Input paper: [[1]](#footnote-1) ENAV30-5.1.1.5

Input paper for the following Committee(s): check as appropriate Purpose of paper:

**□** ARM **□** ENG **□** PAP **□** Input

X ENAV **□** VTS X Information

Agenda item [[2]](#footnote-2) Cyber security

Technical Domain / Task Number 2 Working Group 1 (Digital Information System)

Author(s) / Submitter(s) Junyeon Kim(Korea Maritime Transportation Safety Authority)

JongIl Chae(GMT)

Introduce of cyber security application case of ship`s e-Nav service display device based on international standards.

# Summary

This document introduces the general application of the cyber security requirements (IEC62443 and IEC 61162-460) according to international standards to the e-Nav service display device of ship.

## Purpose of the document

This document is to inform IALA of the application of the cyber security requirements according to the procedure of document ENAV28-5.1.1.4 to the e-Nav service display device in service by the Korean government.

## Related documents

None.

## Terms and definitions

### **authentication**

### provision of assurance that a claimed characteristic of an identity is correct

### **authenticator**

### means used to confirm the identity of a user (human, software process or device) property of ensuring timely and reliable access to and use of control system information and functionality

### **e-Navigation service display device**

### shipboard device to display information of maritime services(refer to MSC.1/Circ.1610) in the context of e-Navigation, which may be ECDIS, INS or a dedicated display unit.

### **identifier**

### symbol, unique within its security domain, that identifies, indicates or names an entity which makes an assertion or claim of identity

### **integrity**

### property of protecting the accuracy and completeness of assets

### **least privilege**

### basic principle that holds that users (humans, software processes or devices) should be assigned the fewest privileges consistent with their assigned duties and functions

### **non-repudiation**

### ability to prove the occurrence of a claimed event or action and its originating entities

### **security level**

### level corresponding to the required set of countermeasures and inherent security properties of devices and systems for a zone or conduit based on assessment of risk for the zone or conduit (IEC 62443-4-2 / 3.1.37)

### **threat**

### circumstance or event with the potential to adversely affect operations (including mission, functions, image or reputation), assets, control systems or individuals via unauthorized access, destruction, disclosure, modification of data and/or denial of service

# Background

The Cyber Security concepts and solutions have mostly been developed for office IT systems and applications. Cyber security for maritime domain not only comes with different security priorities, it also comes with different management & operational characteristics and requirements

The risk of maritime cyber-attacks in the maritime domain is also increasing globally, the importance of maritime cyber security has emerged in the international community such as International Maritime Organization (IMO), International Association of Classification Societies (IACS), Baltic and International Maritime Council (BIMCO), Oil Companies International Marine Forum (OCIMF).

# Discussion

## Analysis of applicable international standards

Maritime digital devices can be any kind of sensors, device or system equipped with IoT or 5G terminal communication.

It is recommended that the during the development of Cyber ​​security standards applicable to maritime digital devices, the following standards are taken into consideration: IEC 62443-4-2, IEC 61162-460 and IEC 63154. This section provides an overview of these standards.

1. cyber security standards applicable to maritime digital devices

|  |  |  |
| --- | --- | --- |
| Category | Standard | Title |
| **Maritime digital devices** | IEC 62443-4-2 | Technical security requirements for IACS components |
| IEC 61162-460 | Maritime navigation and radiocommunication equipment and systems – digital interfaces Part 460: Ethernet interconnection – safety and security |
| IEC 63154 | Maritime navigation and radiocommunication equipment and systems – Cybersecurity – General requirements, methods of testing and required test results |

### IEC 62443 series overview

The international industrial security standard IEC 62443 is a security framework defined by the International Electrotechnical Commission (IEC). It covers both organisational and technical aspects of security, without being prescriptive regarding the technical solution. In the set of corresponding documents, security requirements are defined, which target the solution operator and the integrator, but also the product vendor.

The primary goal of the IEC 62443 series is to provide a flexible framework that facilitates addressing current and future vulnerabilities in IACS(industrial automation and control system) and applying necessary mitigations in a systematic, defensible manner. It is important to understand that the intention of the IEC 62443 series is to build extensions to enterprise security that adapt the requirements for business IT systems and combines them with the unique requirements for strong integrity and availability needed by IACS.

