KR Maritime Cyber Security

News from KOREAN REGISTER

Vol. 030

October 2020

The world's first CS Ready for very large LPG carrier

The Korean Register has issued the world's first Cyber Security (CS Ready) class notation for Hyundai Heavy Industries' very large liquefied petroleum gas (LPG) carrier.

Hyundai LNG Shipping is the owner of the very large LPG carrier built by HHI which is scheduled for delivery later this month. KR granted the notation after completing document and field inspections, which included Kongsberg Maritime's ship alarm and monitoring system (AMS) and Hyundai Global Service's Integrated Smart ship Solution (ISS), KR said in its statement.

This is the first time the KR cybersecurity notation has been awarded to a very large LPG carrier. The notation is issued to newbuilding ships that have successfully passed 49 inspection items in a total of 12 categories, including risk and asset management, cyber incident response and recovery.

The four companies have been collaborating on joint research and developments for the past eight months while working to apply and verify KR's Cybersecurity Rules for newbuilding ships.

HHI and KSOE have built a cybersecurity network encompassing the main systems, conducting risk assessment and vulnerability diagnosis for cybersecurity threats and KR has carried out and completed cybersecurity inspections across the network.

As part of the comprehensive technological testing, KR conducted its first MITRE ATT&CK based penetration test to verify the safety of the cybersecurity system.

Newbuilding vessels increasingly need cybersecurity notation as the application of digital technologies such as advanced automation and integrated control systems become more common. In addition, the International Maritime Organization (IMO) is expected to strengthen its demands for cybersecurity risk management as of 2021.

Satellite internet may be convenient but it's also easy to intercept

Experimental results of cyber hacking against ship and airplane through the satellites in Black Hat 2020 conference

James Pavur, Oxford University researcher, presented the experimental results of cyber hacking against ship and airplane through the satellites in Black Hat 2020 conference.

Delivering internet connectivity from satellites orbiting the Earth is becoming an increasingly popular idea especially as Elon Musk continues to launch low-orbit satellites to build out his upcoming Starlink network. Satellite internet connections are actually already being used today by workers on remote oil rigs, ships traversing international waters and by airlines in areas where broadband or cellular internet is not available.

James Pavur presented the results of his experiment at Black Hat 2020 where he tried to convince the infosec community that the unsecured nature of satellite broadband communications is worth a second look. Over the course of several years, he was able to successfully intercept the signals of 18 satellites transmitting internet across a 100m square kilometre are from a fixed physical location in the UK. During the course of his experiment, Pavur was able to eavesdrop on all sorts of different communications including navigational information sent to a Chinese airliner over an unencrypted connection, messages relayed from an Egyptian oil tanker that allowed him to decrypt information about the ship and even personally identifiable information about its crew, account reset passwords for the network of a Greek billionaire's yacht and more.

Intercepting satellite internet traffic

Satellite internet traffic is easy to intercept due to the fact that technology does not currently exist to allow parties to validate the integrity of an encrypted satellite connection.

With just a $90 satellite dish and $200 video-broadcasting satellite tuner purchased off-the-shelf, Pavur was able to intercept satellite internet traffic. By using publicly available sources, he identified the orbitable tracks of satellites and pointed his satellite dish in their direction.

In order to record the data being transmitted, Pavur used signal-recording software and tweaked it to focus on internet traffic by using HTTP protocols. The technique he used didn't' require a particularly high level of technical ability and in total, he was able to download over 8TB of information from satellites orbiting above him.

Pavur hopes that his experiment and his presentation at the Black Hat conference this year will bring awareness to the potential lack of security in satellite internet connections.

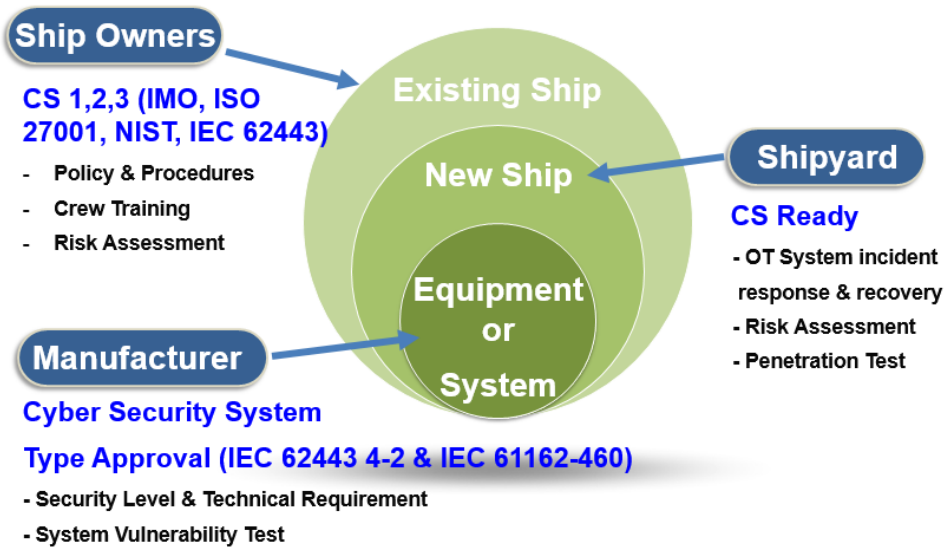
Source : https://www.techradar.com/news/hacking-satellite-internet-connections-is-a-lot-easier-than-youd-think

Understanding of KR CS-Ready Notation

KR Cyber Security Certification System

KR Maritime Cyber Security Certification applies to the company or the ship with cyber security management system (CSMS). When the company/the ship pass the survey for certification(document review and on-site survey), KR issues cyber security compliance certificates to the company/the existing ship, and cyber security notation (CS-Ready) to the new ship. Cyber security compliance for the company/the existing ship is divided to 3 levels (CS1, CS2 and CS3) in accordance with cyber security maturity, and consists of 35 survey areas and 144 survey items.

