KR Cyber Security

News from KOREAN REGISTER

July 2018

Vol. 003

KR Cyber Security Activity

- **Korean Register signs a cyber security MOU with Yokogawa**

On July 2, Korean Register of Shipping (KR) and Yokogawa Electric Co., Ltd. (Yokogawa) signed an MOU to strengthen the mutual technology exchange between the two organizations and confirming cooperation on joint research and development on cyber security for shipping. Yokogawa is a provider of ship automation system solutions, providing unique technologies for specific markets (industrial plants, refinery facilities and LNG carriers) through the integrated control systems and providing high level cyber security solutions for the industry .

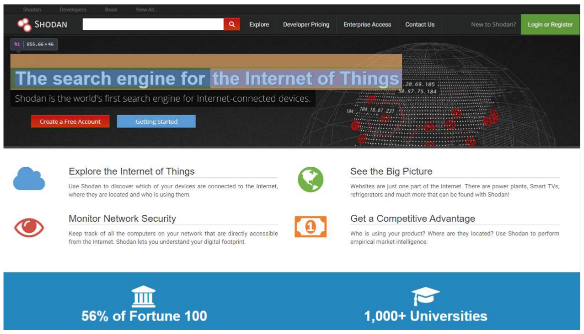
The MOU is expected lead to joint research on the following technologies with consensus on technology exchange and joint research and development between KR and Yokogawa

- Maritime cyber security management system certification
- Application of the ship cyber security operating technology (OT) system rules

Through the signing of the MOU, it is expected that the items to be inspected for maritime cyber security equipment provider certification will be verified and the inspection items of the ship OT system will be improved through actual test application.

YOKOGAWA
Co-innovating tomorrow
(주)요꼬가와전기와 한국선급의
상호협력 강화를 위한 MOU 체결식
2018. 7. 2
KR
KOREAN REGISTER

Pen Tester finds several ways to hijack, track, steal, sink ships



The search engine for the Internet of Things

Shodan is the world's first search engine for Internet-connected devices.

Explore the Internet of Things

Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.

See the Big Picture

Websites are just one part of the Internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan!

Monitor Network Security

Keep track of all the computers on your network that are directly accessible from the Internet. Shodan lets you understand your digital footprint.

Get a Competitive Advantage

Who is using your product? Where are they located? Use Shodan to perform empirical market intelligence.

A pen test found that the cyber security of shipping and marine logistics was Low-level, exposing them to a variety of cyber security threats, as like Hijacking, Tracking, and Steal.

● 20 different ECDIS tested

According to cyber-security penetration testing firm, Pen Test Partners, about 20 different ECDISs have identified vulnerabilities which could allow an attacker to control the operation technology (OT) systems used to control the steering gear, engines and so on. The research team conducted administrative interface access via Telnet and HTTP, firmware authentication bypass, and web application testing, demonstrating that they were able to control ECDIS and change data and ship paths in the course of GPS satellites and communications. In the pen test, information and vulnerabilities were collected and tested through Shodan, which is a popular search engine in ICS.

● Basic Activities, Password, Security Patch

In order to solve this problem, the firm stressed that setting the administrator's password for the systems and patching vulnerabilities as well as prompt response from the ship owner and ship operator. More detailed penetration data can be found at the link below.

Hacking, tracking, stealing and sinking ships

Response and Suggestion

To prevent access by unauthorized people, the on-board operation system should be separation of the network between IT and OT system, and upgrade of Operation System stopped supporting security patch such as Windows NT server.

Ref. : Pen Tester finds several ways to hijack, track, steal, sink ships, SC MEDIA, June , 2018

How to secure the bridge from cyber attacks

With broadband connectivity becoming more common and on-board navigation and data systems have also increased the possibility of unauthorized attacks, navigation company Nautisk emphasizes the need for cybersecurity on bridge.

- **Network and devices security**

Nautisk explained that the vessel's security threats could begin all of the ECDIS download process and communication between ships and the offshore, and thus the network of measures to address these issues. Network units need to prevent malware with firewalls and antivirus, from entering the network, and suggested limitations of connections through USB sticks. They also suggested a strictly closed console policy for operation system such as ECDIS.

- **Three proposal for cyber security**

In addition to detailed measures for ship cybersecurity, Nautisk also emphasized three things

1. Embrace a security-awareness culture that will help reduce the vulnerability of the bridge.
2. Introduce tools – hardware and software – to strengthen your defence as part of your overriding security strategy.
3. Train the crew to understand the risks and their responsibilities on board.

