

KR Maritime Cyber Safety News & Report



Vol. 052
Aug. 2022



CONTENTS

KR Activities

- KR held IACS UR E26 & E27 Seminar
- KR Participated in BLACKHAT USA 2022 conference

Maritime Cyber Safety News

- USCG: Report on Cyber Trends and Insight in the Marine Environment

KR Cyber Security Column

- Chang Choi, Gachon University : AI Security Threats from Adversarial Attack

Advertisement

- KR Cyber Security Training Tool & E-LEARNING

IACS UR E26 & E27 -

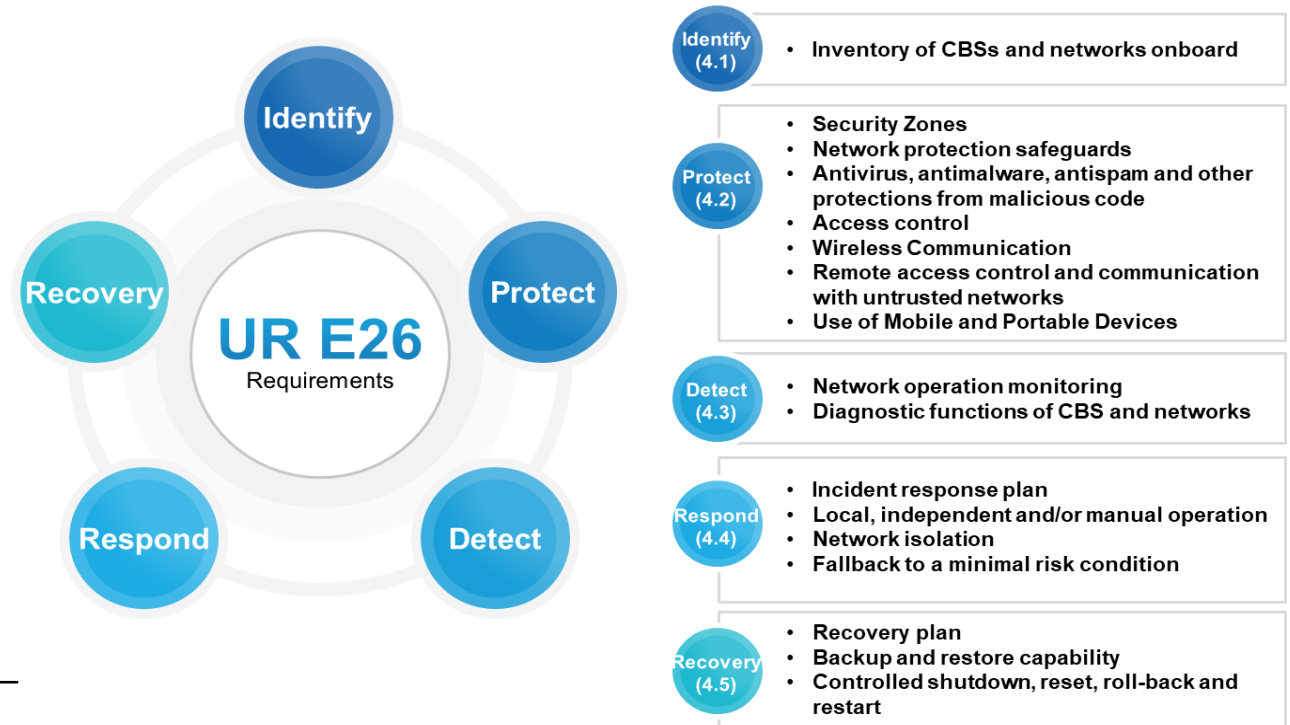
“Cyber Resilience of ships” Technical Seminar

Editor : Kim Juntae, Lim Jeong-gyu, Korean Register

KR visited Shipyard for Daewoo Shipbuilding & Marine Engineering, Hyundai Mipo and Hyundai Samho Heavy Industries at the request of customers from August 23 to 25, 2022, and established the International Association of Classification Societies (IACS) Common Rules for Ship Cybersecurity Resilience (UR, Unified Requirements), a technical seminar related to UR E26 & E27 was held. This seminar was also held at the request of the customer who requested the seminar following last month, and many working-level practitioners and design engineers attended.