- **CS1, CS2, CS3** : Requirements of CSMS for the existing ship **(Shipping company)**
- **CS Ready** : Requirements for establishing integrated cyber security system of new ship **(Shipbuilder)**
- **CS Type Approval** : Requirements of cyber security function of equipment system **(Equipment company)**



Need of Cyber Security Notation (CS Ready) for New Ship

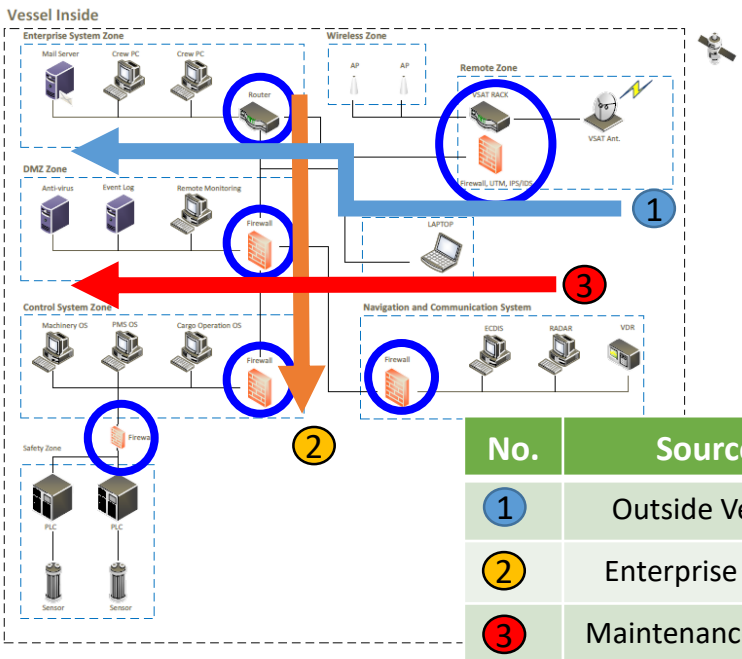
As the marine business environment changes, Advanced automation and integrated control system is equipped in ships, and remote access, control and maintenance of the system in ships became possible from the land, which resulted increase of ship cyber risks. Therefore it is very important for maritime safety that construction and verification of an integrated system preventing and responding cyber incidents from the stage of ship building. KR gives 'CS Ready' notation to the new ship with cyber security system. In this newsletter, the requirements will be introduced.

[CS Ready] Activity : Penetration Test

Penetration tests can be utilized as a way to verify cyber security safety of ship network and system. Penetration test refers to a test in which testers conduct direct penetration to identify vulnerabilities existing in networks and systems and to determine whether they can actually be exploited using the latest hacking techniques. By eliminating potential cyber security vulnerabilities and preparing comprehensive countermeasures through penetration test, cyber security level of ships can be improved. KR will apply MITRE ATT&CK-based penetration test to the actual ship, and the details will be as follows.

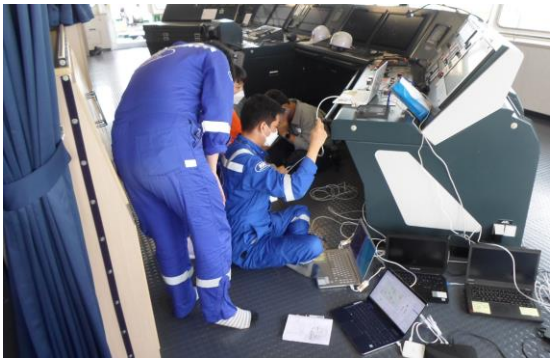
- **Check the performance of security equipment (Firewall, IPS, IDS, etc.) for each zone using penetration test equipment**
- **Enter a test vector* into the tested network to measure the number and ratio of attacks being blocked to determine security capabilities**

*** CVE(Common Vulnerabilities and Exposures) based attacks**



No.	Source	Destination
1	Outside Vessel	Remote Zone
2	Enterprise Zone	Control System Zone
3	Maintenance Zone	DMZ Zone

Penetration Test (ECR)