Response and Suggestion

Ship owners, shipyards must understand the need for more systematic and specialized activities, for vessel cybersecurity. In particular, it should prepare for change management about process and practices without considering cybersecurity.

Ref. :How to secure the bridge from cyber attacks, Hellenic Shipping News Worldwide, June, 2018

Human Element Is Part Of The Maritime Cyber Problem

Most of the cyber security issues on ships are caused by people, and it has been found that it is urgent to upgrade the old version of OS that does not support security patches.

- **The problem is 'people'**

According to Itai Sela, CEO of Naval Dome, who attended the European Maritime Cyber Risk Management Summit held last June, incidents, as like malicious code infections, occur during the process of uploading system files or connecting one's cell phone, laptop, or tablet to the system. Sela added that systems with old OS that do not have security management, such as Window XP, Window 7 or older versions of Linux, should upgrade new version.

- **IMO, TMSA, The maintenance of laws and guidelines**

The cyber security experts in the summit said that the marine industry is likely to be a major target for external attackers due to cost and competitive situations among industries. For this, they expect that laws and guidelines such as ISM code, IMO's MSC.428 and TSMA will be expanded and enhanced.

Response and Suggestion

Vessel's cyber security will continue strengthening with IMO and ISM codes. The owners and the shipping companies need to draw up a direction for investment in cyber security in preparation for compliance, while investing in cyber security education and improved awareness.

Ref. : Global Maritime Information Market Analysis 2018 Forecast to 2022 with Inmarsat, Business Wire, May, 2018

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)

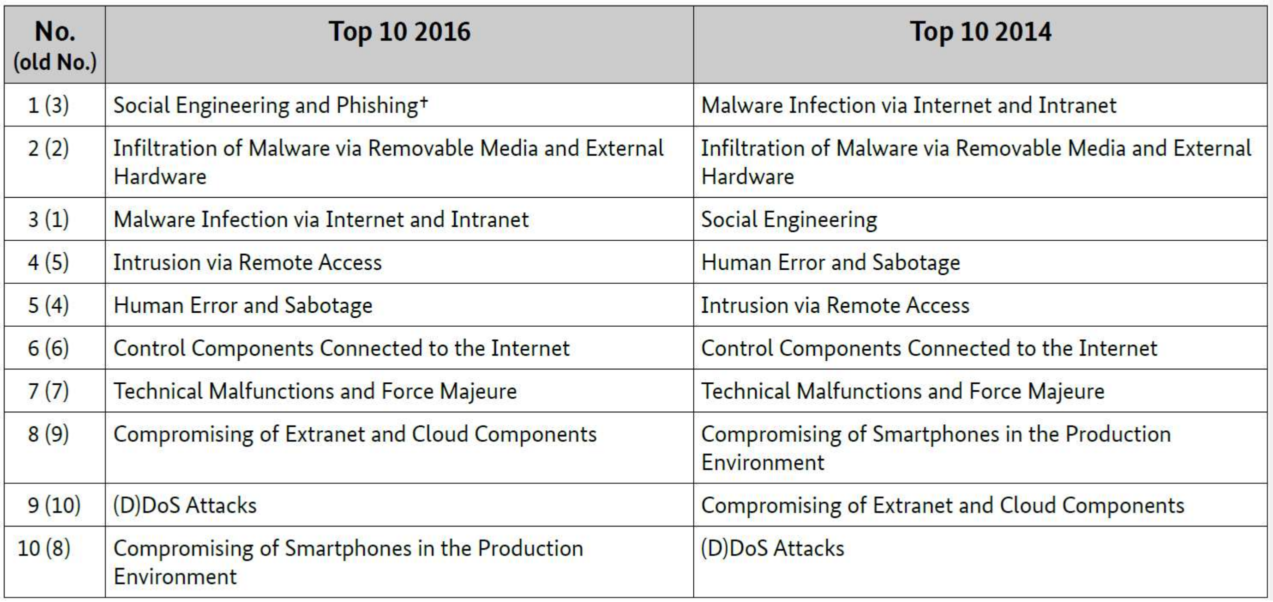
Cyber threats need to be categorized periodically to identify vulnerabilities of assets as their impact on the asset

- **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. This newsletter will refer to 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

Understanding Cyber Threat

● Infiltration of Malware via Removable Media

Removable media such as USB flash drives are very widely used. Company employees often use them both in the office and ICS networks. External personnel often carry their own removable media, too. The use of notebook computers with external data and maintenance software, potentially used by external maintenance staff at different companies, is also widespread and carries comparable risks.

