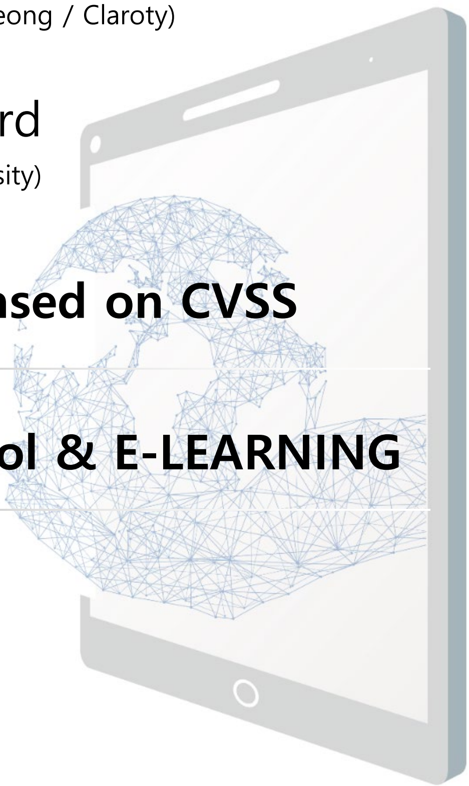
KR Maritime Cyber Safety Newsletter

Vol. 048

April. 2022

Korean Register
www.krs.co.kr

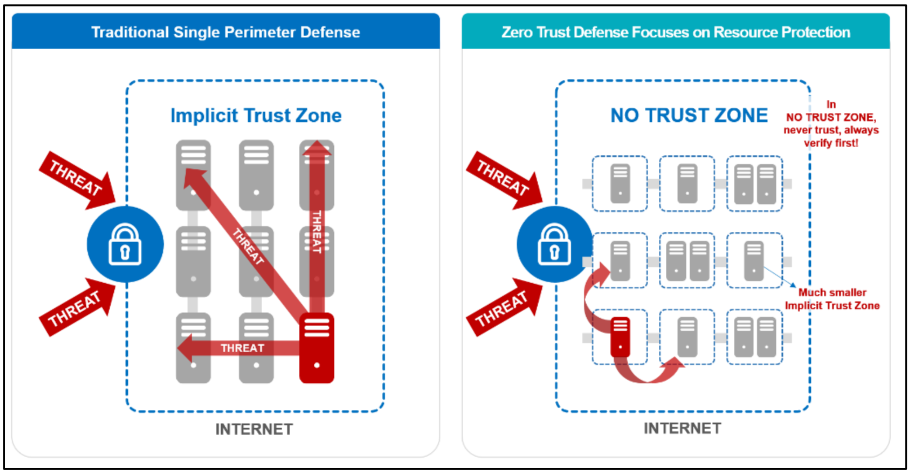
Index



Design of Safe RCS based on Zero Trust for Autonomous Ship

Cyber Threats to Smart Ship and Autonomous Ship

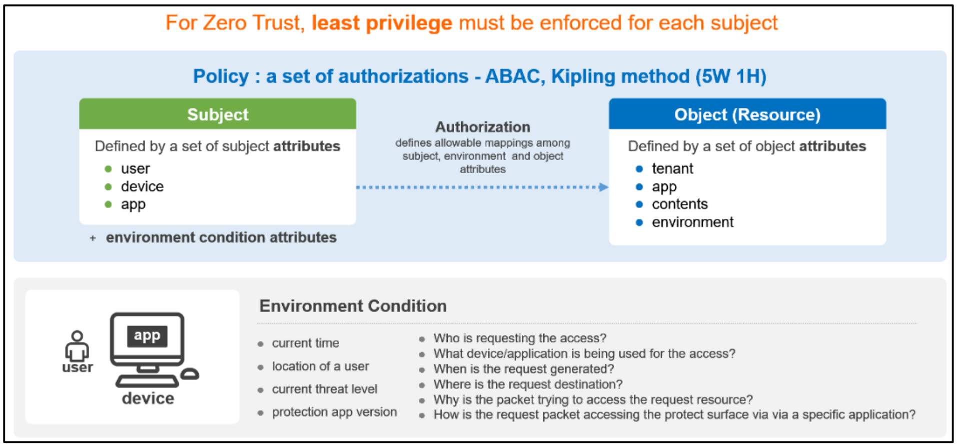
Recently, it is expected that autonomous ship technology which operates on its own without human decision by converging artificial intelligence (AI), the Internet of Things (IoT), big data and advanced sensors beyond smart ships with a high proportion of ICT technology, will rapidly emerge and reach the market size of about 11 billion dollars by 2030. Here, the ship control system, which is the core technology of autonomous ships, consists of information management system, ballast water management system, propulsion control system, engine control management system, power management system, etc., and is expected to account for 81% of the total market for autonomous ships. The development of smart ship and autonomous ship technology is creating new opportunities for the shipping industry, but with the increase of external connectivity to many IoT devices and ship control systems, the vulnerability to cyber attacks is also increasing. In particular, the rise of hacking economy due to the spread of dark web and virtual currency is increasing these threats more rapidly, and Maersk Incident in 2017 is a major example of cyber attacks in the shipping sector. The malware attack on Maersk which was responsible for one-fifth of the world's transportation, infected 45,000 PCs and 4,000 servers, costing $300 million and took about a month to complete system restoration. In response to this growing new security threat in each industry, the Biden administration is calling for the full application of the zero-trust-based security concept recommended in the NIST report in an executive order issued to improve U.S. cyber security in 2021.


Traditional Single Perimeter Defense
Implicit Trust Zone
THREAT
THREAT
THREAT
THREAT
THREAT
INTERNET
Zero Trust Defense Focuses on Resource Protection
NO TRUST ZONE
In NO TRUST ZONE, never trust, always verify first!
THREAT
THREAT
Much smaller Implicit Trust Zone
INTERNET

<Figure1 Difference between security based on perimeter and zero trust>

Concept of Zero Trust

As shown in Figure 1, zero trust can be seen as a concept that contrasts with existing perimeter-based security. Existing boundary network-based security uses barrier technologies such as firewalls to control access to the trust zone. In that security, once connected to the trust zone, users can perform relatively free actions and the means to control these actions are limited. In a typical hacking scenario, often referred to as “Lateral movement” or “East-west traffic” hackers access the internet network through stolen personal information or login information and install a backdoor program. Then they gradually acquire confidential information or access privilege to the internal control system such as administrative privilege or internal usage passwords and finally take control of privilege escalation system. In autonomous ships, remote access control systems (RCS) or crew networks create external entry points, and when the login information of the access authority owner is stolen, vulnerable points that may be the target of hacking methods such as Lateral Movement described above are created. On the other hand, zero-trust-based security does not establish trust zone and details authentication policies related to access requests for each resource, assuming that all boundary networks can be breached someday and remote access terminals or login information can be stolen. Through this, zero-trust-based security controls access authorization in real time and monitors access records and the performance of user’s internal operation, taking into account various variables such as device, access frequency, access application, access location and time.