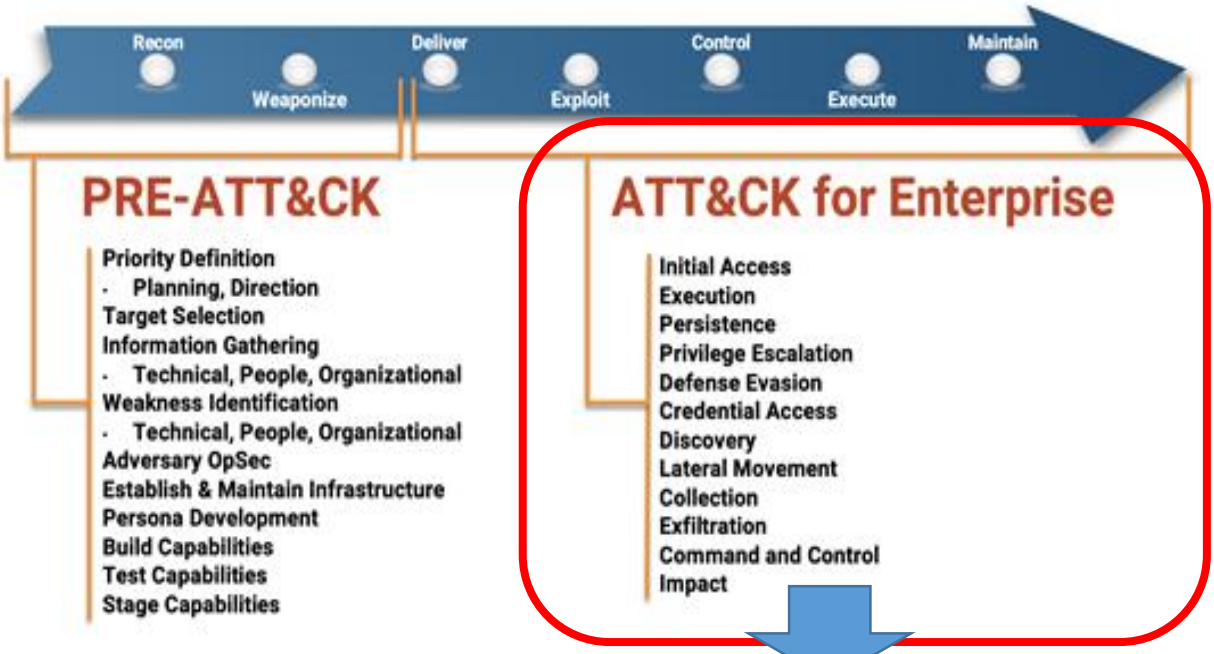


Penetration Test (W/H)

[CS Ready] Activity : MITRE ATT&CK based Penetration Test

MITRE ATT&CK refers to ATT&CK(Adversarial Tactics, Techniques, and Common Knowledge) as a model developed by MITRE in the U.S. and presents attack tactics, infiltration techniques, etc. as a framework through case analysis of post or previous activities of cyber attackers. This test is based on the Cyber Kill-Chain strategy, which identifies and responds to attacks in advance at seven stages, which are classified into PRE-ATT&CK(15 tactics, 148 technics) and Enterprise ATT&CK(12 tactics, 184 technics). Cyber Kill-Chain strategy allows to quickly detect attacks for each stage and block the spread to the next.

- **Tactics describes the attacker's tactical goals.**
- **Technics describes the actions and methods taken by enemies to achieve tactical goals.**
- **Mitigations describes how to respond to a particular technology.**
- **Groups tracks attackers with common names in activity clusters and security communities.**



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Destruction
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Component Object Model and Distributed COM	Clipboard Data	Connection Proxy	Data Encrypted	Data Encrypted for Impact
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Defacement
Replication Through Removable Media	Component Object Model and Distributed COM	AppInit DLLs	Application Shimming	Clear Command History	Credentials from Web Browsers	File and Directory Discovery	Internal Spearphishing	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Content Wipe
Spearphishing Attachment	Control Panel Items	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	Disk Structure Wipe
Spearphishing Link	Dynamic Data Exchange	Authentication Package	DLL Search Order Hijacking	Code Signing	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium	Endpoint Denial of Service
Spearphishing via Service	Execution through API	BITS Jobs	Dylib Hijacking	Compile After Delivery	Exploitation for Credential Access	Network Sniffing	Pass the Ticket	Data Staged	Domain Fronting	Exfiltration Over Physical Medium	Firmware Corruption
Supply Chain Compromise	Execution through Module Load	Bootkit	Elevated Execution with Prompt	Compiled HTML File	Forced Authentication	Password Policy Discovery	Remote Desktop Protocol	Email Collection	Domain Generation Algorithms	Scheduled Transfer	Inhibit System Recovery
Trusted Relationship	Exploitation for Client Execution	Browser Extensions	Emond	Component Firmware	Hooking	Peripheral Device Discovery	Remote File Copy	Input Capture	Fallback Channels		Network Denial of Service
Valid Accounts	Graphical User Interface	Change Default File Association	Exploitation for Privilege Escalation	Component Object Model Hijacking	Input Capture	Permission Groups Discovery	Remote Services	Man in the Browser	Multi-hop Proxy		Resource Hijacking
	InstallUtil	Component Firmware	Extra Window Memory Injection	Connection Proxy	Input Prompt	Process Discovery	Replication Through Removable Media	Screen Capture	Multi-Stage Channels		Runtime Data Manipulation
	Launchctl	Component Object Model Hijacking	File System Permissions Weakness	Control Panel Items	Kerberoasting	Query Registry	Shared Webroot	Video Capture	Multiband Communication		Service Stop
	Local Job Scheduling	Create Account	Hooking	DCShadow	Keychain	Remote System Discovery	SSH Hijacking		Multilayer Encryption		System Shutdown/Reboot
	LSASS Driver	DLL Search Order Hijacking	Image File Execution Options Injection	Deobfuscate/Decode Files or Information	LLMNR/NBT-NS Poisoning and Relay	Security Software Discovery	Taint Shared Content		Port Knocking		Stored Data Manipulation
	Mshta	Dylib Hijacking	Launch Daemon	Disabling Security Tools	Network Sniffing	Software Discovery	Third-party Software		Remote Access Tools		Transmitted Data Manipulation
	PowerShell	Emond	New Service	DLL Search Order Hijacking	Password Filter DLL	System Information Discovery	Windows Admin Shares		Remote File Copy		
	Regsvcs/Regasm	External Remote Services	Parent PID Spoofing	DLL Side-Loading	Private Keys	System Network Configuration Discovery	Windows Remote Management		Standard Application Layer Protocol		
	Regsvr32	File System Permissions Weakness	Path Interception	Execution Guardrails	Securityd Memory				Standard Cryptographic Protocol		
	Rundll32	Hidden Files and Directories	Plist Modification	Exploitation for Defense Evasion	Steal Web Session Cookie				Standard Non-Application Layer Protocol		
	Scheduled Task	Hooking	Port Monitors	Extra Window	Two-Factor Authentication Interception						
	Scripting	Hypervisor									