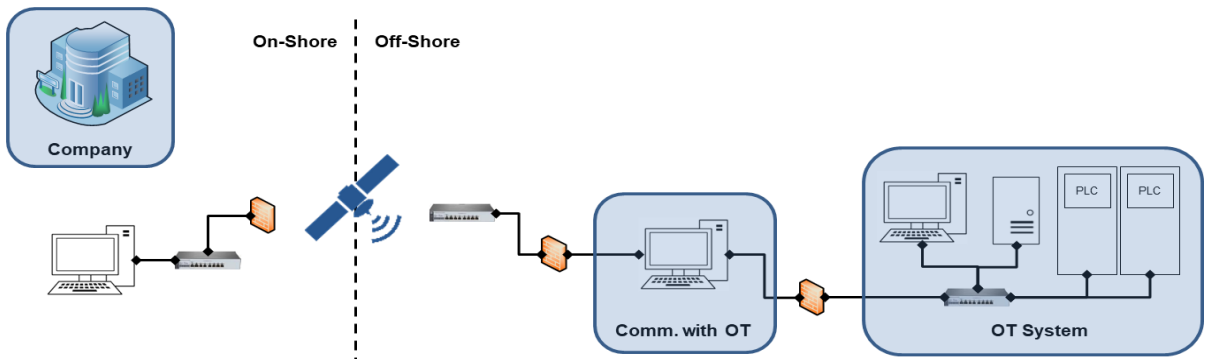
● **UR E26 : Cyber resilience of ships**

UR E26 is a unified requirement for the implementation of cyber resilience in the ship design and construction, and deals with five aspects: Identify, Protect, Detect, Respond, and Recover. This will be applied to ships contracted for construction on or after 1 January 2024.



● *UR E27 : Cyber resilience of on-board systems and equipment*

UR E27 is the cyber resilience of ships' onboard systems and equipment, and applies to category II and category III computer-based systems within the scope of UR E26. This UR consists of requirements for cyber resilience of onboard systems and equipment and requirements for Secure Product development Life Cycle (SDLC) required by manufacturers in product development and manufacturing process.



KR will continue to provide technical seminars upon request from customers in the future, and will also provide customized training services for customers who want more detailed training.




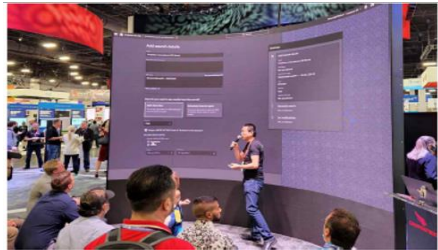
* Customized training Q&A : KR Academy Business Team (academy@krs.co.kr)



BLACKHAT USA 2022 - KR attends global cybersecurity conference

Editor : Lim Jeong-gyu, Choi Sanghoon, Korean Register

KR participated in 'BLACK HAT USA 2022' held in Las Vegas, USA from August 6 to 11, 2022. The BLACK HAT conference is a global cybersecurity conference that celebrated its 25th anniversary this year. It is an event that holds security issue briefings, papers, and exhibitions with the participation of many researchers from cyber security officers and cyber security experts from countries such as the United States and Europe. Korean Register of Shipping participated in this conference to learn about the latest cyber threat trends and defense technologies in cyber security in the OT field. Keynote speaker Kim Zetter said that cyber threats to OT systems have increased since Stuxnet, a malicious code designed to target SCADA, was first discovered in 2010. Korean Register of Shipping plans to continuously acquire the latest cybersecurity threat trends and defense technologies and disseminate them to related industries.

Conference Picture	
	
Entrance of Conference	Presentation Session
	
Booth	Technical Seminar

USCG Report

Cyber Trends and Insight in Marine Environment

Editor : Yoo Jinho, Korean Register

Source : Safety4Sea.com

The USCG released the August 2022 Cyber Trends and Insight in Marine Environment report. This report aims to provide relevant information about best practices to secure their critical systems based on USCG findings. The report intends to aid Sector Commanders, their staffs, and maritime facility leadership teams, including Facility Security Officers (FSOs), IT Directors, Chief Information Officers (CIOs), Chief Information Security Officers (CISOs) and other executives. In this report, we would like to extract and introduce the main contents that should be remembered in the ship and marine environment.