For Zero Trust, **least privilege** must be enforced for each subject

Policy : a set of authorizations - ABAC, Kipling method (5W 1H)

Subject

Defined by a set of subject **attributes**

- user
- device
- app

+ environment condition attributes

Authorization

defines allowable mappings among subject, environment and object attributes

Object (Resource)

Defined by a set of object **attributes**

- tenant
- app
- contents
- environment

Environment Condition

- current time
- location of a user
- current threat level
- protection app version

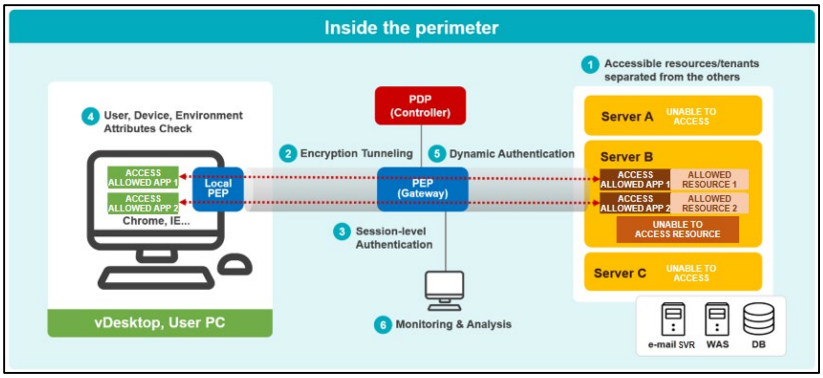
- Who is requesting the access?
- What device/application is being used for the access?
- When is the request generated?
- Where is the request destination?
- Why is the packet trying to access the request resource?
- How is the request packet accessing the protect surface via via a specific application?

<Figure 2 Concept of attributes based access control (ABAC)> <Source : Forwiz System>

In addition, as shown in Figure 2, zero-trust-based security reflects multiple users and complex environmental attributes, giving users only the least privileges essential for performing tasks, requiring additional authentication for additional non-authorization tasks, and minimizing the extent of impact (Blastradius) even if user’s terminal is hacked. To this end, thorough user authentication (Identity) and microsegmentation of operation privilege are essential components of zero-trust-based security.

Basic Zero Trust Architecture

NIST presents a standard ZTA (zero trust Architecture) for implementing zero trust. The main components of the ZTA are Policy Enforcement Point (PEP) and Policy Decision Point (PDP). PDP consists of a Policy Administrator (PA) and a Policy Engine (PE) to determine whether to allow connections between remote users and PEPs. PEP acts as a gateway that mediates only the allowed connections between remote accessors and protection resources. In addition, an Agent may be installed in the connection terminal, and detailed environmental monitoring and connection control of the connection terminal may be performed using the Local PEP. Figure 3 is an example of ZTA implementation in a virtual desktop infrastructure (VDI) based remote access environment, where Local PEP is installed on remote access Desktop, gateway PEP is installed on the front of the protected resource, and whether to allow access is determined by the controller. At the time of access, whether or not to allow access is determined by comprehensively considering various attributes such as the application used and the workable time, and an encrypted tunnel session is formed.



<Figure 3 Example of ZTA in VDI environment> <Source : Forwiz System>

Methodology for Zero Trust Construction

Methodology for Zero Trust Construction

① Definition of protection surface

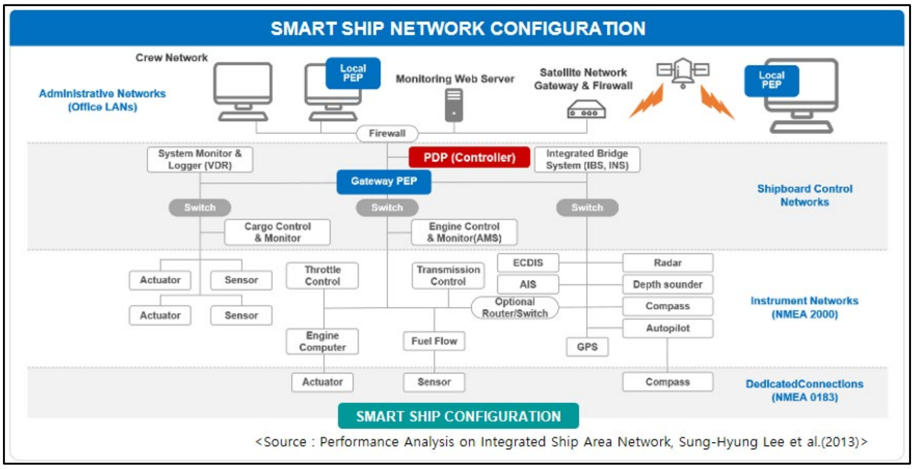
② Identification of transaction flow

③ Design of zero-trust architecture

④ Creation of zero trust policies

⑤ Monitoring and management

Paloalto Networks, which leads the zero-trust-based cybersecurity technology, presents a methodology for building zero trust in five phases: 1) definition of protection surface 2) identification of transaction flow 3) design of zero-trust architecture 4) creation of zero trust policies 5) monitoring and management. Protection surface is a perimeter of resources that require protection through access authority control, such as confidential data and SCADA, and Transaction flow refers to data flow between system components and users interacting with them. Once the protection surface is defined and the Transaction flow is identified, a zero trust architecture and zero trust policy for Microsegmentation can be designed. Finally, through continuous monitoring, zero-trust-based security can be gradually strengthened by accumulating information such as occurrence of unauthorized flows or suspicious connections, and continuing the cycle from 1 to 5. By applying the concept of zero trust and methodology for establishing a zero trust architecture, it is possible to overcome the limitations of existing boundary network-based security as shown in Figure 4 and strengthen the security of autonomous ship remote control infrastructure.



<Source : Performance Analysis on Integrated Ship Area Network, Sung-Hyung Lee et al.(2013)>

<Figure 4 Example of Smart Ship Remote Access Security Infrastructure Using Zero Trust>

Establishing Security Infrastructure for Smart Ship Remote Access Based on Zero Trust

No.	Step	Description
1	Definition of protection surface	Protection surface is an operational technology (OT) network area* to which the autonomous ship's control system is connected. Hackers can access terminals connected to the Crew Network from remote terminals through remote control systems, thereby breaking into the OT network and performing various illegal activities. * Shipboard Control Networks, Instrument Networks, etc.
2	Identity of transaction flow	Identify which flows are used for remote control, i.e., flows that should be allowed to remotely control the control system, register them on the White-list, and log blocking all other flows other than those that are not registered as potential threats.
3	Design of zero trust architecture	• Local PEP*s are installed in remote access terminals** • Gateway PEPs are placed at the front of external entry points • Local PEP controls the environment when the external connection terminal is remotely accessed * Policy Enforcement Point ** On-shore user PC and ship's Crew PC
4	Creation of zero trust policies	• The security manager assigns tasks that can be performed during remote access according to the position and role of each remote accessor. • For critical tasks and security policy changes that require administrative authority, MSA* should be introduced to obtain additional permission from the supervisor, and notifications of job performance should be reached to the director. • The remote accessor must authenticate his/her identity on a work-by-work basis In addition, remote accessors should only be able to access protection resources through pre-authorized apps. • Local PEPs apply policies that check the environment of remote access terminals in real time and immediately block access to remote access terminals in the event of unauthorized external network access, vaccine not installed, or forgery of access programs. * Multi-Subject Authentication
5	Monitoring and control	Collect logs on the Zero Trust system for various activities such as access frequency, access IP, access location, access to protected resources, blocked access requests, etc., and visualize key statistics on the dashboard for administrators to easily understand.

