk management controls.

"We are gaining much better insights and appreciate clients going the extra mile in order to provide comprehensive data to us. This also helps us to provide more value and offer useful information and advice to customers, such as which controls are most effective or where to further improve risk management and response approaches"

Mr. Sayce concluded.

Source: https://safety4sea.com/allianz-cyber-risks-trends-2022/

Voyager Worldwide hit by cyber attack

Source : Splash247.com

Maritime tech giant Voyager Worldwide has become the latest big name in maritime to be hit by a cyber attack.

Since December 2, all systems have been taken offline at the navigation services and solutions provider, which boasts more than 1,000 shipping companies as customers around the world.

“As this is an ongoing investigation, and our priority is keeping the impact of the incident contained, the time frame for recovery could shift,” Voyager stated on its site, aiming initially to get its systems back online this week.

Mandiant, a cyber security firm, is assisting Voyager’s internal team in responding to the attack.

Among Voyager’s range of services is a cyber security and protection portfolio.

A shipping cyber security survey published earlier this year by maritime cyber security company CyberOwl, maritime innovation agency Thetius and law firm HFW, found that 44% of respondents reported that their organisation has been the subject of a cyber attack in the last three years. Of those, 3% resulted in a ransom being paid by the victim to the attacker, at an average cost of $3.1m.

Source: https://splash247.com/voyager-worldwide-hit-by-cyber-attack/

Comparison between LTE and 5G Network

Editor : YOO Jinho, Korean Register

series news

① What is 5G?

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

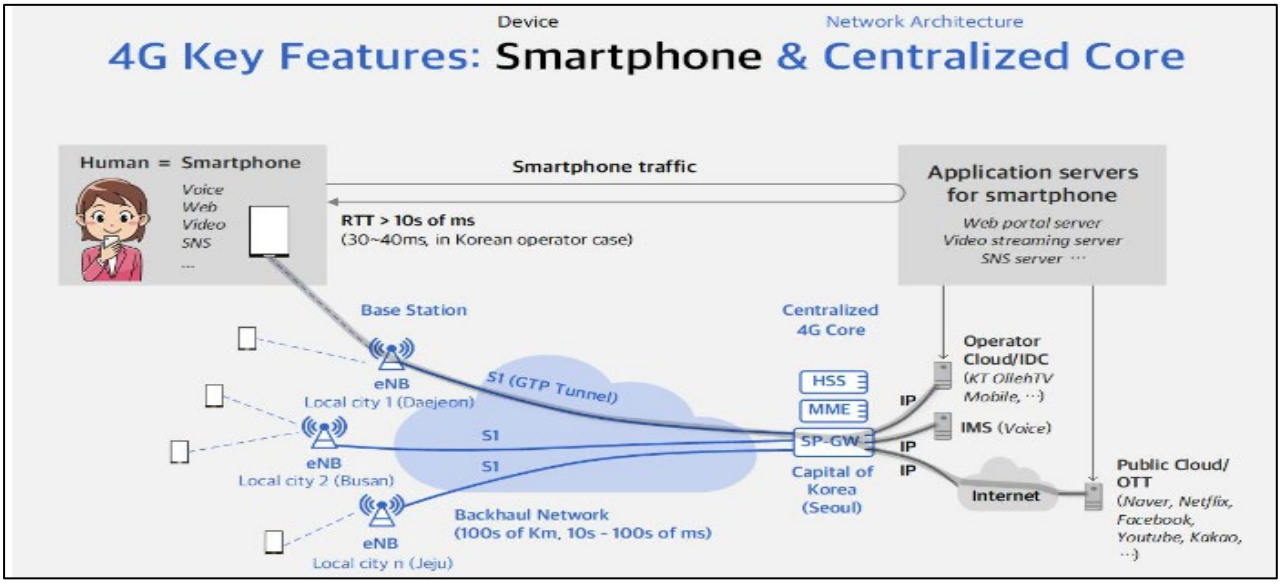
③ **Comparison between LTE centralized network and 5G distributed network**