● *Cyber threats in ships and marine environments*

① Easily Guessable Credentials

One or more services are accessible using an easily guessed username and password. An attacker with minimal technical knowledge can use these credentials to access the related services.

The below tables show some of the most common default usernames and passwords, along with the number of unique technology vendors that utilize them. The information comes from a public analysis of 2,866 vendor products.

Top 10 Default Usernames	
Admin	553
<BLANK>	372
<N/A>	261
root	145
Administrator	73
User	37
guest	33
MGR	23
operator	23
system	21

Top 10 Default Passwords	
<BLANK>	418
admin	275
PASSWORD	133
1234	46
epicrouter	18
0	34
root	19
system	23
user	19
DEMO	21

<Fig 1. Easily Guessable Credentials Top 10>

<Source: USCG, 2021 Cyber Trends and Insights in the Marine Environment>

Cyber threats in ships and marine environments (Cont.)

② Easily Crackable Passwords

User account passwords on the system are common and widely used. An attacker can successfully predict the victim’s password, using a wordlist to gain access to the account.

The below table shows the twenty most common passwords used according to several data breach repositories from NordPass. Using a common password can greatly increase the probability of an attacker accessing an account without authorization.

Top 20 Most Common Passwords		
Rank	Password	Time to Crack
1	123456	<1 Second
2	password	<1 Second
3	12345	<1 Second
4	123456789	<1 Second
5	password1	<1 Second
6	abc123	<1 Second
7	12345678	<1 Second
8	qwerty	<1 Second
9	111111	<1 Second
10	1234567	<1 Second
11	1234	<1 Second
12	iloveyou	<1 Second
13	sunshine	<1 Second
14	monkey	<1 Second
15	1234567890	<1 Second
16	123123	<1 Second
17	princess	<1 Second
18	baseball	<1 Second
19	dragon	<1 Second
20	football	<1 Second

<Fig 2. Easily Crackable Passwords Top 20>

③ Open Mail Relay

An open mail relay is an email server that allows anonymous users to send emails. There is no authentication when using an open mail relay. Open mail relays will send emails with spoofed source addresses that appear to be coming from legitimate addresses within your organization. MCAs often use open mail relays to send phishing emails and spam.

④ Patch Management

Vendors release patches and updates to address existing and emerging security threats and address multiple levels of criticality. Failure to apply the latest patches can leave the system open to attack with publicly available exploits. The risk presented by missing patches and updates can vary.

● *Mitigation Recommendations*

① **Disable or Remove Feature or Program**

Remove or deny access to unnecessary and potentially vulnerable software to prevent abuse by adversaries.

② **Password Policies**

Set and enforce secure password policies for accounts. Despite widespread frustration with the use of passwords from both a usability and security standpoint, they remain a very widely used form of authentication.

③ **Multi-Factor Authentication**

Use two or more means to authenticate to a system, such as a username and a password in addition to a token from a physical smart card or token generator.

④ **Network Intrusion Prevention**

Use signatures and anomaly detection to block malicious traffic.

⑤ **Network Segmentation**

Design sections of the network to isolate critical systems, functions, or resources; Use physical and logical segmentation to prevent access to potentially sensitive systems and information; A Demilitarized Zone (DMZ) contains Internet-facing services preventing exposure of the internal network to the Internet; Configure separate virtual private cloud (VPC) instances to isolate critical cloud systems.

⑥ **Vulnerability Scanning**

Regularly scan externally facing systems and internal networks for vulnerabilities and establish procedures to rapidly patch systems when critical vulnerabilities are discovered through scanning and through public disclosure; Implement continuous monitoring of vulnerability sources and the use of automatic and manual code review tools.

⑦ **Update Software**

Perform regular software updates to mitigate exploitation risk.