텍스트, 스크린샷, 실외, 주차장이(가) 표시된 사진

자동 생성된 설명

*Figure 1 IEC 62443 series overview*

#### IEC 62443 3-3 : system security requirements and security level

This standard expands the seven foundational requirements (FRs) defined in IEC 62443 1-1 into a series of system requirements (SRs). Each SR has a baseline requirement and more requirement enhancements (REs) to strengthen security. All seven FRs have a defined set of four SLs.

1. Foundational Requirements (FRs) and Purpose

|  |  |
| --- | --- |
| **FR(Foundational Requirement)** | **Purpose** |
| FR1. Identification and authentication control (IAC) | Identify and authenticate all users (humans, software processes and devices), prior to allowing them access to the system or assets. |
| FR2. User Control (UC) | Enforce the assigned privileges of an authenticated user (human, software process or device) to perform the requested action on the component and monitor the use of these privileges. |
| FR3. System Integrity (SI) | Ensure the integrity of the component to protect against unauthorized manipulation or modification. |
| FR4. Data confidentiality (DC) | Ensure the confidentiality of information on communication channels and in data stored in repositories to protect against unauthorized disclosure. |
| FR5. Restricted data flow (RDF) | Segment the control system via zones and conduits to limit the unnecessary flow of data. |
| FR6. Timely response to events(TRE) | Respond to security violations by notifying the proper authorities, reporting needed evidence of the violation and taking timely corrective action when incidents are discovered. |
| FR7. Resource availability (RA) | Ensure the availability of components against the degradation or denial of essential services. |

1. Security Levels (SLs) definition

|  |  |
| --- | --- |
| Security Level(SL) | Purpose |
| SL 1 | Prevent the unauthorized disclosure of information via eavesdropping or casual exposure |
| SL 2 | Prevent the unauthorized disclosure of information to an entity actively searching for it using simple means with low resources, generic skills and low motivation. |
| SL 3 | Prevent the unauthorized disclosure of information to an entity actively searching for it using sophisticated means with moderate resources, IACS specific skills and moderate motivation. |
| SL 4 | Prevent the unauthorized disclosure of information to an entity actively searching for it using sophisticated means with extended resources, IACS specific skills and high motivation. |

#### IEC 62443-4-2 standard : Technical security requirements for IACS components

This standard provides detailed technical control system component requirements (CRs) associated with the seven foundational requirements (FRs) described in IEC 62443 1‑1 including defining the requirements for control system capability security levels and their components, SL-C(component). Component requirements for four types of components: software application, embedded device, host device and network device. Thus the CRs for each type of component will be designated as follows:

* Software application requirements (SAR); one or more software programs and their dependencies that are used to interface with the process or the control system itself (for example, configuration software and historian)
* Embedded device requirements (EDR) : special purpose device designed to directly monitor or control an industrial process
* PLC (Programmable Logic Controller), IED (Intelligent Electronic Device)
* Host device requirements (HDR) : general purpose device running an operating system (for example Microsoft Windows OS or Linux) capable of hosting one or more software applications, data stores or functions from one or more suppliers
* Operator workstation, Data historian
* Network device requirements (NDR) : device that facilitates data flow between devices, or restricts the flow of data, but may not directly interact with a control process
* Switch, VPN (Virtual Private Network)

### Overview of IEC 61162 standards

IEC 61162 series : Maritime navigation and radiocommunication equipment and systems – digital interfaces

1. IEC 61162 series overview

|  |  |
| --- | --- |
| Part | Title |
| IEC 61162-1(NMEA 0183) | Part 1: Single talker and multiple listener |
| IEC 61162-2(NMEA 0183) | Part 2: Single talker and multiple listener, high speed transmission |
| IEC 61162-3(NMEA 2000) | Part 3: Serial data instrument network |
| IEC 61162-450 | Part 450: Ethernet interconnection |
| IEC 61162-460 | Part 460: Ethernet interconnection – safety and security |

#### IEC 61162-460 : Ethernet interconnection – safety and security

This standard is an add-on to the IEC 61162-450 standard where higher safety and security standard are needed due to higher exposure to external threats or to improve network integrity. This standard provides requirements and test method for equipment to be used in an IEC 61162-460 compliant network as well as requirements for the network itself and requirements for interconnection from the network to other networks.