④ Role of 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

4G LTE Network Architecture

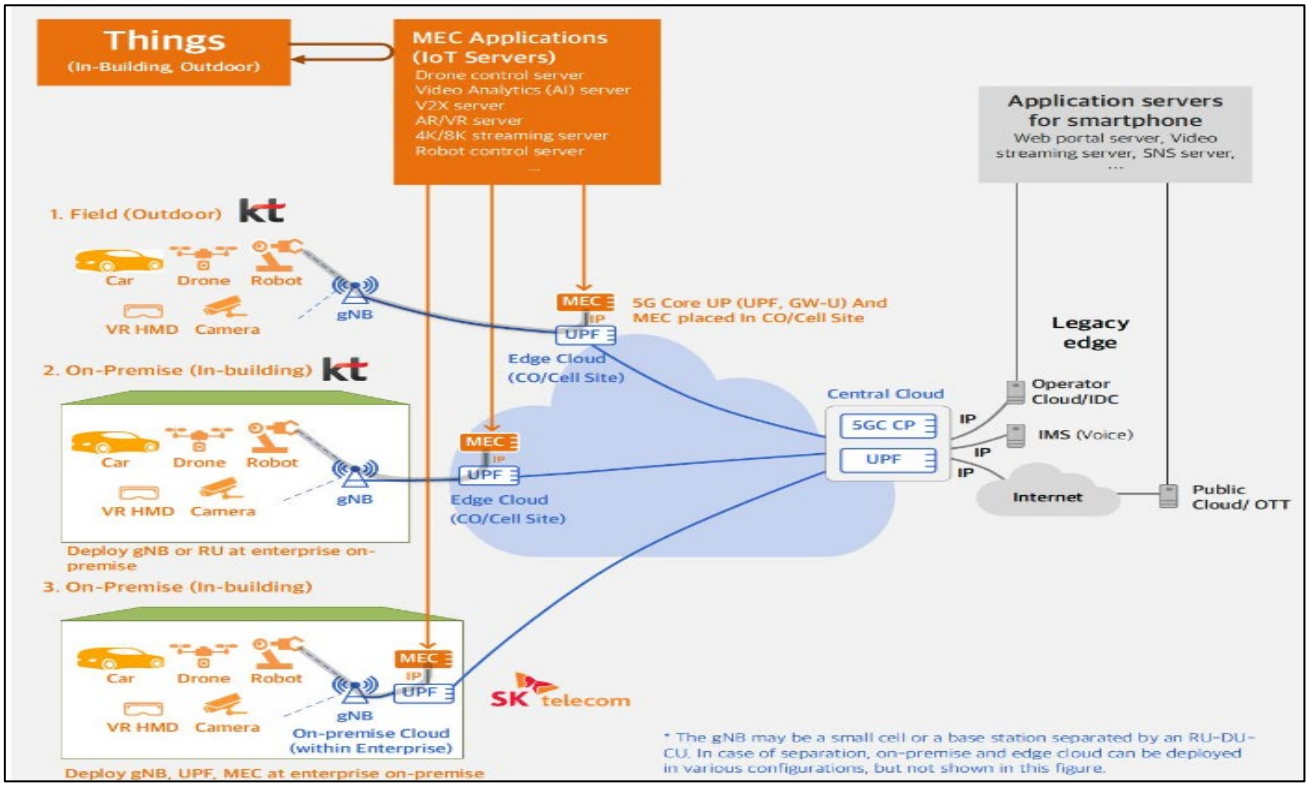
Today's LTE smartphones includes wired networks as well as wireless communication. LTE wired and wireless networks are largely two-step structures with base station equipment (e Node B) and a core network. The core network plays the role of handover, IP allocation, charging, policy, and terminal authentication, while the LTE Core (SP-GW) is a structure based on several sites nationwide. All mobile traffic is delivered to the central LTE Core (SP-GW), and then via IP routing, it can receive IP services (i.e., voice (IMS), the Internet, OTT, etc.). Since smartphone application services are not very sensitive to delays and require dozens of Mbps because of their high capacity, the 4GLTE network structure is mainly specialized on smartphones.



Source : https://www.netmanias.com/ko/post/oneshot/14273/5g-iot-mec/mec-concept-and-deployment-architecture-in-4g-and-5g-network