<Table1 Five-Step Process for Establishing Security Infrastructure for Smart Ship Remote Access Based on Zero Trust>

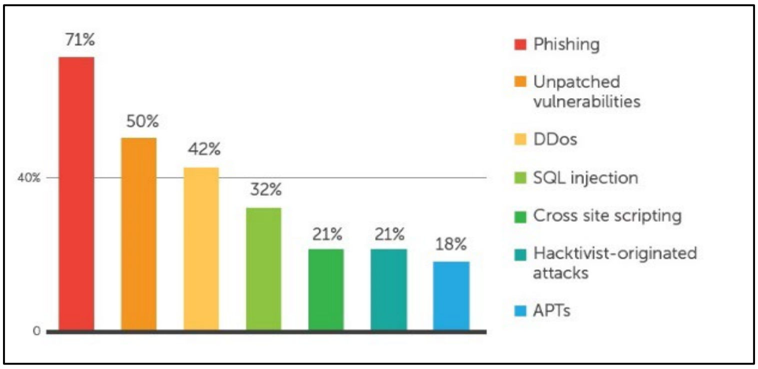
Cyber Attack Surface and Threat Intelligence

Abstract

In this document, understand the key point of the latest cyber threat management, attack surface management plan and preemptive cybersecurity, learn about the countermeasures in the maritime sector through the recently known ship cyber attack scenario description

What Is an Attack Surface?

Attack Surfaces refers to all points that can be target to cyber attacks, such as hacking and malicious infection. Recently, cyber security activities have reduced the resources required for cyber security management activities by reducing the attack surface and concentrate on important cybersecurity activities. Attack vectors are explained as paths or methods used by an attacker to access to the attack surface. Major attack vectors include ransomware, phishing, hacked accounts, weak supply chains, weak cryptography, misconfiguration, etc.. According to a cyberattack vector research by E.U. on critical infrastructure such as railways, electricity and the like, phishing, unpatched security vulnerabilities and denial of service attack (DDoS) were relatively high tendency.



<Source : CIPSEC Website>

Cyber Asset Attack Surface Management Plan

Attack surface management plan of cybersecurity threat management

① Implement risk identification and control measures through enterprise risk management strategies

② Using standardized development processes and system tools

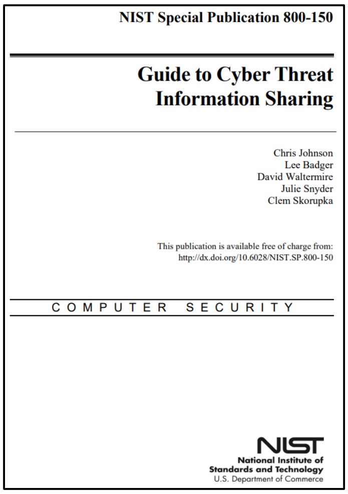
③ Identifying shipping company or ship attack surfaces and threat/vulnerabilities

④ Regulating of supply chain and control process of a shipping company or ship

Cyber Attack Surface and Threat Intelligence

Cyber Threat Intelligence

Cyber threat intelligence(CTI) is defined as a method to collect information that threatens the safety of cyber systems, analyze the situation and effectively respond to cybersecurity threat. It has the advantage of being able to preemptive cyber risk management activities by collecting and analyzing information on various cyber threats. According to a document(NIST 800-150) from the U.S. National Institute of Standards and Technology, the types of cyber threat intelligence are described as Indicators of Compromise (IOC), Attacker strategy, tactics, and Tactics, Techniques, Procedures, (TTPs), Security Alerts, and Threat Intelligence Reports.



NIST Special Publication 800-150

Guide to Cyber Threat Information Sharing

Chris Johnson
Lee Badger
David Waltermire
Julie Snyder
Clem Skorupka

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.800-150

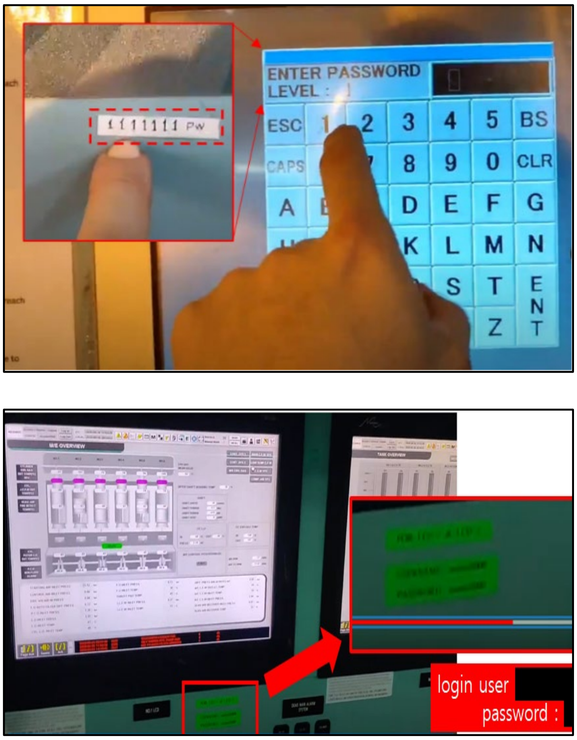
COMPUTER SECURITY

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

<NIST 800-150>

Maritime Cyber Threat Intelligence

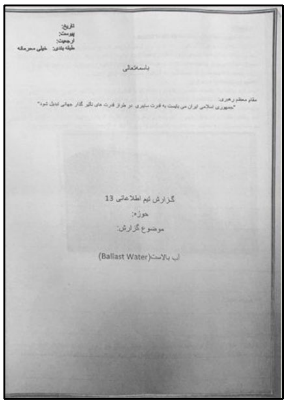
Maritime cyber threat intelligence is a cyber threat collection and analysis system specializing in shipbuilder and marine industries. For example, if a crew on board is exposing important information about the ship's internal system along with uploaded the video, name of the ship in the photo, the flight schedule on his social network service(SNS), where through the crew may become the attack surface and creating an attack vector to hack the system. So there is need to identified and reduce cyber threat early because of cyber attack exploits these threats information and open source vulnerabilities of the maritime satellite communication system it may cause critical cyber risks.



<Username, Password exposed by crew SNS>

Actual Threat of Ship Cyber Attack

In July 2021, British media Sky News released a document putative to have been written by Iran's cyberattack group[1]. The document mentions the scenario in which Iran's Revolutionary Guard's cyber attack group hacks the cargo ship's ballast water management system and pump equipment in a gas station. It has a heavily influenced because a cyber attack scenario was disclosed to the ship target and that a specific system in the hull was selected as the target of the attack.