*Figure 2 Functional overview of IEC 61162-460 requirement applications*

1. IEC 61162-460 component definition

|  |  |
| --- | --- |
| Name | [Definition](http://www.3gpp.org/ftp/Specs/html-info/21-series.htm) |
| 460-Network | Network which consists of only 460-Nodes, 460-Switches, 460 Forwarder, 460-Gateway and 460- Wireless gateway as well as 450-Nodes |
| 460-Node | Device complaint with the requirements of a 450-Node and which satisfies the safety and security requirements as specified in this standard |
| 460-Switch | Network infrastructure device used to interconnect nodes on a 460-Network and which satisfies the safety and security requirements as specified in this standard |
| 460-Forwarder | Network infrastructure device that can safely exchange data stream between a 460- Network and other controlled networks including other 460-Networks |
| 460-Gateway | Network infra structure device that connects 460-Netowrk and uncontrolled networks and which satisfies the safety and security requirements as specified in this standard |
| 460-Wireless gateway | Network infrastructure device that connects a 460-Netowrk and wireless networks and which satisfies the safety and security requirements as specified in this standard |

### Overview of IEC 63154 standard : Maritime Navigation and Radiocommunication equipment and systems – cyber security – General requirements, methods of testing and required test results

#### Scope

This document specifies requirements, methods of testing and required test results for shipborne navigation and radiocommunication equipment where standards are needed to provide a basic level of protection against cyber incidents:

* shipborne radio equipment forming part of the global maritime distress and safety system (GMDSS) mentioned in the International Convention for Safety of Life at Sea(SOLAS) as amended, and by the Torremolinos International Convention for the Safety of Fishing Vessels as amended and to other shipborne radio equipment, where appropriate;
* shipborne navigational equipment mentioned in the International Convention for Safety of Life at Sea (SOLAS) as amended, and by the Torremolinos International Convention for the Safety of Fishing Vessels as amended,
* other shipborne navigational aids, and Aids to Navigation (AtoN), where appropriate.

1. IEC 63154 overview

|  |  |
| --- | --- |
| Part | Title |
| Module A | Data files |
| Module B | Execution of executables |
| Module C | User authentication |
| Module D | System defense |
| Module E | Network access |
| Module F | Access to operating system |
| Module G | Booting environment |
| Module H | Maintenance mode |
| Module I | Protection against unintentional crash caused by user input |
| Module J | Interfaces for removable devices including USB |
| Module K | IEC 61162-1 or IEC 61162-2 as interface |
| Module L | IEC 61162-450 as interface |
| Module M | IEC other interfaces |
| Module N | Software maintenance |
| Module O | Remote maintenance |
| Annex A | [Guidance on implementing virus and malware protection ontype approved equipment for IMO SOLAS regime and practical limitations](#_bookmark86) |
| Annex B | File authentication |
| Annex C | [Methods of authentication of data files and executables – some](#_bookmark93) examples |
| Annex D | USB class codes |
| Annex E | Cyber security configuration document for equipment |
| Annex F | Guidance on interconnection between networks |

## Cyber Risk Assessment

### Scope of the assessment

The scope of the assessment work confines e-Navigation service display devices, which may be ECDIS, INS or dedicated device for this purpose.

We assumed that e-Navigation service display device subject to the cyber risk assessment has the below general specification and functions referring to the information obtained by searching for products regarding ECDIS and INS on sale in the market.

**[General specifications]**

* Power Supply : 230 VAC, 50/60Hz
* Display Unit : 26 in LCD display
* Main Control Unit
* OS : Windows 10
* Interfaces
* Multiple Ethernet LAN ports (1GB)
* Multiple serial ports (IEC 61162-1 & IEC 61162-2)
* Multiple USB ports
* CD/DVD-ROM : optional
* Keyboard, trackball mouse

**[General functions]**

* Display of e-Navigation service information.
* Electronic chart display
* Display of AIS vessels

### Identification of cyber threats

The below examples are not exhaustive. Threats may be intentional, accidental or environmental (natural) and may result, for example, in damage or loss of essential services. Other cyber attack methods are evolving such as impersonating a legitimate shore-based employee in a shipping company to obtain valuable information, which can be used for a further attack. The potential number and sophistication of tools and techniques used in cyber attacks continue to evolve and are limited only by the ingenuity of those organizations and individuals developing them.