5G distributed network architecture

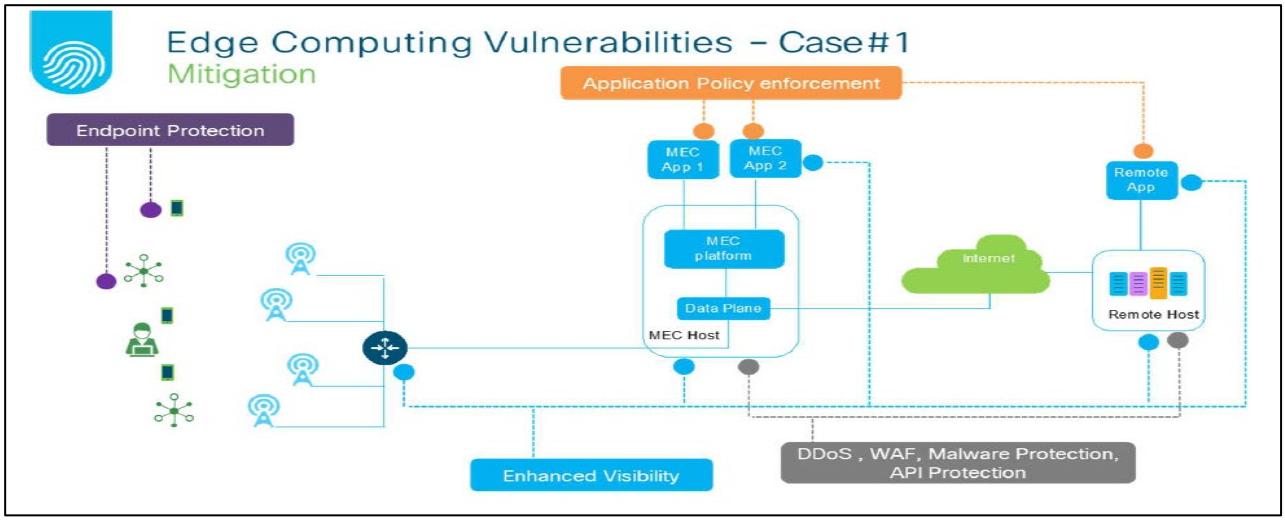
With the emergence of many Internet of Things (IoT) devices, a new era of reliability and integrity of communication between devices is approaching. For example, in order to control autonomous vehicles, drones, and robots, the delay time and traffic distribution between the terminal and the application server must be resolved in order to ensure the reliability and integrity of communication. However, an LTE network is a structure in which all traffic is concentrated on LTE Core (SP-GW) and then IP routing, so there is a long delay time and backhaul traffic load can result. To solve this problem, a 5G distribution network structure is appearing. The present invention provides an ultra-low delay response by forwardly arranging a mobile edge computing (MEC) to be an object near a terminal and reduces the traffic of a backhaul network. If the distributed network structure of 5G is applied to an internal network of a ship, a monitoring service on a ship is effectively implemented through numerous sensors, device control, and on-board CCTV image analysis, and an IoT device can be installed on a cargo (container, etc.) attaching this can significantly enhance the shipping logistics service, offering opportunities for innovation.



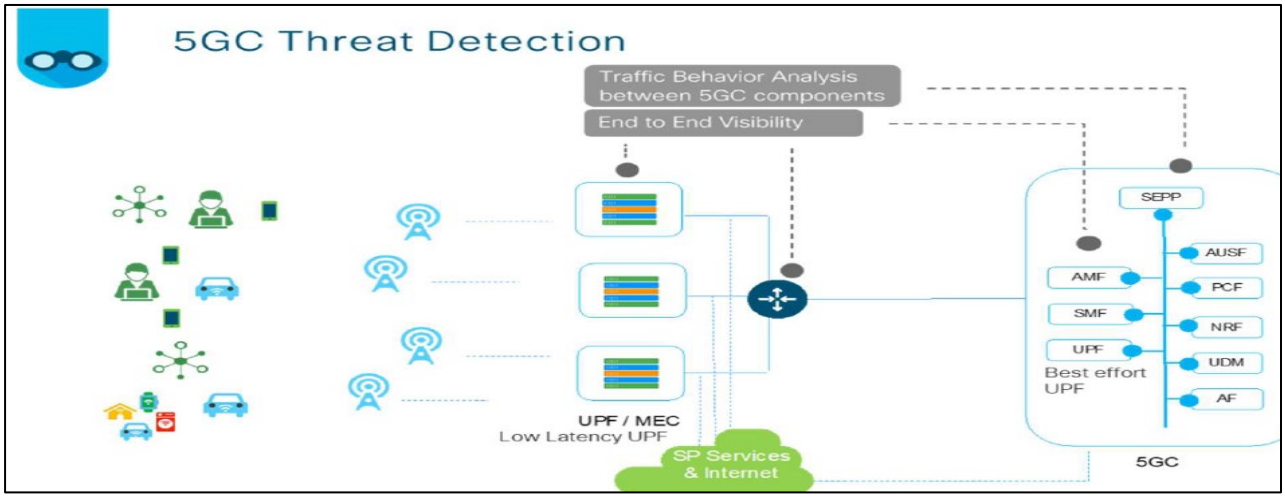
Source : https://www.netmanias.com/ko/post/oneshot/14273/5g-iot-mec/mec-concept-and-deployment-architecture-in-4g-and-5g-network

5G cyber security risk factors - Vulnerabilities of 5G distributed network

Across a 5G distributed network, various network slices may share physical infrastructure such as servers, memory, networks and storage. In such cases, resource reservations and isolation for each slice may be variable, and they may share a common resource pool set. As a result, DoS/DDoS type attacks on one or more slices may indirectly affect other slices. Therefore, physical infrastructures should be designed to provide appropriate resource isolation between slices when sharing common resources.