ICS security awareness is mainly limited to the aspects of availability and physical security such as safety, access restrictions and protection from external influences. In contrast, employees are often unaware of the effects caused by malware.

<Potential threat scenarios>

▣ USB flash drives may have been infected in the office network or in private environment. That way, malware can find its way directly into ICS networks.

▣ Notebook computers used for maintenance may have been infected when accessing the Internet, office networks or in the infrastructure of the respective service provider. As soon as they are then operated in the ICS network, systems and components there become infected with malicious code.

<Countermeasures>

1. Organizational policies and technical controls with regard to removable media

- Taking inventory and whitelisting of approved removable media.
- Security perimeter for removable media (virus protection and file whitelisting)
- Exclusive use of in-house, possibly personalized removable media
- Exclusive use in the ICS network.
- Physical barriers preventing (unauthorized) connection of USB
- Full encryption of data media

2. Organizational policies and technical controls with regard to external notebook computers used for maintenance

- Exchange of data only via removable media subject to the controls above
- Introduction of quarantine networks for access of external service providers
- Scanning the brought-in notebooks for vulnerabilities before accessing
- Full encryption of maintenance notebook computers

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

Guideline for Cyber Security Asset List

● The need for cyber security asset list

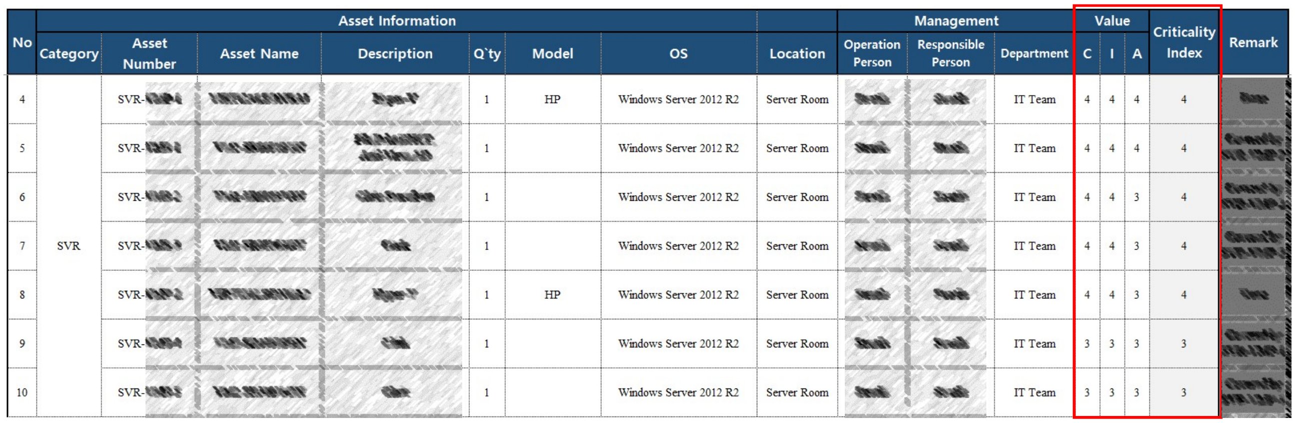
Asset management is required to identify and classify major cyber assets and to protect cyber incidents such as damage, tampering, and leakage. An asset list is the first step in asset management and can identify key assets by performing asset criticality assessments in terms of confidentiality, integrity, and availability. Asset classification and asset importance evaluation results can be used for the cyber risk assessment

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

205.1 Asset Management) All assets to be protected, such as systems, facilities, data, etc. should be established and classified.