1. Identified threats list

| No. | Threat | Description |
| --- | --- | --- |
| 1 | Malware | Malware is any software intentionally designed to cause damage to a computer, server, client, or computer network. By contrast, software that causes unintentional harm due to some deficiency is typically described as a software bug. A wide variety of malware types exist, including computer viruses, worms, Trojanhorses, ransomware, spyware, adware, rogue software, wiper and scareware. |
| 2 | Brute force. | An attack trying many passwords with the hope of eventually guessing correctly. The attacker systematically checks all possible passwords until the correct one is found. |
| 3 | Denial of Service (DOS) | a cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet. Denial of service is typically accomplished by flooding the targeted machine or resource with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled. |
| 4 | Social engineering. | A non-technical technique used by potential cyber attackers to manipulate insider individuals into breaking security procedures, normally, but not exclusively, through interaction via social media. |
| 5 | Data breach | A data breach is a security violation in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an individual unauthorized to do so. |
| 6 | Phishing. | Sending emails to a large number of potential targets asking for particular pieces of sensitive or confidential information. The email may also contain a malicious attachment or request that a person visits a fake website using a hyperlink included in the email. |
| 7 | Scanning | Searching large portions of the internet at random for vulnerabilities that could be  exploited. |
| 8 | Network manipulation and information gathering | Illegal collection of information through unauthorized access to the network |
| 9 | Man-in-the-middle attack | a cyberattack where the attacker secretly relays and possibly alters the communications between two parties who believe that they are directly communicating with each other. One example of a MITM attack is active eavesdropping, in which the attacker makes independent connections with the victims and relays messages between them to make them believe they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker. The attacker must be able to intercept all relevant messages passing between the two victims and inject new ones. |
| 11 | Erroneous use or erroneous administration of devices | During system maintenance(e.g., software update), the introduction of malicious code, system malfunction, setting mistake, integrity test not conducted, etc. |
| 12 | Careless use of removable media or device (USB, Laptop, etc) | Careless use of removable media (USB, portable drives, laptops, etc) |
| 13 | OS vulnerabilities | Security vulnerabilities that can be caused by failure to patch operating system(Windows, Linux, Android, etc). |
| 14 | Application software vulnerabilities | Security vulnerabilities that can be caused by software bugs or failure to patch software |
| 15 | Hardware failure | Hardware failure caused by failure of hardware devices such as CPU, memory, and interfaces |
| 16 | Credential stuffing. | Using previously compromised credentials or specific commonly used passwords to attempt unauthorized access to a system or application. |
| 17 | Subverting the supply chain | Attacking a company or ship by compromising equipment, software or supporting services being delivered to the company or ship. |

## Application case for security requirements for E-Navigation display devices based on IEC 62443-4-2

### Equipment specification of application case

**[Specifications]**

* Power Supply : 230 VAC, 50/60Hz
* Display Unit : 10.1 in LCD display
* Main Control Unit
* OS : Android 9.0
* Interfaces
* Ethernet LAN ports (100MB)
* Serial ports (IEC 61162-1 & IEC 61162-2)
* Wireless communication unit
* LTE-M transceiver
* POE(Power over ethernet) adapter
* GPS antenna
* LTE-M antenna

**[Functions]**

* Display of e-Navigation service information.
* Electronic chart display
* Display of AIS vessels

