KR Maritime Cyber Security

News from KOREAN REGISTER

Oct 2018

Vol. 006

KR Maritime Cyber Security Activities

● Cyber Security MOU Signing with NSHC SECURITY & SHIELD CONSULTING

Last September, KR and NSHC SECURITY & SHIELD CONSULTING signed MOU to strengthen mutual technology exchanges and cooperation for joint research and development in the field of ship cybersecurity. Major contents of MOU are as follows:

- Achievement of Company Cyber Security Management System Certification
- Application of Maritime Cyber Security Guidance to OT System on board ship and technical cooperation for penetration testing
- Joint development of maritime cyber security training contents

NSHC SECURITY, the only cyber security company in Domestic and Asian that can carry out penetration testing of ICS/SCADA(OT), is conducting malicious code analysis such as ransomware and APT attacks, penetration testing of industrial devices and source code diagnosis. SHIELD CONSULTING is providing consulting on physical security(CCTV, control of outsider's access, control of electronic devices and locks) required in cyber security.

By signing MOU this time, it is expected that KR will expand their skills in penetration testing of OT system on board ships and enhance rules, and establish bases for cyber safety technologies for future ships such as autonomous ship and unmanned ship.

● IACS, Ship Cyber system Recommendations Deployment

IACS releases 9 out of 12 key recommendations on Sept. 27 to ensure safety of ship cyber system. 12 recommendations consists of Software Maintenance, Manual Backup Devices, Contingency Plans in case of Incident, Network Structure, Data Security, Network Security, Ship System Design, Computer System Inventory, System Integration, Remote Update and Access, and Interface, etc. KR led the development of **'Contingency Plans in case of Incident'.**

Cyber system panel newly established in July 2016 and its main topic is cyber safety of ship cyber system (Software, hardware, network, data, etc.). 3 recommendations will be released by the end of this year. Cyber system panel aims the development of integrated guidelines for ship cyber system through integrating 12 recommendations into single document. recommendations can be found on the following IACS homepage.

※ http://www.iacs.org.uk/publications/recommendations/141-160/

Rec No	Title	Status
Rec 153	Recommended procedures for software maintenance of shipboard equipment and systems	Published
Rec 154	Recommendation concerning manual / local control capabilities for software dependent machinery systems	Published
Rec 155	Contingency plan for onboard computer based systems	Published
Rec 156	Network Architecture	Published
Rec 157	Data Assurance	Published
Rec 158	Physical Security of onboard computer based systems	Q4 2018
Rec 159	Network Security of onboard computer based systems	Published
Rec 160	Vessel System Design	Q4 2018
Rec 161	Inventory List of computer based systems	Published
Rec 162	Integration	Published
Rec 163	Remote Update / Access	Published
Rec 164	Communication and Interfaces	Q4 2018

Ref. International Association of Classification Societies

Port of San Diego Hit by Cyber Attack

It is confirmed that IT system in the Port of San Diego has been attacked by Ransomware. The Port of San Diego said that system crash was first reported on Sept. 25, and the port mobilized a team of industry experts, regions, state, federal agents and partners to minimize the effect and recover the system taking into account of public safety systems

Some of the Port's IT systems were damaged by attacks, but others were also closed as a precaution. The Port said they are finding out the extent and timing of the incident, the scale of damage and are developing a recovery plan.

- **Parts have become targets of cyber attack.**

Only a week ago, the Port of Barcelona was also found to have been attacked by a cyber attack. Until now, technical details of cyber attack have not been made public, but they have reportedly attacked multiple servers in the port security infrastructure. Last July, a port terminal of a COSCO shipping company in Long Beach, California, was attacked by Ransomware. With three reports reporting cyber attacks in two months, some doubt that the threat group intentionally targeted them. Any confusion in the port could lead to serious financial and social losses, and proper countermeasures are needed.

Response and Suggestion

Responding to cyber threats requires operation and management of systematic security system, and regular training to improve the ability of security personnel in order to respond to crisis management and take quick initial actions. In addition, awareness and professional education of executives and employees is required, and responding of cyber threats are required through analysis of breaches and quarterly hacking defense drills.