Source : https://attack.mitre.org/

ENTERPRISE ATT&CK 12 tactics

ENTERPRISE ATT&CK consists of 12 tactics and 184 technics, and the details of 12 tactics are as follows.

ID	Tactics	Descriptions
TA0001	**Initial Access**	▪ Techniques that use various entry vectors to gain their initial foothold within a network Ex) Phishing, supply chain compromise, etc.
TA0002	**Execution**	▪ Techniques that result in adversary-controlled code running on a local or remote system Ex) Malicious scripts, Payload attack using Powershell, etc.
TA0003	**Persistence**	▪ Techniques that adversaries use to keep access to systems across restarts, changed credentials, and other interruptions that could cut off their access Ex) Account Manipulation, BITS Josb, Browser Extensions, etc.
TA0004	**Privilege Escalation**	▪ Techniques that adversaries use to gain higher-level permissions on a system or network Ex) Bypass User Access Control, Abuse Elevation Control Mechanism, etc.
TA0005	**Defense Evasion**	▪ Techniques that adversaries use to avoid detection throughout their compromise EX) Pass the hash, Abuse Elevation Control Mechanism, etc.
TA0006	**Credential Access**	▪ Techniques for stealing credentials like account names and passwords Ex) keylogging, credential dumping, etc.
TA0007	**Discovery**	▪ Techniques an adversary may use to gain knowledge about the system and internal network Ex) finding public IP addresses and open ports, Browser Bookmark Discovery, tec.
TA0008	**Lateral Movement**	▪ Techniques that adversaries use to enter and control remote systems on a network. Following through on their primary objective often requires exploring the network to find their target and subsequently gaining access to it Ex) Window adminshare, Replication Through Removable Media, mimikatz
TA0009	**Collection**	▪ Techniques adversaries may use to gather information and the sources information is collected from that are relevant to following through on the adversary's objectives Ex) Clipboard Data, email, screen capture, Data from Local System, etc.
TA0011	**Command and Control**	▪ Techniques that adversaries may use to communicate with systems under their control within a victim network. Ex) Malicious URL access test known as Ransomware, C&C, etc.
TA0010	**Exfiltration**	▪ Techniques that adversaries may use to steal data from your network Ex) Information leakage test with http, dns, ssh, telnet, etc.
TA0040	**Impact**	▪ Techniques that adversaries use to disrupt availability or compromise integrity by manipulating business and operational processes Ex) Account access removal, data destruction, etc.