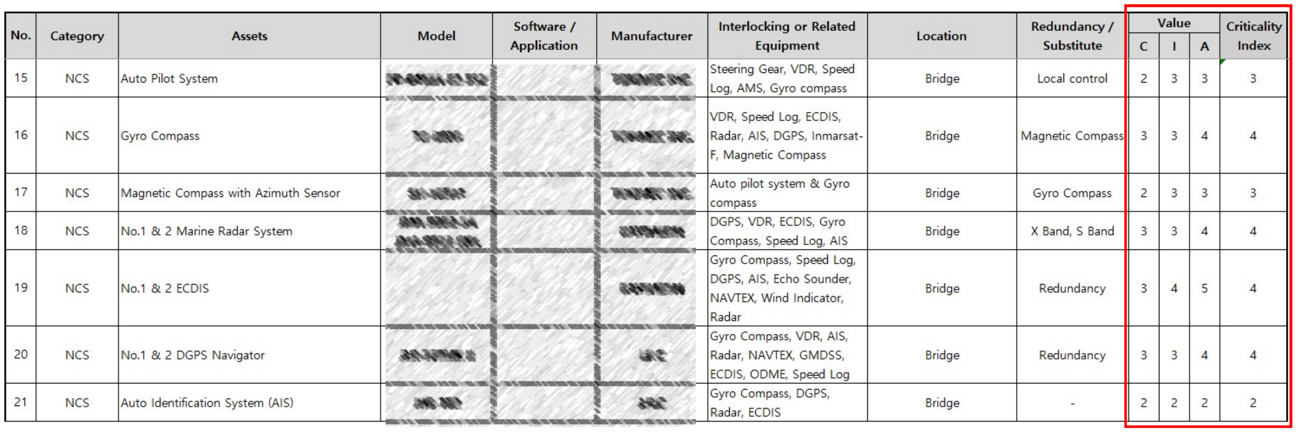
● Example of asset list

<Server System>



No	Asset Information								Management			Value			Criticality Index	Remark
	Category	Asset Number	Asset Name	Description	Q`ty	Model	OS	Location	Operation Person	Responsible Person	Department	C	I	A		
4	SVR	SVR-[redacted]	[redacted]	[redacted]	1	HP	Windows Server 2012 R2	Server Room	[redacted]	[redacted]	IT Team	4	4	4	4	[redacted]
5		SVR-[redacted]	[redacted]	[redacted]	1		Windows Server 2012 R2	Server Room	[redacted]	[redacted]	IT Team	4	4	4	4	[redacted]
6		SVR-[redacted]	[redacted]	[redacted]	1		Windows Server 2012 R2	Server Room	[redacted]	[redacted]	IT Team	4	4	3	4	[redacted]
7		SVR-[redacted]	[redacted]	[redacted]	1		Windows Server 2012 R2	Server Room	[redacted]	[redacted]	IT Team	4	4	3	4	[redacted]
8		SVR-[redacted]	[redacted]	[redacted]	1	HP	Windows Server 2012 R2	Server Room	[redacted]	[redacted]	IT Team	4	4	3	4	[redacted]
9		SVR-[redacted]	[redacted]	[redacted]	1		Windows Server 2012 R2	Server Room	[redacted]	[redacted]	IT Team	3	3	3	3	[redacted]
10		SVR-[redacted]	[redacted]	[redacted]	1		Windows Server 2012 R2	Server Room	[redacted]	[redacted]	IT Team	3	3	3	3	[redacted]

<OT System>



No.	Category	Assets	Model	Software / Application	Manufacturer	Interlocking or Related Equipment	Location	Redundancy / Substitute	Value			Criticality Index
									C	I	A	
15	NCS	Auto Pilot System	[redacted]	[redacted]	[redacted]	Steering Gear, VDR, Speed Log, AMS, Gyro compass	Bridge	Local control	2	3	3	3
16	NCS	Gyro Compass	[redacted]	[redacted]	[redacted]	VDR, Speed Log, ECDIS, Radar, AIS, DGPS, Inmarsat-F, Magnetic Compass	Bridge	Magnetic Compass	3	3	4	4
17	NCS	Magnetic Compass with Azimuth Sensor	[redacted]	[redacted]	[redacted]	Auto pilot system & Gyro compass	Bridge	Gyro Compass	2	3	3	3
18	NCS	No.1 & 2 Marine Radar System	[redacted]	[redacted]	[redacted]	DGPS, VDR, ECDIS, Gyro Compass, Speed Log, AIS	Bridge	X Band, S Band	3	3	4	4
19	NCS	No.1 & 2 ECDIS	[redacted]	[redacted]	[redacted]	Gyro Compass, Speed Log, DGPS, AIS, Echo Sounder, NAVTEX, Wind Indicator, Radar	Bridge	Redundancy	3	4	5	4
20	NCS	No.1 & 2 DGPS Navigator	[redacted]	[redacted]	[redacted]	Gyro Compass, VDR, AIS, Radar, NAVTEX, GMDSS, ECDIS, ODME, Speed Log	Bridge	Redundancy	3	3	4	4
21	NCS	Auto Identification System (AIS)	[redacted]	[redacted]	[redacted]	Gyro Compass, DGPS, Radar, ECDIS	Bridge	-	2	2	2	2

Guideline for Asset List

- **Asset criticality index**

The importance of assets in cybersecurity can be determined through their importance to the organization enabling it to maintain business functions, the assets can be further evaluated based on confidentiality, integrity, and availability.