تاریخ:
پیوست:
از جهت:
طبقه بندی: خیلی محرمانه

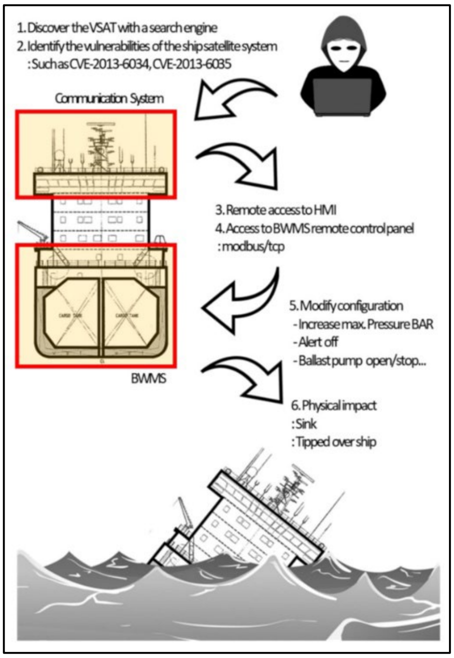
باسمه‌تعالی

مقام معظم رهبری:
"جمهوری اسلامی ایران می بایست به قدرت سایبری در طراز قدرت های تاثیر گذار جهانی تبدیل شود"

گزارش تیم اطلاعاتی 13
حوزه:
موضوع گزارش:
آب بالاست(Ballast Water)

<Leaked report>

Attack Scenario and Countermeasures


1. Discover the VSAT with a search engine
2. Identify the vulnerabilities of the ship satellite system
:Such as CVE-2013-6034, CVE-2013-6035
Communication System
3. Remote access to HMI
4. Access to BWMS remote control panel
:modbus/tcp
5. Modify configuration
-Increase max. Pressure BAR
-Alert off
-Ballast pump open/stop...
BWMS
6. Physical impact
:Sink
:Tipped over ship

In a research[2] to present a systematic cybersecurity model through a ship cyberattack scenario, the attack surface and attack vector were identified by analyzing the documents on Iran's BWMS hacking plan. Cyber attacker can find a vulnerable maritime satellite communication system on the internet, access to the inside of the hull, and manipulate the data of the BMWS system. The cyber risk management plan in this scenario is as follows.

Mitigation plan

① Establishment and management of password policy
② Prevent tempering with sensitive information
③ Patch the Open security vulnerabilities
④ Delete unnecessary programs

In the future, preemptive cyber risk management is required by development of cyberattack surface and attack vector identification technology specialized in the maritime sector through maritime cyber threat intelligence

[1] https://news.sky.com/story/irans-secret-cyber-files-on-how-cargo-ships-and-petrol-stations-could-be-attacked-12364871
[2] https://www.mdpi.com/1424-8220/22/5/1860/htm

Ship control system attack detection through Claroty CTD

CPS (Cyber-Physical Security) Company "Claroty"

Claroty empowers organizations to secure cyber-physical systems across industrial (OT), healthcare (IoMT), and enterprise (IoT) environments: the Extended Internet of Things (XIoT). The company's unified platform integrates with customers' existing infrastructure to provide a full range of controls for visibility, risk and vulnerability management, threat detection, and secure remote access. Backed by the world's largest investment firms and industrial automation vendors, Claroty is deployed by hundreds of organizations at thousands of sites globally. Claroty's cyber research organization, Team82, recently published a report on cyber attacks on industrial environments.

WHITE PAPER

THE GLOBAL STATE
OF INDUSTRIAL
CYBERSECURITY 2021:
RESILIENCE AMID
DISRUPTION

CLAROTY

<Claroty Report>

Report Summary – Severity of OT Security (including Ship Control Systems)

Global survey of 1,100 IT/OT security professionals who work for enterprises that own, operate or support components of critical infrastructure, explores how they have dealt with the significant challenges in 2021, their levels of resiliency, and priorities moving forward.

Key findings include:

① A staggering 80% of respondents experienced an attack, with 47% reporting an impact to their OT/industrial control system (ICS) environment.

② More than 60% paid the ransom and just over half (52%) paid $500,000 USD or more.

③ 90% are looking to hire but 54% say it is hard to find qualified OT security candidates.

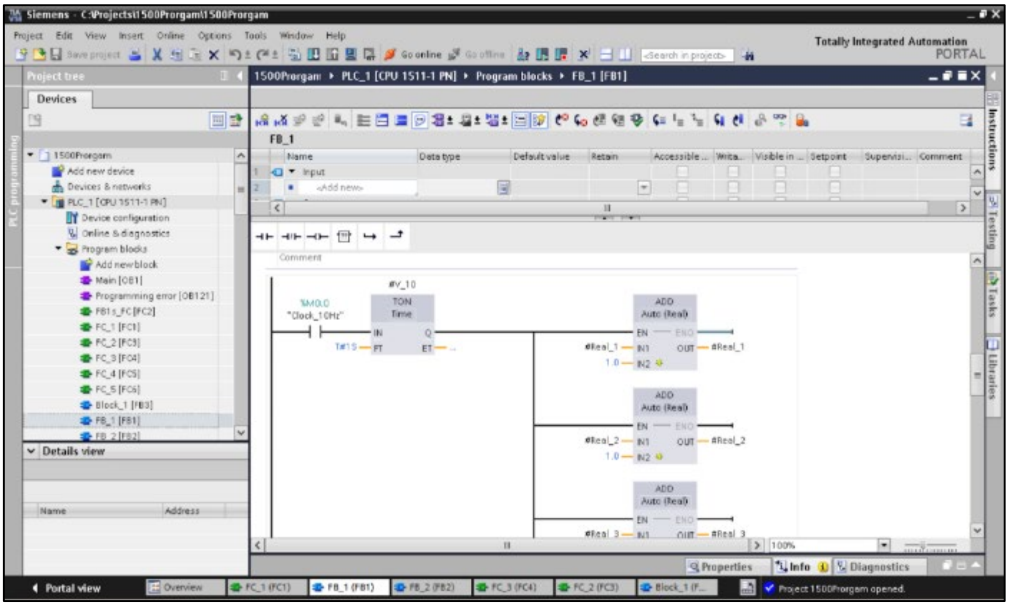
OT security vulnerabilities are reported almost every day, and OT hacking techniques targeting control systems are becoming more diverse. When a network or asset in this vulnerable OT environment is actually exploited, it can cause astronomical damage to production, safety, environment, and corporate image. However, in most OT environments including ships, the systems of various foreign manufacturers exist without security management, and security visibility and response systems were impossible because of the use of each manufacturer's dedicated communication method. In response to this, it is management, and security visibility and response systems were impossible because of the use of each manufacturer's dedicated communication method. In response to this, it is possible to respond with a security platform dedicated to Claroty OT, and it is actually being applied to various OT environments at home and abroad. The following is an example of Claroty response to a Siemens system vulnerability that is often used in ships.

Security vulnerabilities related to Siemens S7 PLC, often used in ships

A previously announced security vulnerability that could control a Siemens S7-1500 PLC bypasses the encryption mechanism of modern Siemens PLCs and allows commands to be executed on the device, allowing an attacker to tamper with the PLC's status, settings and execution logic can be changed without alarm to engineers.

Siemens PLC Settings Download Procedure

The process of changing PLC settings consists of several steps. Engineers write the logic as ladder diagrams or structured text and compile the code at the engineering station. The Totally Integrated Automation (TIA) software then encrypts the binary code using the key value provided by the PLC. The encrypted binary file is downloaded to the PLC along with the plain text code, and the PLC decrypts the binary and then executes it.