Guideline for Type Approval of Maritime Cyber Security

Understanding Guideline for Type Approval of Maritime Cyber Security

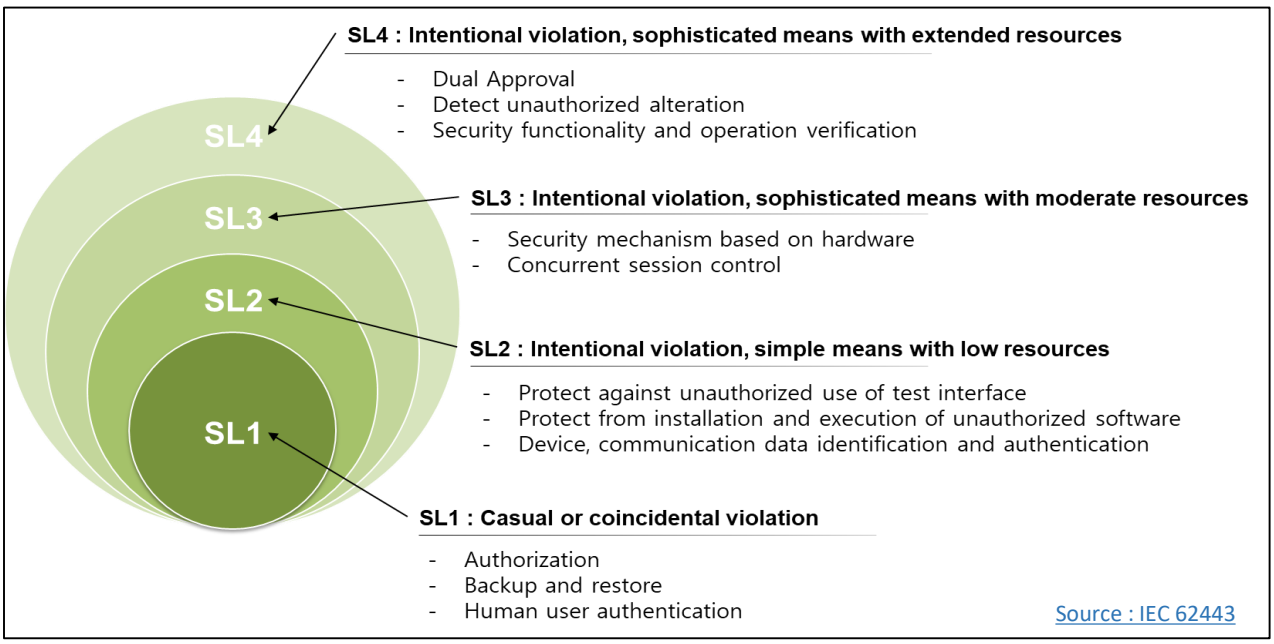
Type approval is to certify for the manufacturers of equipment for marine use that equipment comply with the provisions for the type approved products in the Guidance, where deemed satisfactory by the Society as the results of carrying out the examination, tests and inspection specified in the Guidance before installation on board. The cyber security type approval has been developed based on international standards such as ISA 62443 4-2, IEC 61162-460, and inspect cyber security level and function of cyber systems including remote access equipment, integrated control and monitoring systems on board the ship. The security requirements and their levels are verified on 12 categories and 124 requirements.

< Composition of KR Cyber Security Type Approval Guidelines >

Section 1 General	Section 5 Data Confidentiality	Section 9 Software Application Requirements
Sections 2 Identification and Authentication	Section 6 Restricted Data Flow	Section 10 Embedded Device Requirements
Section 3 Use Control	Section 7 Timely Response to Events	Section 11 Host Device Requirements
Section 4 System Integrity	Section 8 Resource Availability	Section 12 Network Device Requirements

Source : http://www.krs.co.kr/KRRules/KRRules2019/data/data_other/ENGLISH/gc31e000.pdf

Understanding Security Level (SL)



Source : IEC 62443

KR Type Approval of Maritime Cybersecurity Inspection Items

Authenticator management (205)

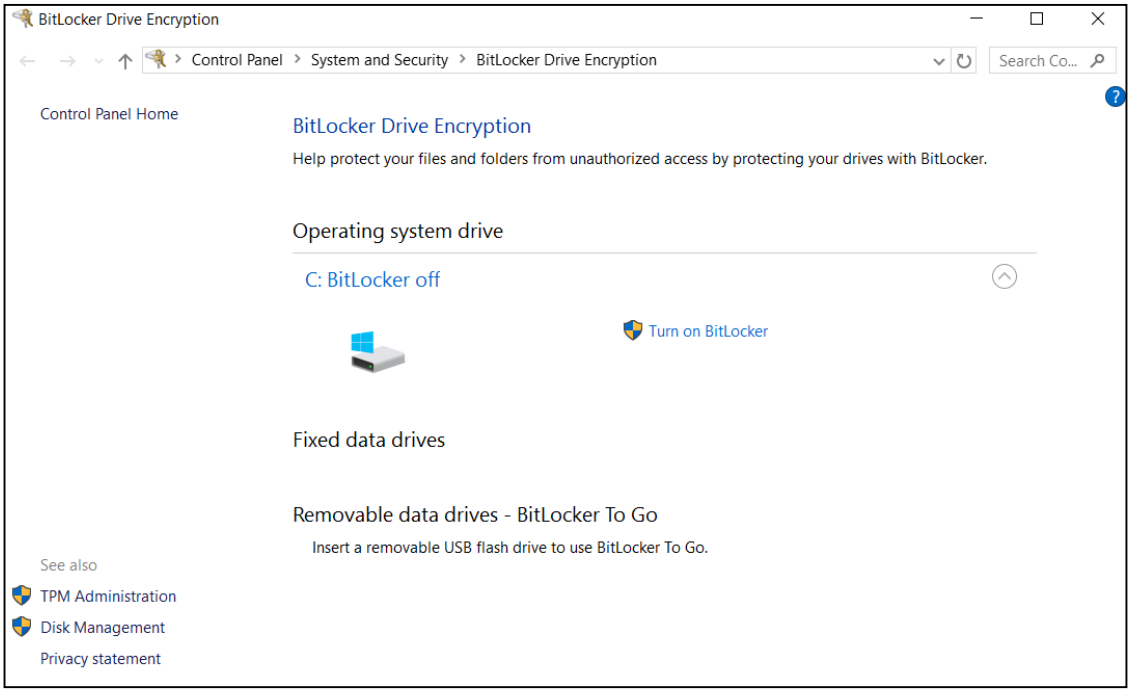
1. Components should provide the capability to:(SL 1,2)
 (1) support the use of initial authenticator content
 (2) support the recognition of changes to default authenticators made at installation time
 (3) function properly with periodic authenticator change/refresh operation
 (4) protect authenticators from unauthorized disclosure and modification when stored, used and transmitted.
2. The authenticators on which the component rely should be protected via hardware mechanisms like OTP memory. (SL 3,4)

Authenticator Requirement

Authenticator is a mean used to confirm the identity of a user. In case that ID and Password are used to log on to web site, password is an authenticator. In addition, tokens, digital signatures, and encrypted authentication keys are examples of authenticator.