Introduction to Adversarial Attack Threats and Mitigation of Artificial Intelligence (AI)

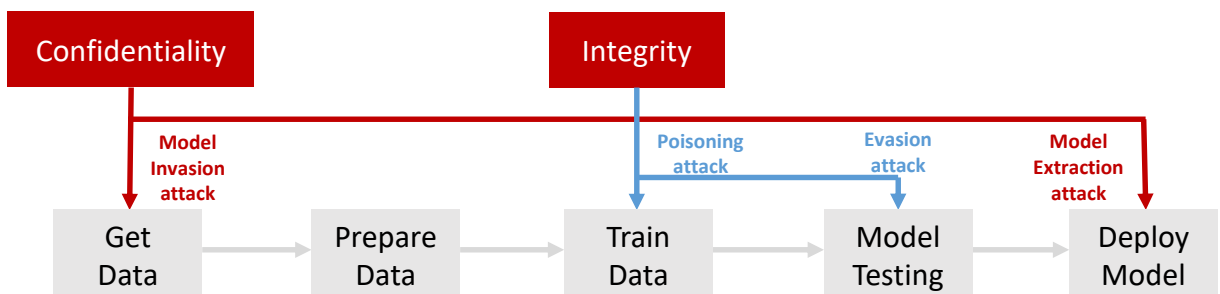
Editor : Prof. Chang Choi, Gachon University

● Security threats from AI(Artificial Intelligence) commercialization

Recently, with the advent of the ICT era, the commercialization of AI technology is in full swing, and the artificial intelligence market is also showing great growth. In particular, various technologies applying artificial intelligence, such as intelligence of objects and autonomous driving, have already been applied and are in use in real life. However, in the event of malicious attack such as malfunction of autonomous vehicles and leakage of personal information used for artificial intelligence learning, the damage will be significant. Accordingly, the importance of detailed security review of artificial intelligence models is emerging. Therefore, we introduce the most important concept in current artificial intelligence security, Adversarial Attack..

● The concept of Adversarial Attack

The Adversarial Attack is one of the most talked-about areas of AI security research. Adversarial attacks are security risks that lead models to make bad judgments through vulnerabilities in artificial intelligence algorithms. As shown in <Fig 3>, Adversarial attacks are attacks that can infringe the confidentiality and integrity of the AI model, and it is a fatal attack that infringes the three security elements.



<Fig 3. Adversarial Attack overview>

<Source: Sandip Kundu, security and Privacy of Machine Learning Algorithms, ISQD 2019>

● *The concept of Adversarial Attack (Cont.)*

Integrity attacks of artificial intelligence include Poisoning Attack that interferes with artificial intelligence learning by inserting malicious data during the learning process and Evasion Attack that modulates data by inserting noise into normal data, and confidentiality attacks can be classified as Inversion Attack that extracts learning data directly from the model.

● *The purpose of a Adversarial Attack*

The ultimate goal of adversarial attacks is to make artificial intelligence make bad decisions. Detailed purposes include reduced reliability, misclassification, target misclassification, and input/target misclassification, which destroy the model or prevent normal operation. Attackers should be careful because they can attempt attacks for different purposes depending on the nature of the victim model.



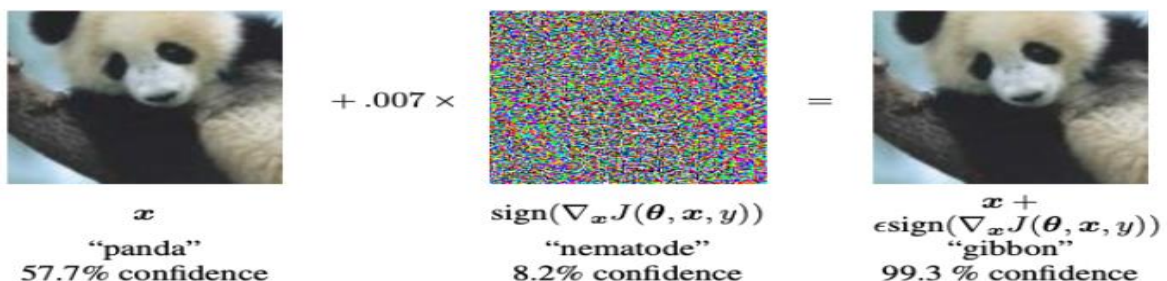
<Fig 4. Example of Adversarial attacks>

<Source: University of Washington, 2017>

● *Representative offensive techniques of adversarial attack*

① FGSM(Fast Gradient Signed Method)

Fast Gradient Signed Method (FGSM) is a technique that uses gradient in neural networks to generate adversarial samples. Adversarial samples are specialized inputs designed to confuse neural networks, which make it difficult for neural networks to classify samples.