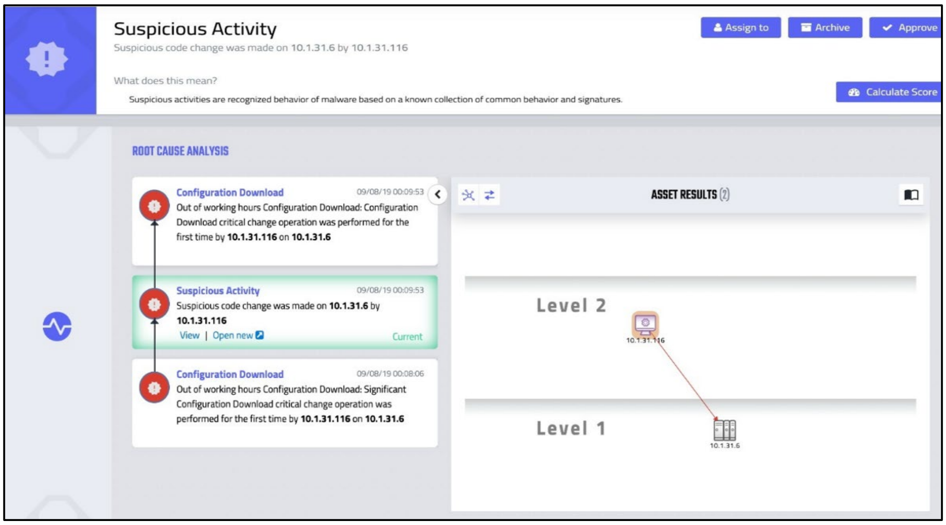
<Siemens – TIA Portal>

The flow described above has a flaw where the plaintext code is downloaded separately from the binary. The code provided to engineers in TIA software is plain text and does not necessarily match the binary being executed. Therefore, an attacker can change the PLC using the binary without changing the original plain text code, and as a result, the attacker can change the real-time code executed in the PLC in a defenseless state that the engineer cannot detect.

Response to Siemens S7 PLC security vulnerabilities through Claroty CTD solution

The Claroty CTD (Continuous Threat Detection) solution supported Siemens' Next-Gen 'S7CommPlus protocol' from its initial version, and it was able to identify all engineering tasks by monitoring the S7CommPlus protocol communication. In addition, Claroty CTD was able to analyze the configuration changes of the Siemens S7 PLC and extract the plain text code and the encrypted binary code that are downloaded to the Siemens S7 PLC. Through this, Claroty CTD can track and compare the settings of Siemens S7 PLC and detect whether a specific function block logic has been changed. As you can see in the image below, even if the code is encrypted, a legitimate setting change will also change the plaintext code and setting metadata.

Detection of "Suspicious Activity Alert" during Siemens PLC configuration download process



Suspicious Activity

Suspicious code change was made on 10.1.31.6 by 10.1.31.116

What does this mean?

Suspicious activities are recognized behavior of malware based on a known collection of common behavior and signatures.

ROOT CAUSE ANALYSIS

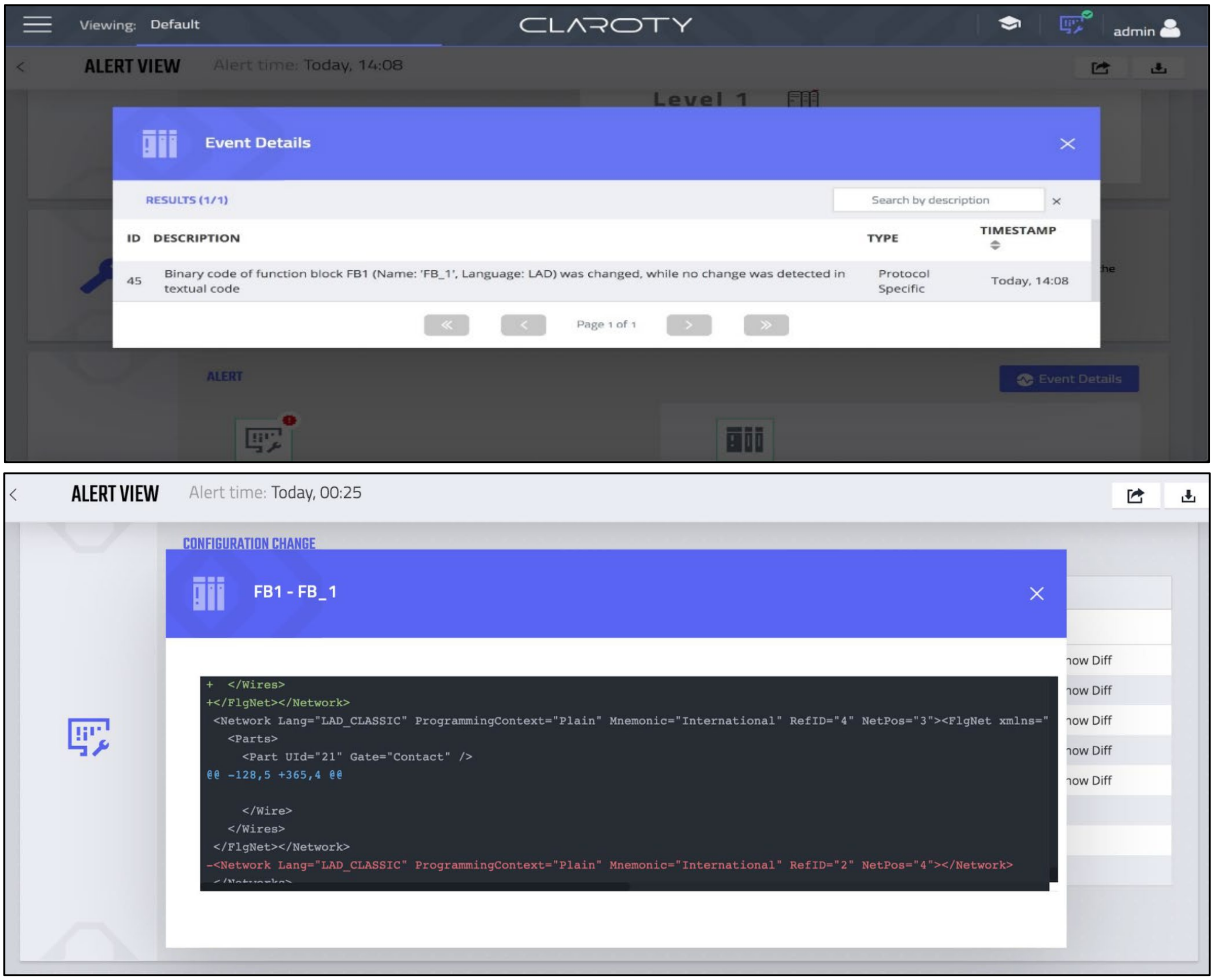
Configuration Download 09/08/19 00:09:53
Out of working hours Configuration Download: Configuration Download critical change operation was performed for the first time by **10.1.31.116** on **10.1.31.6**

Suspicious Activity 09/08/19 00:09:53
Suspicious code change was made on **10.1.31.6** by **10.1.31.116**
View | Open new
Current

Configuration Download 09/08/19 00:08:06
Out of working hours Configuration Download: Significant Configuration Download critical change operation was performed for the first time by **10.1.31.116** on **10.1.31.6**

<Claroty CTD (Continuous Threat Detection)>

Ship control system attack detection through Claroty CTD



RESULTS (1/1)

ID	DESCRIPTION	TYPE	TIMESTAMP
45	Binary code of function block FB1 (Name: 'FB_1', Language: LAD) was changed, while no change was detected in textual code	Protocol Specific	Today, 14:08