### Composition of application case

텍스트이(가) 표시된 사진

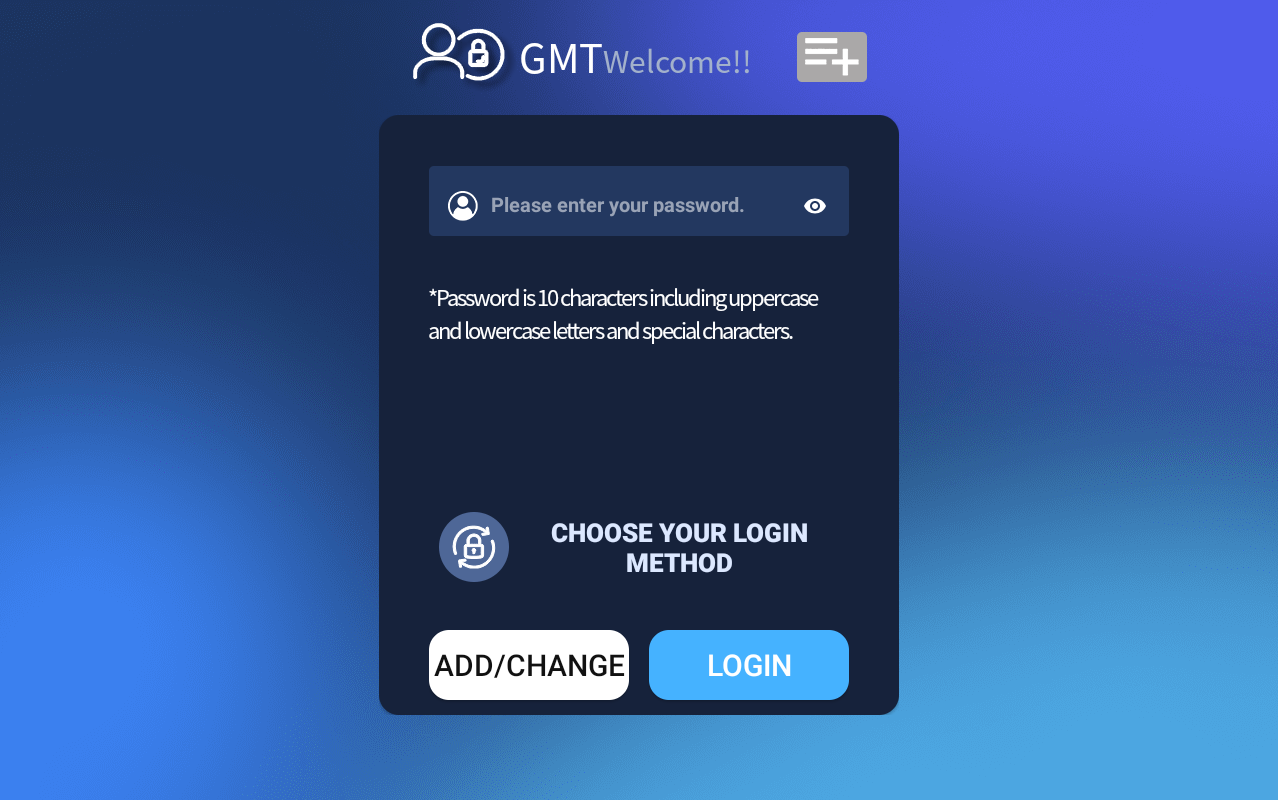
자동 생성된 설명*Figure 3 Composition of e-Nav service display*