<Example of asset criticality index evaluation>

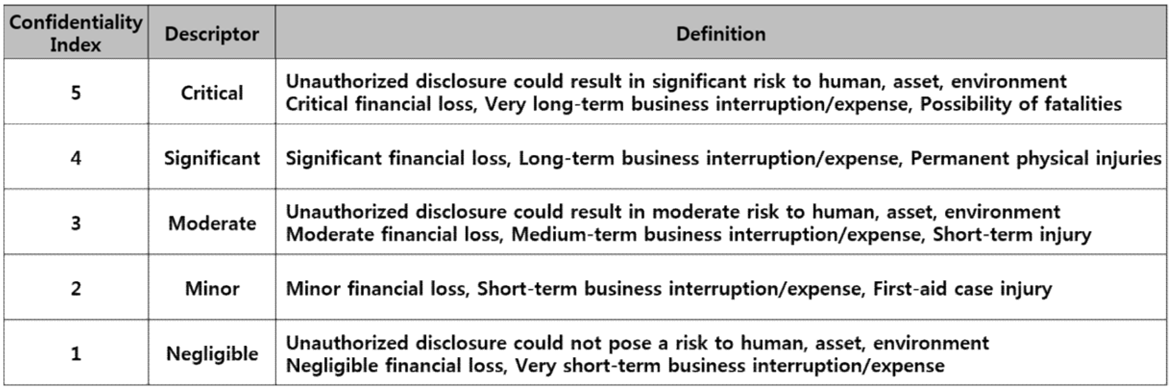
Criticality Index : CrI = CoI + II + AI

Three(3) factors are considered : **Confidentiality (C), Integrity (I), Availability (A)**

Sum of Asset Criticality Value	Category	(CrI)
13 ≤ Asset Criticality ≤ 15	Definite	5
10 ≤ Asset Criticality ≤ 12	Probable	4
7 ≤ Asset Criticality ≤ 9	Occasional	3
5 ≤ Asset Criticality ≤ 6	Remote	2
3 ≤ Asset Criticality ≤ 4	Improbable	1

- **Confidentiality index**

Confidentiality ensures that only the authorized users have access to the asset and classifies it by taking into account the business impact of the unauthorized use of assets and access to information.



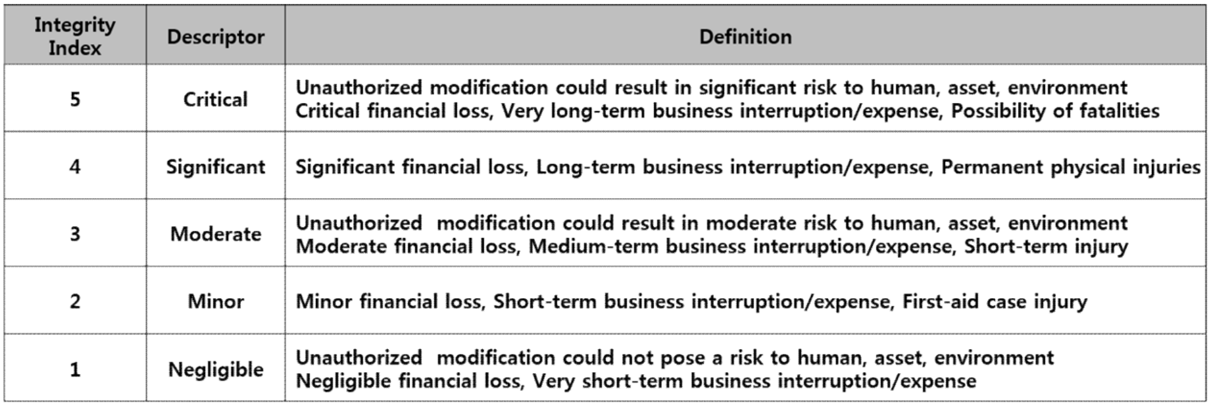
Confidentiality Index	Descriptor	Definition
5	Critical	Unauthorized disclosure could result in significant risk to human, asset, environment Critical financial loss, Very long-term business interruption/expense, Possibility of fatalities
4	Significant	Significant financial loss, Long-term business interruption/expense, Permanent physical injuries
3	Moderate	Unauthorized disclosure could result in moderate risk to human, asset, environment Moderate financial loss, Medium-term business interruption/expense, Short-term injury
2	Minor	Minor financial loss, Short-term business interruption/expense, First-aid case injury
1	Negligible	Unauthorized disclosure could not pose a risk to human, asset, environment Negligible financial loss, Very short-term business interruption/expense

Guideline for Asset List

- **Integrity index**

Integrity is the specific properties that prevent forgery by unauthorized persons. Classification is based on the impact of business damage if the accuracy or reliability of assets or information is lost.