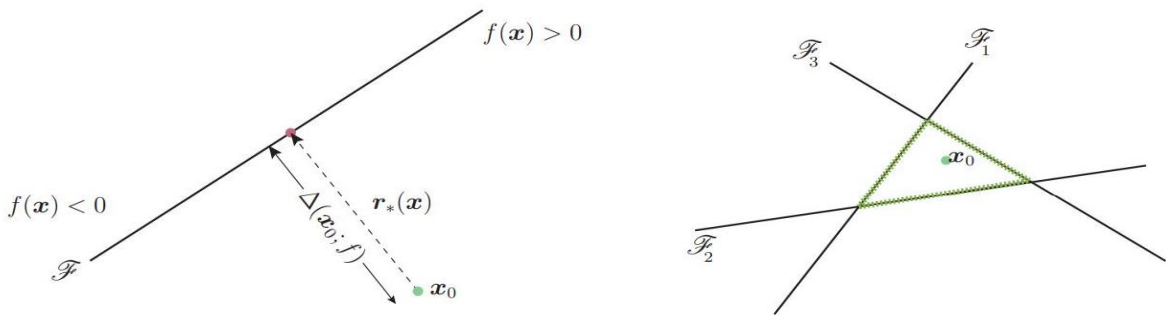
<Fig 5. Example of generating adversarial samples on the FGSM>

<Source: Explaining and Harnessing Adversarial Examples>

● *Representative offensive techniques of adversarial attack (Cont.)*

② Deepfool

An algorithm called deepfool can obtain an optimal solution by projecting perpendicular to a decision boundary at a given point using two dimensions and adding appropriate constants to create adversarial samples. Many deep learning models are misclassified by very small perturbation, and the DeepFool method has the advantage of having smaller perturbation compared to the FGSM.



<Fig 6. Deepfool's method of generating adversarial samples>

<Source: DeepFool: a simple and accurate method to fool deep neural networks>

③ JSMA(Jacobian-based Saliency Map Attack)

Jacobian-based saliency map attack (JSMA) techniques are derived from FGSM methods using gradients, which generate adversarial samples through mapping of inputs and outcomes in neural networks by changing them to 1 pixel unit at a time to increase misclassification. After mapping the input data to the saliency map, we add Perturbation in the most misrecognized direction to generate adversarial samples.

④ C&W(Carlini & Wagner) Attack

It is an attack technique available in all dimensions and is a technique related to optimization problems using adam optimizer. Since C&W attacks do not specify Thresholds that limit maximum distortion, attacks using C&W always succeed. Adversarial samples are classified with higher reliability than real samples, and are evaluated as the strongest attack techniques that complement the FGSM attack techniques.