### Case of application of security requirements

#### User identification (ID) and authentication (certificate and password)

1. Unique identifier(ID) and authentication

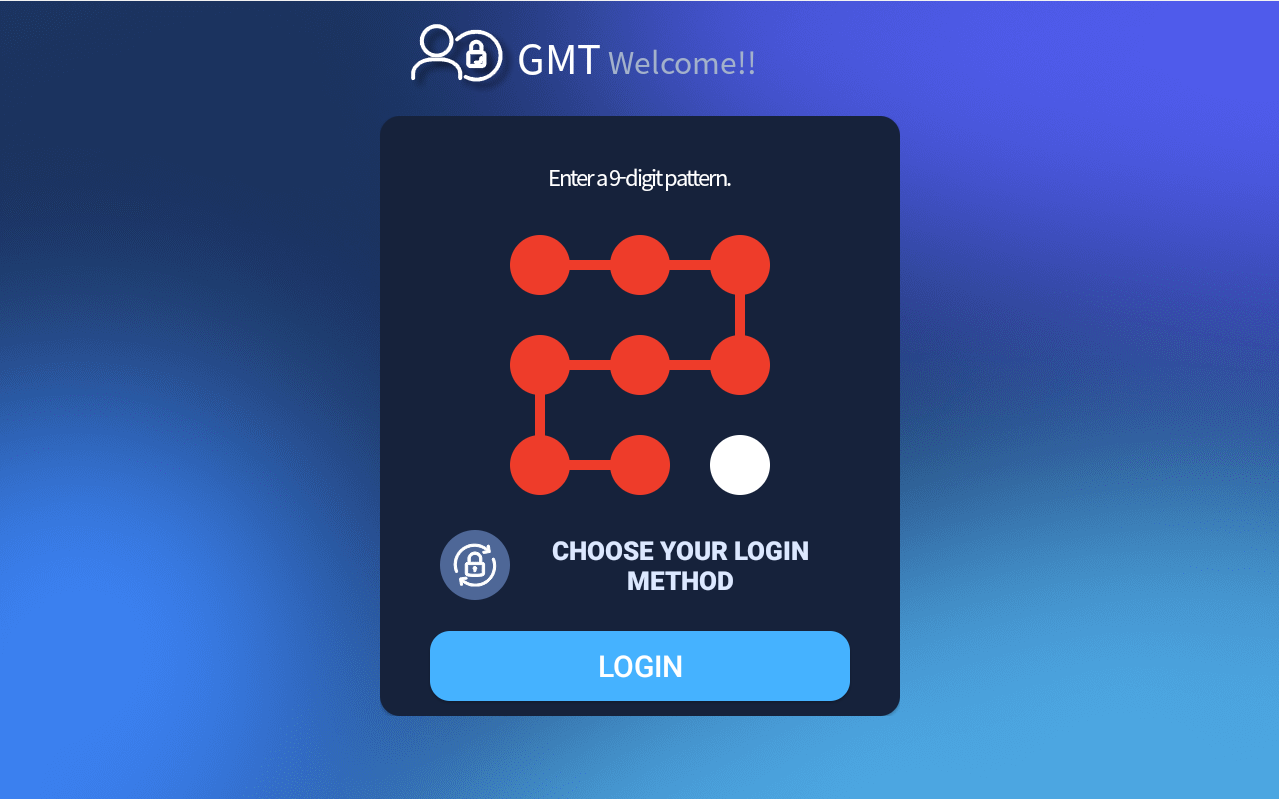
ID and password are issued for each user for unique identifier and authentication.

1. Multi-factor authentication

For the multi-factor authentication, authentication functions through patterns and pin numbers other than password authentication for each user are implemented.