< Example of integrity index evaluation >

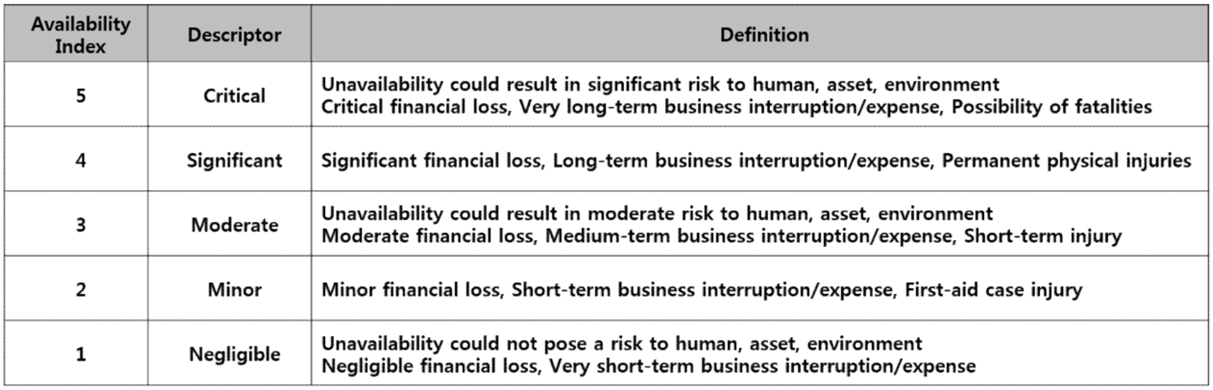


Integrity Index	Descriptor	Definition
5	Critical	Unauthorized modification could result in significant risk to human, asset, environment Critical financial loss, Very long-term business interruption/expense, Possibility of fatalities
4	Significant	Significant financial loss, Long-term business interruption/expense, Permanent physical injuries
3	Moderate	Unauthorized modification could result in moderate risk to human, asset, environment Moderate financial loss, Medium-term business interruption/expense, Short-term injury
2	Minor	Minor financial loss, Short-term business interruption/expense, First-aid case injury
1	Negligible	Unauthorized modification could not pose a risk to human, asset, environment Negligible financial loss, Very short-term business interruption/expense

- **Availability index**

Availability is the properties that ensures access to and use of assets or information in a timely manner. Classification is based on the impact of business damage when unable to use of assets or difficult access to information.

< Example of availability index evaluation >



Availability Index	Descriptor	Definition
5	Critical	Unavailability could result in significant risk to human, asset, environment Critical financial loss, Very long-term business interruption/expense, Possibility of fatalities
4	Significant	Significant financial loss, Long-term business interruption/expense, Permanent physical injuries
3	Moderate	Unavailability could result in moderate risk to human, asset, environment Moderate financial loss, Medium-term business interruption/expense, Short-term injury
2	Minor	Minor financial loss, Short-term business interruption/expense, First-aid case injury
1	Negligible	Unavailability could not pose a risk to human, asset, environment Negligible financial loss, Very short-term business interruption/expense

Explanation of terms

- **Shodan :** A search engine that lets the user find specific types of computers (webcams, routers, servers, etc.) connected to the internet using a variety of filters. It is especially focused on SCADA systems and has recently been exploited as a search engine to find vulnerabilities in target systems. The various IT / OT system vulnerabilities used in ships can also be searched through this site. **(URL : https://www.shodan.io)**
- **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.
- **Telnet :** Telnet is a protocol used on the Internet or local area network to provide a bidirectional interactive text-oriented communication facility using a virtual terminal connection. However, because of serious security concerns when using Telnet over an open network such as the Internet, its use for this purpose has waned significantly in favor of SSH.
- **Old version OS(Operation System) Threat :** When it comes to cybersecurity, older versions of OS are a serious threat to a company, because of they do not support security-related patches such as Windows XP. If security patches are not added, the vulnerability in OS could be discovered by attackers. Ships that have been operated on the same system for decades need to be prepared to update their operating systems.
- **ICS** : Industrial control system (ICS) is a general term that encompasses several types of control systems and associated instrumentation used for industrial process control.