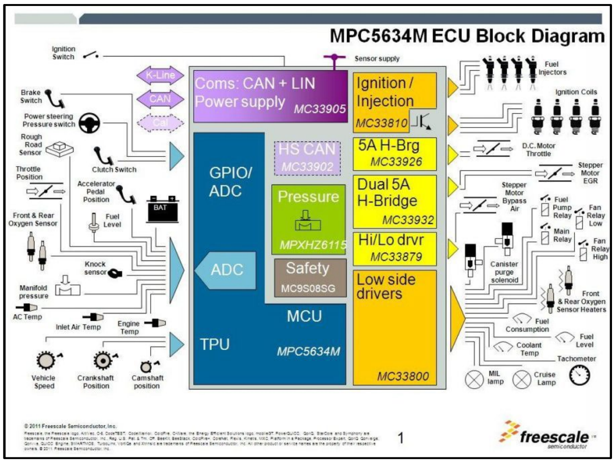
```
+  </Wires>
+</FlgNet></Network>
 <Network Lang="LAD_CLASSIC" ProgrammingContext="Plain" Mnemonic="International" RefID="4" NetPos="3"><FlgNet xmlns="
   <Parts>
     <Part UId="21" Gate="Contact" />
@@ -128,5 +365,4 @@

     </Wire>
   </Wires>
 </FlgNet></Network>
-<Network Lang="LAD_CLASSIC" ProgrammingContext="Plain" Mnemonic="International" RefID="2" NetPos="4"></Network>
```

<Claroty CTD (Continuous Threat Detection)>

Using Claroty CTD's S7CommPlus protocol and detection technology for Siemens configuration downloads, you can verify configuration changes and ensure that your binary and plaintext code have been changed consistently. In other words, in the case of a previously announced security vulnerability ‘in case of a binary code change attack’, Claroty CTD can detect/analyze that the settings have been suspiciously changed as follows. Although it is impossible with existing IT security solutions, by using the Claroty platform like this, security visibility of networks and systems in the OT environment including ships is basically secured, and known vulnerabilities (CVE) and Purdue model-based inter-area/inter-asset threat alert monitoring and OT By providing a dedicated remote access control solution, you can complete the OT security management and response system.

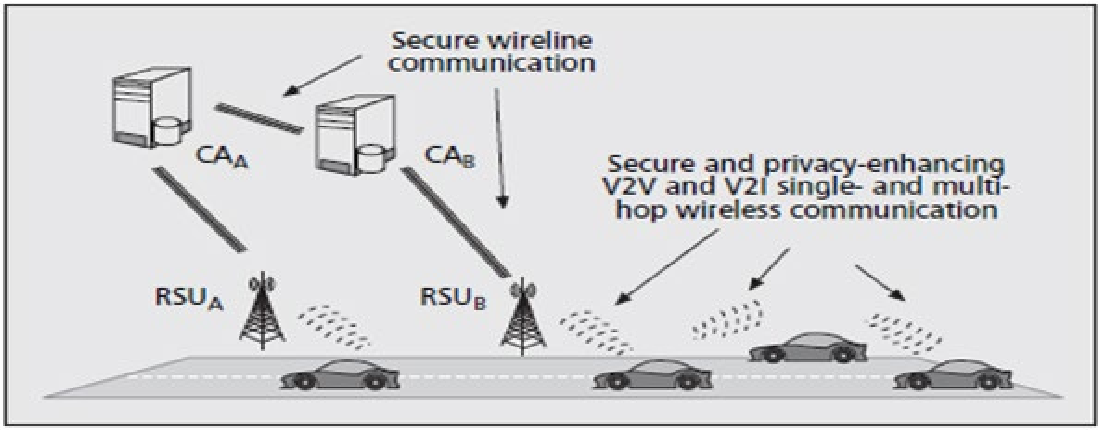
Road vehicle security standard development status

Technically in order to secure the cyber security of a ship, it is necessary to know how the equipment and systems installed on the ship are connected and operated. In the case of a car, it is possible to access the ECU (Electronic Control Unit) with a certain amount of effort and analyze the operating principle of the CAN (Controller Area Network) which is an internal network and it is possible to easily purchase and analyze a drone. However in reality it is difficult to obtain domain knowledge about the vessel because it is difficult to access the vessel. Due to the difficulty in acquiring domain knowledge, the field of ship cyber security is relatively behind compared to other fields. Therefore it is time to apply the security technologies and standards already applied in various fields in consideration of the special environment of the ship. In the automobile sector we would like to introduce the road vehicle security standard development status that is applicable to the maritime sector as it is similar to the situation of ships, such as for the purpose of transporting people and cargo and applying autonomous driving technology. With the development of IT technology, various IT technologies are being applied to automobiles as well. The latest automobiles are equipped with various ICT technologies to build advanced automobile environments such as autonomous driving systems and active safety systems and to minimize exhaust gas emissions. In addition the connected car industry, in which automobiles and mobile communication technologies converge, is drawing attention as a new blue ocean, and various infotainment services that connect portable electronic devices (e.g., smartphones, tablet PCs, MP3 players) and automobiles is also growing rapidly. However recently various ICT technologies have been applied to automobiles without adequate consideration of security and automobiles have also become targets of cyber attacks.



<Example of ECU and CAN diagram>

CAN, the standard communication standard for automobiles, is built as an internal network in various types of automobiles. However although CAN is a broadcast communication protocol, it does not provide any data encryption or authentication function so an attacker can eavesdrop on CAN communication and forge or forge the communication section message. In the Tied Car Vulnerability Analysis Study, the vulnerability of the Aqlink protocol was analyzed and an attack was performed to remotely control the car. In order to respond to such security threats to automobiles, countries around the world are developing automobile security standards while conducting automobile security projects. In Korea we conducted a research project to prove the vulnerability of CAN communication through hacking experiments using real cars and to design encryption and authentication techniques that can protect CAN communication from these threats. The SEVECOM project that defined and defined cryptographic primitives for this was carried out. The automotive security standard is typically IEEE 1609, which defines the comprehensive contents of the IEEE 802.11p upper layer, such as the architecture for WAVE communication, specification of standardized services and interfaces, and security for V2V and V2I wireless communication. IEEE 1609 was divided into four parts from 1609.1 to 1609.4 and standardization proceeded. In particular, IEEE 1609.2 describes the security message standard used in the intelligent car network and the processing procedure for secure communication.

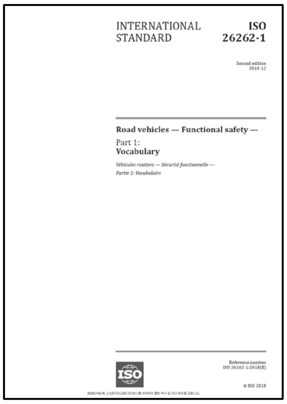

Secure wireline communication
CA$_A$
CA$_B$
Secure and privacy-enhancing V2V and V2I single- and multi-hop wireless communication
RSU$_A$
RSU$_B$

<Example of security structure of SEVECOM project>

(Picture Source: Smart car security technology trends (2015) / Journal of Information Processing Society)

Road vehicle security standard development status

AUTOSAR (AUTomotive Open System Architecture) and ISO 26262 standards were established to enhance the functional safety and interoperability of electronic control devices for automobiles. AUTOSAR is an open automotive standard software structure, developed by major automotive manufacturers and automotive electronic component developers. Since 2009, the specification for automotive encryption service has been added, and as of 2014, version 2.2.0 for automotive encryption service has been released. The ISO 26262 standard is an international standard that adapts the functional safety international standard (IEC 61508) to the automotive electrical/electronic system, and was established to prevent accidents caused by errors in the software installed in the vehicle. Road vehicle issued in 2021 – ISO/SAE 21434, an international standard for cyber security engineering, reduces the risk of damage caused by cyber attacks or attacks that may occur in the stages of design, manufacturing, shipment, operation, and disposal of vehicles from planning research It is a vehicle cyber security standard that aims to establish and operate a cyber security response system in all activities at each stage to reduce It is being developed, and based on this, new car models are required to receive type approval from July 2022 and existing car models from July 2024.