<Example of authenticator management function>

The picture above is a menu provided by the router and it can be shown that it provides a password-based authenticator management function. For non-administrator users, reset password function is provided via e-mail in case forgotten. And also password complexity function is provided which force to use numeric characters, special characters, etc. The authenticator should be protected and encryption function can be an example of this. Encryption for the authenticator can not be implemented only by S/W application but also provided by OS.

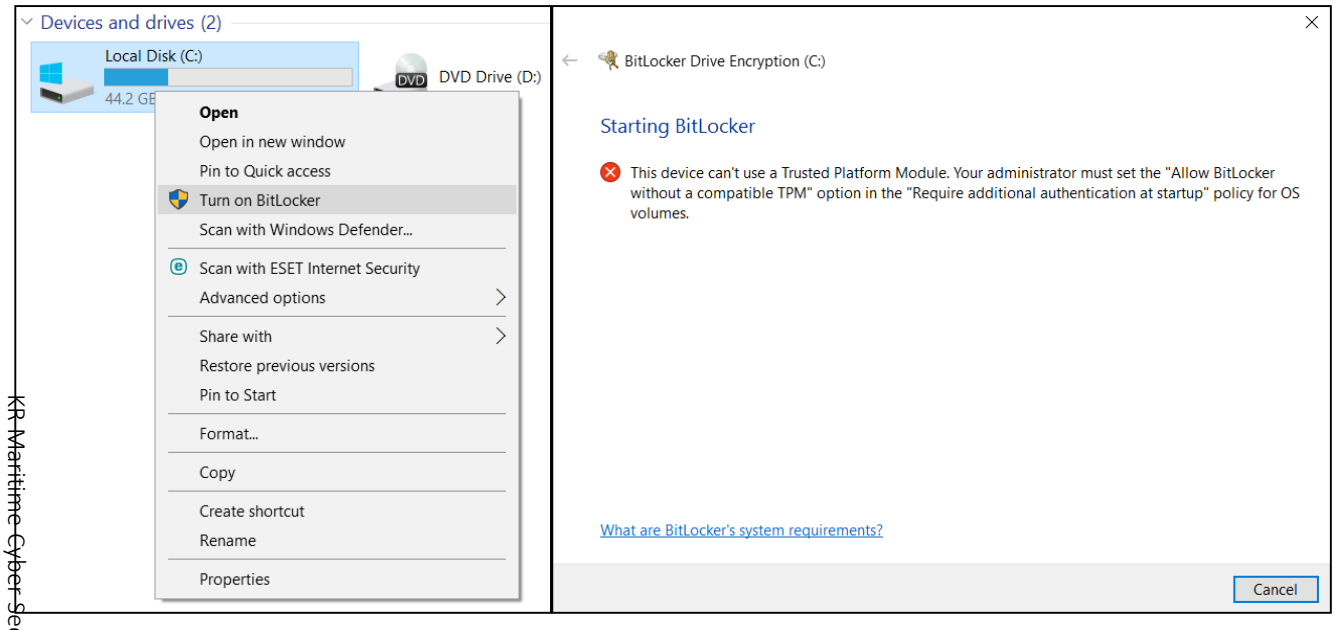


<Example of BitLocker – encryption function provide by Windows OS>

BitLocker, an encryption function provided by Windows OS, is a drive encryption technology that can protect authenticator and Windows OS provides folder/file encryption function also.

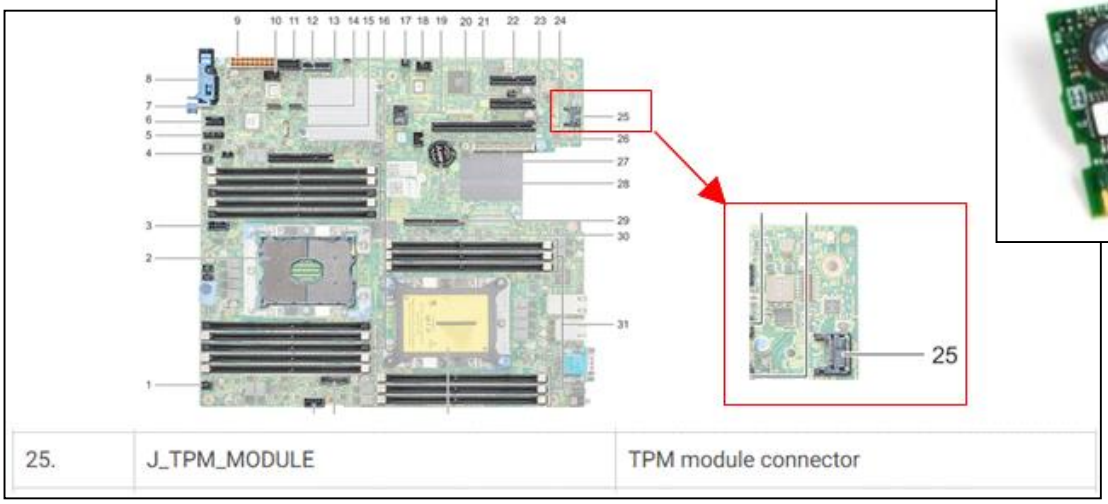
TPM(Trusted Platform Module) – hardware based authenticator protection

In case, TPM is not installed the following message appears during active BitLocker.