텍스트, 하늘, 전자기기, 계산기이(가) 표시된 사진

자동 생성된 설명 

1. The use of an appropriate PKI considering commonly accepted best practice where PKI is utilized

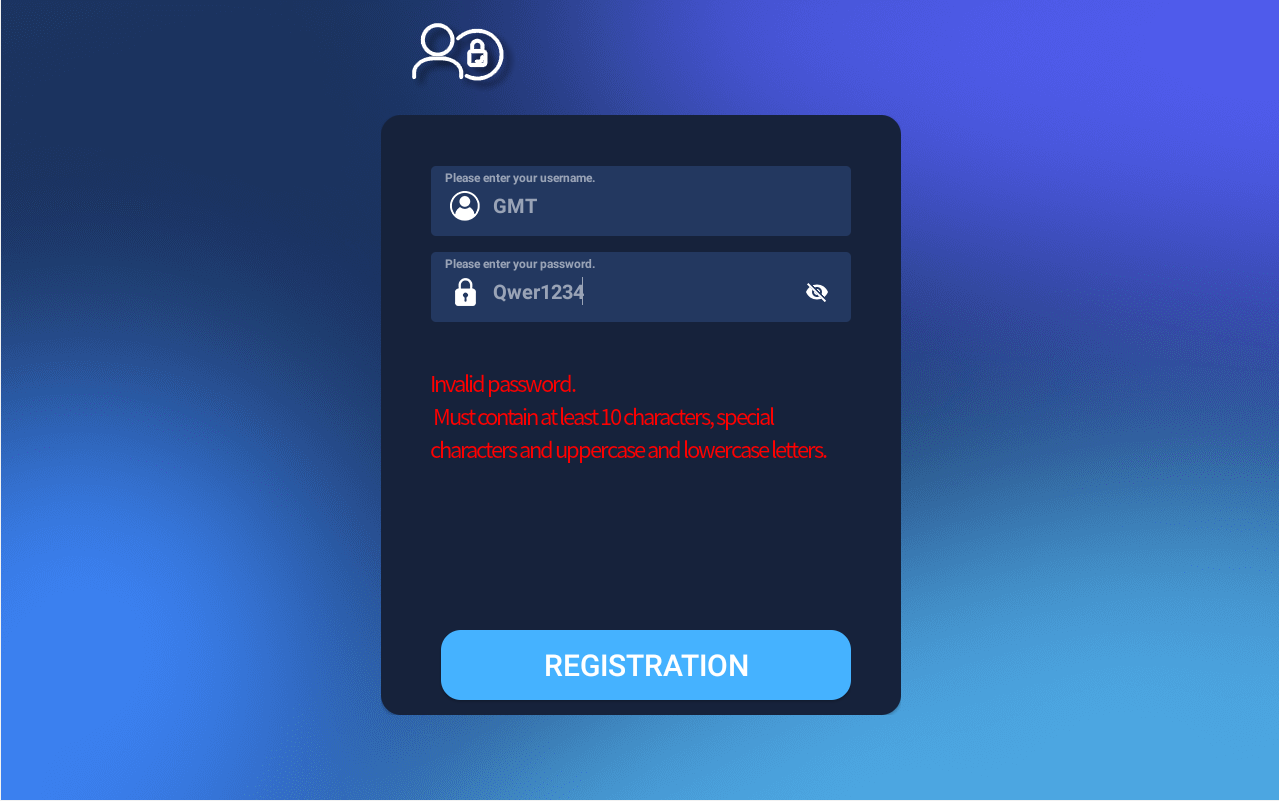
The e-Nav service display device needs a certificate to receive a service, and transmits request information based on the certificate information when requesting information from the e-Nav service platform. The e-Nav service platform transmits data only in normal cases by checking the validity of the information based on certificate and the unique number of the e-Nav service display device.

텍스트이(가) 표시된 사진

자동 생성된 설명

1. Authenticator management (password strength and life limit, etc.)

When creating passwords, strong password conditions such as length, special characters, and capitalization restrictions are applied, and the validity period of passwords is managed to ensure password security.

 텍스트, 스크린샷, 모니터, 화면이(가) 표시된 사진

자동 생성된 설명

#### Auditable log record

Auditable log record is saved for review history of set value changes and important data changes.

테이블이(가) 표시된 사진

자동 생성된 설명

#### Ensure service data integrity and confidentiality

1. Provide communication integrity mechanism

To provide communication integrity, when communicating with the e-Nav service platform, hash value according to the message content is generated and transmitted for each message. The e-Nav service platform provides information to the e-Nav service display device only for messages that have not been tampered with by comparing the message content with the hash value.