Ref. www.zdnet.com

Understanding Cyber Threat

● Understanding cyber threat

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

● KR Guidance for Maritime Cybersecurity Management System requirement (CSMS1)

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

● BSI top 10 cyber threat

Threats to ICS are due to attacks or events that could potentially damage ICS and its related businesses due to existing vulnerabilities. The following table lists the most serious threats to ICS published by the German Federal Information Security Agency. Following the newsletter in July, we will analyze the **"Human Error and Sabotage"** of the BSI 10 cyber threats.

No. (old No.)	Top 10 2016	Top 10 2014
1 (3)	Social Engineering and Phishing†	Malware Infection via Internet and Intranet
2 (2)	Infiltration of Malware via Removable Media and External Hardware	Infiltration of Malware via Removable Media and External Hardware
3 (1)	Malware Infection via Internet and Intranet	Social Engineering
4 (5)	Intrusion via Remote Access	Human Error and Sabotage
5 (4)	Human Error and Sabotage	Intrusion via Remote Access
6 (6)	Control Components Connected to the Internet	Control Components Connected to the Internet
7 (7)	Technical Malfunctions and Force Majeure	Technical Malfunctions and Force Majeure
8 (9)	Compromising of Extranet and Cloud Components	Compromising of Smartphones in the Production Environment
9 (10)	(D)DoS Attacks	Compromising of Extranet and Cloud Components
10 (8)	Compromising of Smartphones in the Production Environment	(D)DoS Attacks

Ref. : Industrial Control System Security – Top 10 Threats and Countermeasures 2016

● BSI top 10 cyber threat : Human Error and Sabotage

Staff working in an ICS environment are in a special position with regard to security. This ap- plies to in-house staff as well as to all external personnel, e. g. for maintenance or construction, no matter if they have access to facilities or work from a remote location. Security can never be guaranteed by technical controls only, but always requires organizational regulations.

<Potential threat scenarios>

▣ Incorrect configuration of components relevant to security (e.g. firewall) or network components, but also ICS components.

▣ In particular, the uncoordinated installation of updates or patches can lead to problems with the functionality of individual components and their interaction.

▣ Side-effects of intentional actions need to be considered (damage to devices and installations, placing of covert listening devices and taps etc.).

▣ Compromise of systems by unauthorized software or hardware. This includes e. g. games, digital cameras, smartphones or other USB devices owned by operators.

▣ Creation of unreleased configurations for infrastructure and security components (e. g. adding a firewall rule to allow unauthorized access from outside via mobile endpoints).

<Countermeasures>

- Introduction of the “need to know“ principle: Knowledge of system details, passwords etc. as well as access to sensitive data only if necessary.
- Creation of a general framework for motivated, qualified and connected staff to ensure operator and administrator competence for functional as well as security-specific components. Qualification and training programmes, as well as awareness-raising measures, are to be designed sustainably and should be compulsory.
- Disabling of internet access for control systems and systems in close proximity to the production environment as well as provision of components for tasks separate from the ICS, available for operators e. g for office, e-mail, ERP etc., sufficiently secured and integrated into a different network.
- Introduction of standardized processes for recruitment and staff leaving the enterprise as well as external contractors (product suppliers, vendors, service providers).
- Suitable standards (policies & procedures) for the handling of technical systems by staff (e. g. handling of removable media, communication behavior in e-mail and social networks, password policies, installation of individual software etc.).
- Automatic monitoring of system health and configurations.

Ref. : Industrial Control System Security – Top 10 Threats and Countermeasures 2016

Guidelines of Establishing Physical Security System

● The need for establishing physical security system

The Purpose is to protect the company and the ship major cyber assets from various type of threats by establishing procedures and criteria for access control and facility security. The company and the ship should apply physical sand environmental security standard to establish integrated protective measures for physical access control.