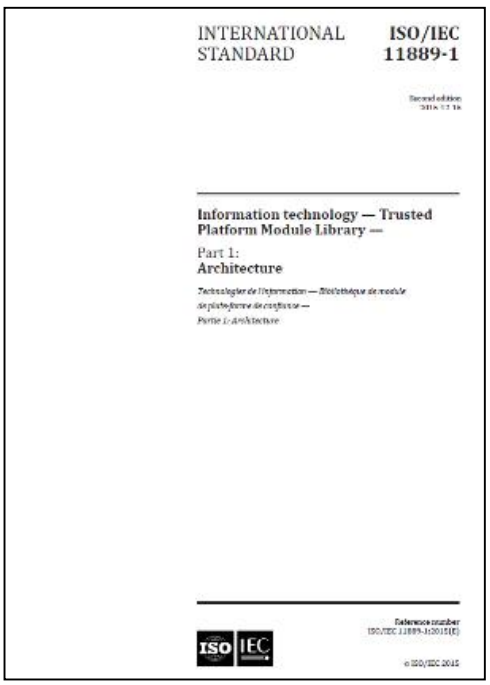


< Example of BitLocker – In case TPM is not installed>

TPM stands for Trusted Platform Module. In conclusion, it is an example of a hardware-based encryption method that performs encryption using a physical chip so that decryption is impossible without this chip. In high-end notebooks manufactured recently, this TPM chip is already installed on the main board and mass-produced in many cases. Some PCs offer the chip as an option. In this case, you can use the TPM function by simply purchasing a separate TPM chip and inserting it into the slot of the main board.



<example of TPM chip>


INTERNATIONAL STANDARD
ISO/IEC 11889-1
Information technology — Trusted Platform Module Library —
Part 1: Architecture

<IEC 11889-1>

The content of TPM has already been established as an international standard, and related S/W is required to utilize the function of TPM. BitLocker provided by Windows OS is an example, and there are other commercial programs. If the TPM chip is installed and encryption is performed through S/W based on it, decryption is impossible without the chip. For example, if a TPM-based encrypted hard disk drive is stolen, the contents of the hard disk alone cannot be decrypted and viewed. For strong security, you can use these hardware-based encryption functions. Finally, whether the TPM function is provided (the TPM chip is installed) can be checked in the specification information of the PC or notebook or in the menu on the operating system.

Understanding of IEC 62443 4-2

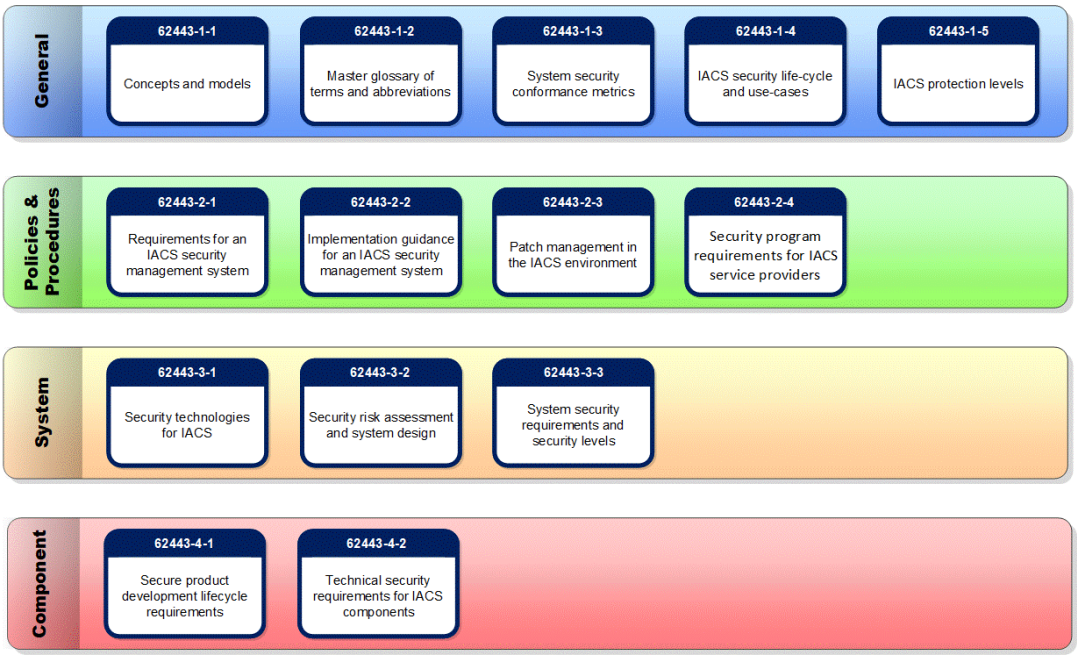
Understanding of IEC 62443

KR adopts/applies ISO 27001, IEC 62443 3-3 & 4-2, IEC 61162-460 for cyber security services. In particular, IEC 62443 4-2 is used as technical requirements for cyber security, with the majority being applied in cyber security type approval services. To promote broader understanding, we would like to contribute to the concept and the requirements of IEC 62443 4-2.