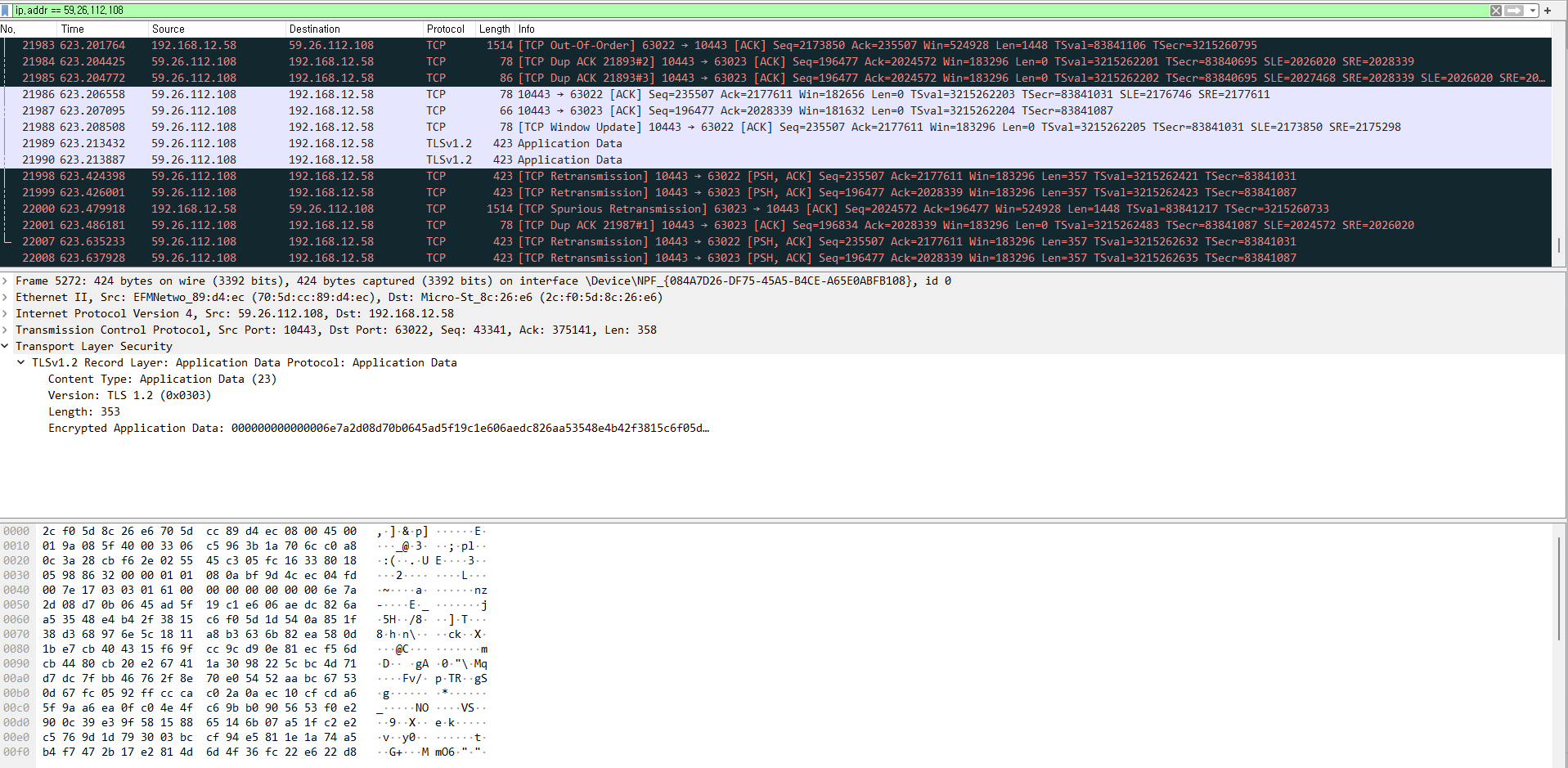
텍스트이(가) 표시된 사진

자동 생성된 설명

1. Service data encryption

The service guarantees data confidentiality by sending and receiving TLS-based encryption/ decryption data.

텍스트이(가) 표시된 사진

자동 생성된 설명 

#### System recovery function

1. Important data backup

The e-Nav service display device backs up important data periodically or according to user actions to prevent loss of it.

텍스트, 스크린샷, 모니터, 화면이(가) 표시된 사진

자동 생성된 설명

1. System initialization function

Users can select backed up data automatically or manually to restore the data.

텍스트이(가) 표시된 사진

자동 생성된 설명

#### Updates to the device

It checks whether the latest version of S/W from the e-Nav centre, and if there is a latest distributed version, the e-Nav service display device automatically downloads and updates the software.



#### Restriction on the use of removable media

To restrict the use of removable media, inserting a USB will deny access to the USB and display a message stating that it cannot be used.

텍스트, 모니터, 실내, 선반이(가) 표시된 사진

자동 생성된 설명

# Action requested of the Committee

None.

1. Input document number, to be assigned by the Committee Secretary [↑](#footnote-ref-1)
2. Leave open if uncertain [↑](#footnote-ref-2)