● KR Guidance for Maritime Cybersecurity Management System requirement (CSMS1)

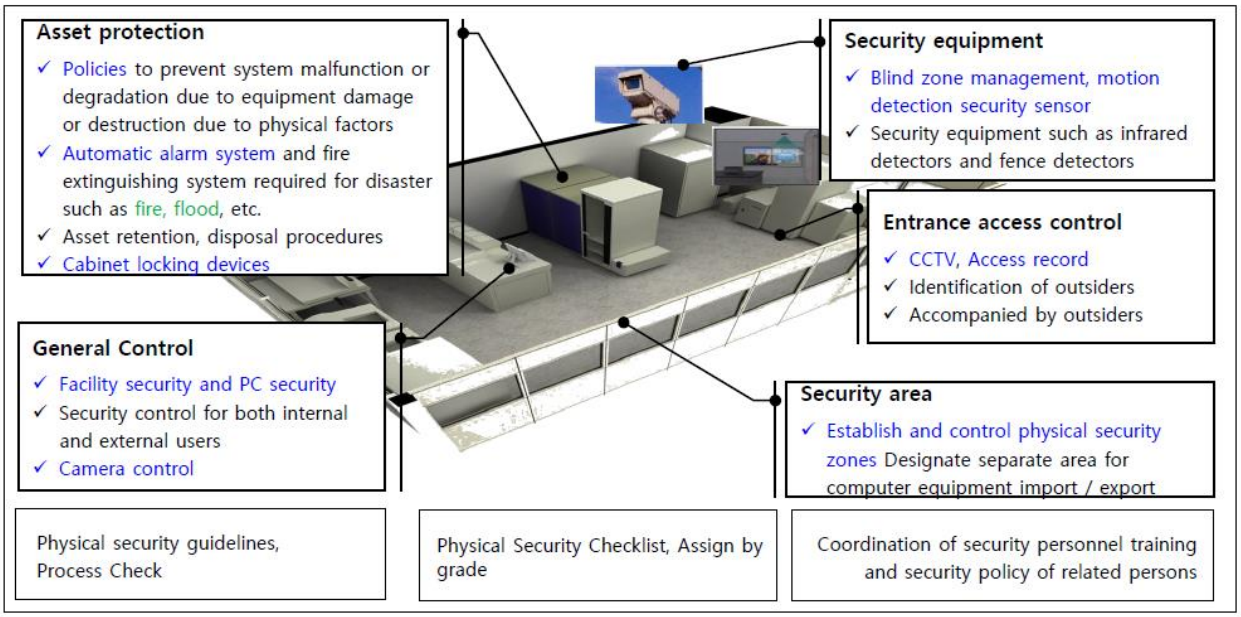
Establish physical security policy (207.1) : The company shall establish policies that define the physical security standards for system equipment, facilities, etc.

Protected area controls (207.2) : The company shall provide physical controls to access protected areas containing assets only to authorized persons.

Portable storage media controls(207.8) : The company should control its internal assets and network connections through portable storage media such as USB.

Environmental security (207.11) : Clean desk operation and terminal screen protection policy of space where documents and portable storage media are stored should be prepared and applied.

● Physical security terminology



- **Access control in Restricted Area (Example)**

- **Mobile Device Control (Example)**

Explanation of Term

- **Cyber System :** Hardware or software system or subsystem for acquiring, processing, storing or exchanging information or data.(IMO MSC 94)
- **Cyber Security** : Protection of computer networks and control systems from intentional failure, damage or malicious use by unauthorized users. Physical, administrative and technical security activities are need to protect systems, networks, applications, and data that make up cyberspace.
- **Cyber Safety** : Protection of computer networks and control systems from unintentional consequences due to accidental incident or cyber-system failure by an authorized user including owner, operator. Cyber safety is a broad concept that includes cyber security and means a state in which no cyber incidents occurs.
- **Penetration Test** : A pre-determined simulated attack to gauge the level of cybersecurity for systems and a company. In some cases, the system is divided into white boxes that provide information for the system under test and black boxes that do not provide any information in advance.