Purpose of IEC 62443

IEC 62443 is a standard for industrial automation and control system security that provides product providers and system integrators with a holistic approach to cyber security to mitigate risks within the industrial network.

< IEC 62443 series >



Source : IEC 62443-4-2

Scope

IEC 62443 targets systems that can affect safe and reliable operations in industrial processes, such as industrial control systems, network-connected support systems, officials and software related to remote operations.

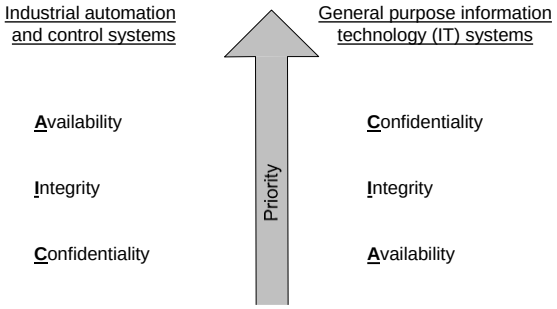
Source : IEC 62443-1-1

Purpose of security

While the requirements of traditional information security are aimed at achieving confidentiality, integrity and availability, security in an industrial automation and control system environment is related to maintaining the availability of all system components. In addition, the integrity of industrial equipment controlled/monitored by industrial automation systems is also important, but confidentiality is not significantly addressed because the exchange data of most industrial automation and control systems are structured in raw data format.

Source : IEC 62443-1-1

<Difference of security purpose between industrial automation & control systems and IT system>



Minimum security requirements of industrial automation and control system

IEC 62443 presents the following basic requirements for industrial automation and control system security.

- Access Control (AC) : Access control to protect against unauthorized access to selected devices or information
- Use Control (UC): Control the unauthorized control of the device or the use of selected equipment or information to prevent the use of information
- Data Integrity (DI): Ensure data integrity for selected communications to protect against unauthorized changes
- Data confidentiality (DC): Ensure data confidentiality for selected communications to protect against eavesdropping
- Data Flow Proposal (RDF) : Restriction of data flow over communications to protect against unauthorized disclosure of information
- Timely Response to Events (TRE): Response of timely events to respond to security breaches through appropriate authorization and reporting of violations, and automated timely remediation in dangerous situations.
- Resource Availability (RA) Service : Ensure availability of all network resources to protect against denial-of-service attacks (DOS) and so on

Explanation of Term

CVE(Common Vulnerabilities and Exposures

Common Vulnerabilities and Exposures (CVE) is a publicly known list of computer security faults. When referring to CVE, it usually refers to the CVE ID number assigned to the security fault. CVE helps IT professionals manage computer systems more securely by working together to prioritize and address these vulnerabilities.

Source : RedHat

Payload

Payload refers to malicious codes that are generated or downloaded additionally after an exploit, an attack technique that uses vulnerabilities in applications, such as operating systems (OS), web browsers, and word programs to change the flow of programs and allow malicious code planted by attackers to run without user's knowledge, occurs and additional actions or damages that occur on the intention of the attacker.

Source : AhnLab

Pass-the-Hash Attack

Pass-the-Hash (PtH) attack is a technique in which an attacker captures a cryptographic hash corresponding to a cryptographic character and then utilizes it to access authentication and other network system. The threat actor does not need to decrypt the hash's password to obtain a plain text password. PtH attacks use authentication protocols because the password hash remains static for all sessions until the password is changed. An attacker typically obtains a hash by scraping the active memory and other skills of the system.

Source : BeyondTrust

Credential dumping

Credential dumping refers to obtaining login information (user name and password) from the system's operating system (OS) and software. And then use these credentials to access restricted information and install other malware.

Source : MITRE ATT&CK, 2020

Introduction of Maritime Cyber Security Training

KR Cyber Security Training

According to IMO Resolution MSC.428(98) Maritime Cyber Risk Management in Safety Management Systems, administrations such as Marshall Islands ask the ship owner and ship managers to appropriately addressed in safety management systems no later than the first annual verification of the company's Document of Compliance after 1 January 2021. Therefore, the demand for maritime cyber security training that can help to understand maritime cyber security and establish proper cyber security management system has increased.

KR is providing cyber security training to domestic and overseas shipping companies, shipbuilders, equipment companies, service providers from 2015. In particular, in March, KR received approval from Singapore MPA for the training course named as the understanding of maritime cyber security and provided cyber security training to shipping companies in Singapore through the Maritime Cluster Fund (MCF).

KR provides maritime cyber security e-learning course in cooperation with Orange Security, a cyber security consulting company, for clients who have difficulty in collective training due to COVID-19. Maritime cyber security e-learning course consist of ‘Understanding of Maritime cyber Security’ and ‘Practice of Maritime Cyber Security.’ While the former was developed for cyber security awareness of all employees and includes overview of maritime cyber security, examples of maritime cyber incident, etc., the latter is for hands-on staff and consists of implementation of cyber risk management, etc. The clients can apply this course through the maritime cyber security e-learning system of Orange Security (https://edu.orangecq.com/).

The samples of these courses can be founded on YouTube: ‘Understanding Maritime Cybersecurity (https://youtu.be/fSIDLMj4gho)' and ‘Management Office of Maritime Cybersecurity (https://youtu.be/67t0ckrNtiA)’