INTERNATIONAL STANDARD

ISO 26262-1

Second edition
2018-12

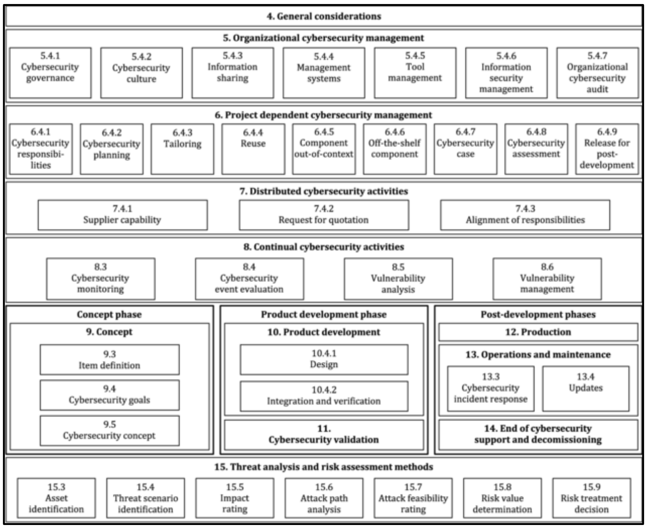
Road vehicles — Functional safety —
Part 1:
Vocabulary

Véhicules routiers — Sécurité fonctionnelle —
Partie 1: Vocabulaire

Reference number
ISO 26262-1:2018(E)

© ISO 2018

<ISO 26262>



4. General considerations

5. Organizational cybersecurity management
- 5.4.1 Cybersecurity governance
- 5.4.2 Cybersecurity culture
- 5.4.3 Information sharing
- 5.4.4 Management systems
- 5.4.5 Tool management
- 5.4.6 Information security management
- 5.4.7 Organizational cybersecurity audit

6. Project dependent cybersecurity management
- 6.4.1 Cybersecurity responsibilities
- 6.4.2 Cybersecurity planning
- 6.4.3 Tailoring
- 6.4.4 Reuse
- 6.4.5 Component out-of-context
- 6.4.6 Off-the-shelf component
- 6.4.7 Cybersecurity case
- 6.4.8 Cybersecurity assessment
- 6.4.9 Release for post-development

7. Distributed cybersecurity activities
- 7.4.1 Supplier capability
- 7.4.2 Request for quotation
- 7.4.3 Alignment of responsibilities

8. Continual cybersecurity activities
- 8.3 Cybersecurity monitoring
- 8.4 Cybersecurity event evaluation
- 8.5 Vulnerability analysis
- 8.6 Vulnerability management

Concept phase
9. Concept
- 9.3 Item definition
- 9.4 Cybersecurity goals
- 9.5 Cybersecurity concept

Product development phase
10. Product development
- 10.4.1 Design
- 10.4.2 Integration and verification

11. Cybersecurity validation

Post-development phases
12. Production
13. Operations and maintenance
- 13.3 Cybersecurity incident response
- 13.4 Updates

14. End of cybersecurity support and decomissioning

15. Threat analysis and risk assessment methods
- 15.3 Asset identification
- 15.4 Threat scenario identification
- 15.5 Impact rating
- 15.6 Attack path analysis
- 15.7 Attack feasibility rating
- 15.8 Risk value determination
- 15.9 Risk treatment decision

<ISO 21434 document configuration example>

Just as international standards for cyber security for automobiles composed of systems with enhanced automation and connectivity are continuously issued and applied, in the maritime field, research on autonomous vessels and unmanned vessels is also conducted to protect these vessels from cyber attacks. and cyber security international standards for ship-mounted equipment/systems are needed.

(Original source: TTA automobile-ICT technology convergence
and security technology trends (2014))

Risk Assessment Technique Based on CVSS

Cyber Risk Assessment Technique for IT and OT System in Companies/Ships

① Conduct a vulnerability check on cyber assets

② Establish a cyber risk scenario based on the vulnerability check result

③ Evaluate my assets for cyber risk scenarios with colleagues

Understanding Cyber Asset Risk Assessment

In "Industrial Cyber Security (Pascal Ackerman, 2017)", risk assessment is defined as evaluating the vulnerabilities hidden in cyber assets, the likelihood that the vulnerabilities will be attacked*, and the consequences that a successful attack will have on the system**. The risk score for the discovered vulnerabilities is explained as the result of risk evaluation, and the following formula is provided to calculate the risk score.

$$\text{risk} = \frac{severity+(criticality*2)+(likelihood*2)+(Impact*2)}{4}$$

<Risk Scoring Formula>

(Source : Industrial Cybersecurity by Pascal Ackerman)

Cyber asset risk assessment is the first step in building a company / ship cyber security system and is a necessary step to minimize unnecessary costs in establishing a cyber security system. For the above cyber asset risk assessment, the following tasks should be performed.

- Step 1 (Asset Identification and Vulnerability Check) : Identifies assets that can be the target of potential cyber attacks in companies/ships, and analyzes the security vulnerabilities of the identified assets

- Step 2 (Risk Scenarios) : List possible actionable cyber risk scenarios by defining threat targets (attackers) and threat events for each cyber asset

- Step 3 (Risk Assessment) : Conduct risk assessment with relevant stakeholders based on risk scenarios for the target company/ship

* Refers to a procedure or series of commands, scripts, programs, or specific pieces of data designed to perform an attacker's intended action by exploiting design flaws such as bugs and security vulnerabilities in cyber assets such as computer software or hardware.

** Includes companies affected by this

Step 2 : Risk Scenario

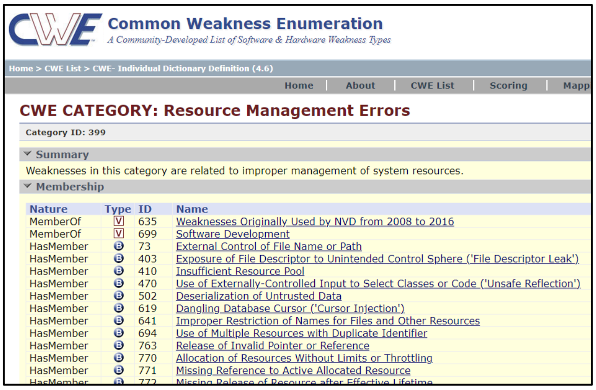
For cyber risk assessment, when target asset identification is completed and vulnerabilities fo r each asset are identified, it is recommended to create a imaginary risk scenario by inferring possible cyber threats through the identified vulnerabilities. The cyber risk imaginary scenari o can be used as a risk assessment index by objectively quantifying the attack type and possi bility by asset, and can be usefully used from the perspective of cyber asset management.