Proper visibility, segmentation, DNS level security (for example, known bad talkers, bad domains) and detection of abnormal flows is essential. The appropriate visibility and behavior analysis can then detect any malicious operator or actions affecting the 5G network core. proper visibility and behavior analysis allows the operator to detect threats impacting the 5G network core.

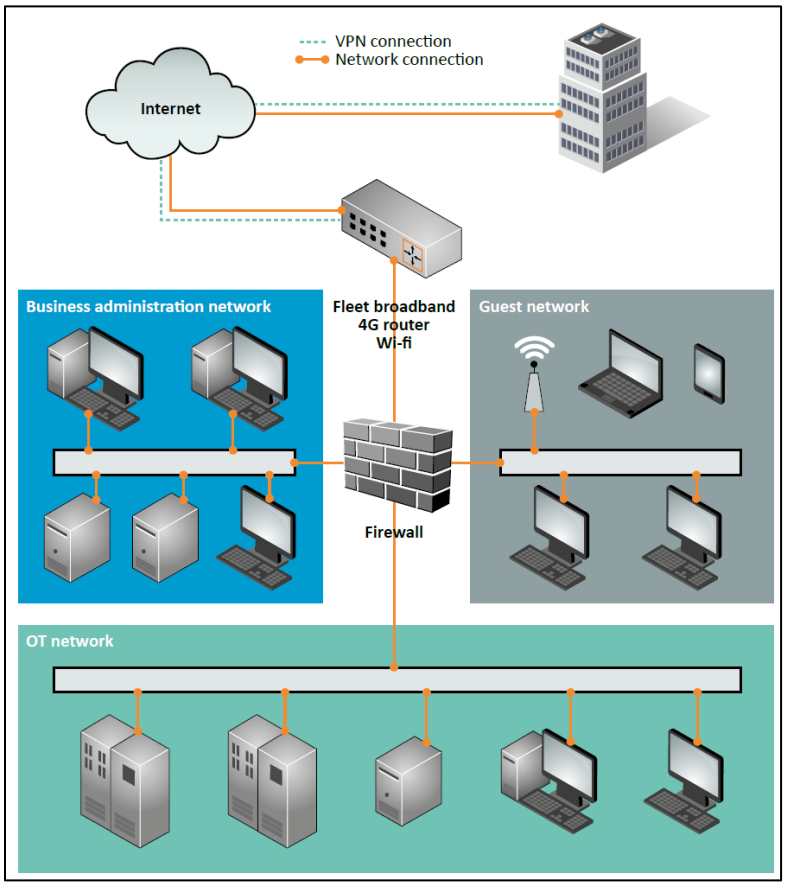


Source : The Evolution of Security in 5G, 5G America white paper, July 2019

Untrusted Network Security

Editor : CHOI Sanghoon, Korean Register

IACS (International Association of Classification Societies) issues UR (Unified Requirements) E27 in April of this year and it includes requirements for cyber resilience of on-board systems and equipment. UR E27 requires additional security capabilities when the system communicating via untrusted network. UR E27 defines untrusted network as any network outside the scope of applicability of the UR. Additional security requirements include Security Level 3 in IEC 624433-3. According to UR E27, the 10 additional security function requirements required by manufacturers supplying onboard systems and equipment connected to untrusted networks are as follows.



< Example of an onboard network (source : BIMCO)>

1. Multifactor authentication for human users

Multifactor authentication is to perform authentication using two or more of the three factors (knowledge / possession / inherence-based factor). For example, when you log-in password (knowledge-based factor) and fingerprint (inherence-based factor) both are required.

2. Software process and device identification and authentication

Prohibit installation of unauthorized software or prevent unauthorized devices from being used on the system.

3. Unsuccessful login attempts

A function to restrict access via an untrusted network when login attempts fail more than a predetermined number of times consecutively for a specified period of time should be provided.

4. System use notification

A function to display a notification message about system use before user authentication should be provided. And notification message setting should be possible by an authorized person.

5. Access via untrusted networks

A function to monitor and control access via an untrusted network should be provided.

6. Explicit access request approval

Access via untrusted networks should only be allowed with the approval of authorized personnel on board.

7. Remote session termination

A function that allows a user who has not been in use for a preset period of time or has started a session to manually terminate a remote session should be provided.

8. Cryptographic integrity protection

When communicating via untrusted network, a cryptographic mechanism should be provided to recognize data change.

9. Session integrity

A function to protect session integrity should be provided and invalid session IDs should be rejected.

10. Invalidation of session IDs after session termination

When a session ends such as user logs, the system should invalidate the session ID.

KR CS++
KR Maritime Cybersecurity Training Tool

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/

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