● Representative defense techniques of adversarial attack

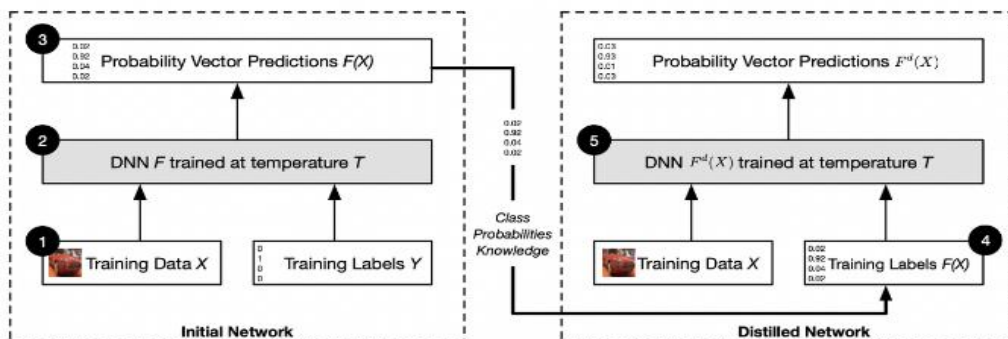
① Adversarial Training

Adversarial training is a defense technique that adds adversarial samples of a particular attack in the case of model learning in preparation for a particular attack to develop resistance to the attack. This is a defense technique to prepare for the poisoning attack, and has the advantage of being able to defend a specific attack very effectively. However, there is a limitation that it is necessary to learn attack data one by one to defend against certain attacks, and that it is not possible to prepare perfectly for unspecified attacks.

② Defensive Distillation

Defensive distillation aims to hide the gradient of artificial intelligence models utilized for adversarial attacks. Based on the structure of <Fig 7>, using the distillation concept, the gradient size of the training and validation steps is contracted or expanded, confounding the attacker, making it impossible to access the gradient.

In the initial network (learning stage), the probability distribution is unformed by specifying a large value of temperature T , which is called a distillation process. After that, probability distribution has the advantage of being able to produce discretized results without causing model performance degradation by designating temperature T as 1 again in the Distilled Network. In the case of the defense technique, a new paradigm of AI defense was presented, but further research is needed to supplement robustness in the future as vulnerabilities are revealed in C&W Attack.



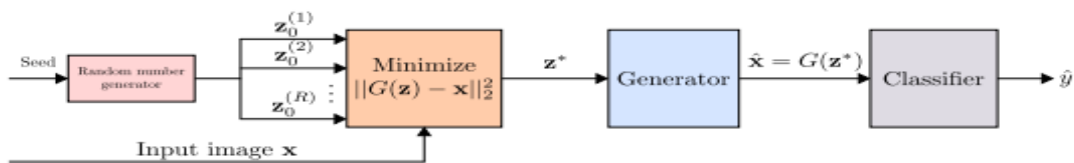
<Fig 7. Defensive distillation structure>

<Source: Distillation as a Defense to Adversarial Perturbations against Deep Neural Networks>

● *Representative defense techniques of adversarial attack (Cont.)*

③ Defense GAN(Generative Adversarial Network)

Defense Generative Adversarial Network (GAN) minimizes the difference between adversarial samples and virtual images generated by artificial intelligence. As shown in <Equation 1>, the random sample derived through the corresponding model minimizes the difference between adversarial examples and normal images, and extracts features as similar as possible to normal images. This allows us to eliminate the Perturbation of adversarial samples and effectively defend against adversarial attacks.



<Fig 8. Defense GAN structure>

<Source: Defense-GAN: Protecting Classifiers Against Adversarial Attacks Using Generative Models>

The advantage of Defense GAN is that it can defend against attacks without modification of existing artificial intelligence models, and it can defend against overall attacks without distinction between Black-box and White-box. However, due to the instability of GAN training, perfect defense is difficult, and there is a limitation that user-specified learning conditions absolutely affect performance.

$$z_{j-1}^i + \eta_j * \nabla_z ||G(z_j^i) - x||_2^2, \text{ iterate } L \text{ times}$$

< Equation1. Defense GAN latent vector minimization method >

<Source: Defense-GAN: Protecting Classifiers Against Adversarial Attacks Using Generative Models>

● *The trend of adversarial attacks*

The field of adversarial attack has been studied in the white-box environment, assuming that all information about the target is known, and to date various attack and defense techniques have been published. Furthermore, in recent years, previously announced attack techniques are being studied so that they can be applied to black-box rather than white-box, and defense techniques are also being studied for defense against unspecified attacks on black-box. This is considered a very important research area for the practical defense of AI technology used in practice, and suggests that it should be supported by technologies in the security aspect in line with the development of artificial intelligence.

KR CS++

KR 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 부산광역시 강서구 명지오션시티 9로 36 (명지동)

(46762) 36, Myeongji ocean city 9-ro, Gangseo-gu, Busan Republic of Korea

Tel +82 70 8799 8595

Fax +82 70 8799 8594

www.krs.co.kr

Copyright © 2022 ALL RIGHTS RESERVED BY KOREAN REGISTER