☐ Risk Scenario

○ Target Ship/System :

Asset Name	Asset Detail Info.	Asset Type	Threat Vector	Threat Agent	Attack Targets	Possible Consequence	Likelihood Index	Impact Index
XXX Team Server	XXX Team Server RM (2nd fllor) MAC Add: 88:D7:F6:xx:xx:xx IP Add : 192.168.102.xxx OS: MS Windows 10 1709 - 1909	SCADA Server	Computer and ICS Applications	hackers/ hacktivists	Gain remote access rigth/control	Credential leak (control)	2	1

- (Attack targets) identify the attack targets of the threat factors(hackers) through identified vulnerabilities in the assets. The method for identifying an attack target can infer an attack target by using CWE information (simple information), or define the type of attack by type of asset (server, network equipment, etc.) in advance and define the target through this.


CWE
Common Weakness Enumeration
A Community-Developed List of Software & Hardware Weakness Types
Home > CWE List > CWE- Individual Dictionary Definition (4.6)
Home
About
CWE List
Scoring
Mapp

CWE CATEGORY: Resource Management Errors

Category ID: 399

Summary

Weaknesses in this category are related to improper management of system resources.

Membership

Nature	Type	ID	Name
MemberOf	V	635	Weaknesses Originally Used by NVD from 2008 to 2016
MemberOf	V	699	Software Development
HasMember	B	73	External Control of File Name or Path
HasMember	B	403	Exposure of File Descriptor to Unintended Control Sphere ('File Descriptor Leak')
HasMember	B	410	Insufficient Resource Pool
HasMember	B	470	Use of Externally-Controlled Input to Select Classes or Code ('Unsafe Reflection')
HasMember	B	502	Deserialization of Untrusted Data
HasMember	B	619	Dangling Database Cursor ('Cursor Injection')
HasMember	B	641	Improper Restriction of Names for Files and Other Resources
HasMember	B	694	Use of Multiple Resources with Duplicate Identifier
HasMember	B	763	Release of Invalid Pointer or Reference
HasMember	B	770	Allocation of Resources Without Limits or Throttling
HasMember	B	771	Missing Reference to Active Allocated Resource
HasMember	B	772	Missing Release of Resource after Effective Lifetime

<Attack target inference method using CWE information>

- (Possible consequences) The impact of an asset through a cyber attack should be defined. The impact of an asset on a cyber attack should be defined in advance in the form that can occur for each type of asset, and based on the defined impact, stakeholders should list the impact of the asset for each attack target.

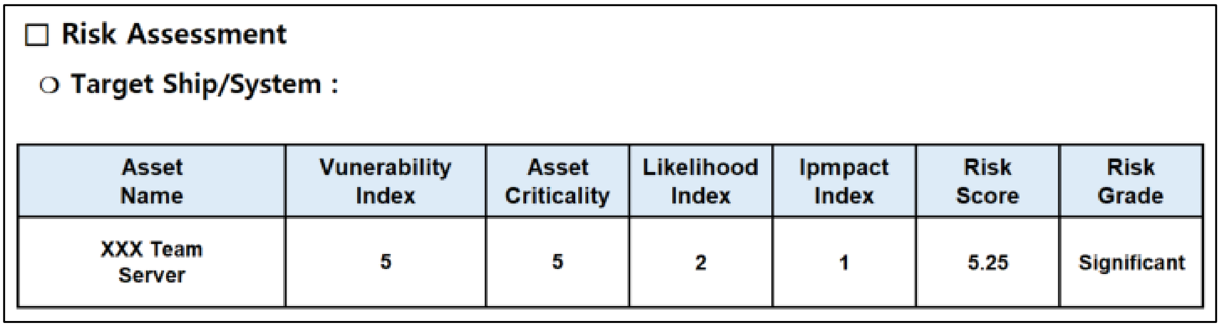
Table. 3 Possible Consequence

Type	List of possible consequence
Controller/PLC	Controller fault
	Factory downtime/closed
	Process degradeation/failure
	Loss of process control
	Process image loss
	Data corruption detection

<examples of possible consequence by asset>

Step 3: Risk Assessment

Once the asset identification and cyber risk scenario for each asset are established, it is reco mmended to quantify the risk by allocating scores for attack success probability, impact, and asset importance.



□ Risk Assessment

○ Target Ship/System :

Asset Name	Vunerability Index	Asset Criticality	Likelihood Index	Ipmpact Index	Risk Score	Risk Grade
XXX Team Server	5	5	2	1	5.25	Significant

- (Attack Success Probability, Impact) Once the target of a cyber attack and possible results are defined, a score should be assigned and used for risk quantification. In order to objectively quantify the attack success probability and influence, it is recomme nded to classify it into 5 grades and define the criteria for each grade. It is recommended t hat the attack success probability be based on accessibility or security equipment level, an d the impact level based on system usability.
- (Asset Criticality) For risk assessment, the materiality of each asset should be defined. It is recommended to classify the criteria of asset importance into five grades. It is suggest ed to refer to the classification criteria (UR E22) when defining the class.
- (Risk Assessment) After asset identification, vulnerability assessment, risk scenario develo pment, and quantification are completed, risk score quantification should be performed us ing the formula below, and risk mitigation activities should be carried out through this.

$$\text{risk} = \frac{severity+(criticality*2)+(likelihood*2)+(Impact*2)}{4}$$

<Example risk assessment formula>

KR cyber security training tool release, E-LEARNING training

KR, cyber security training tool released

KR released cyber security training tool. In the 2021 version compared to the 2020 version of KR-CS++ released last year, new videos consisting of more specific and practical contents were added.

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-CS^{++} 2021

The Maritime Cyber Security Awareness Training

KR-CS^{++} is a training material for your shore staffs and crews to raise maritime cyber security awareness.

CS^{++} means beyond Cyber Security Services.

Copyright © Korean Register All rights reserved.

KR is keen to provide its services in various ways, eg. online and via USB-type KR-CS++ 2021 for the convenience of its customers. KR currently provides the same service through cyber security e-learning training and plans to release a tablet-enabled KR-CS++.

KR maritime cyber security E-learning center reorganization of curriculum

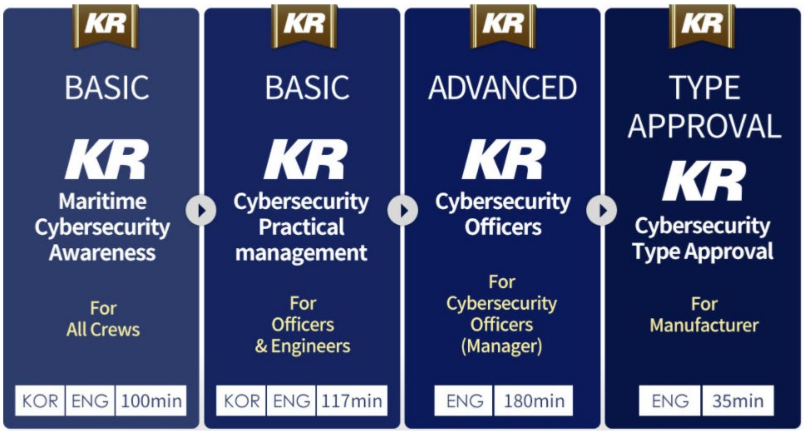
KR reorganized the cyber security e-learning training in cooperation with Orange Security, who is a maritime cyber security specialist. Through this reorganization of e-learning training, KR becomes to provide customized training for each customer.

Korean Register's Maritime Cyber Security e-Learning Course

MCS e-Learning system open!

- https://edu.orangecq.com/

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.



KOREAN REGISTER

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