Guidance for Type Approval of Maritime Cyber Security

(Development Review : For internal opinion inquiry)

2021. 01.

Machinery Rule Development Team

Effective Date : 1 July 2021

(The contract date for ship construction)

Present	Amendment	Remark
CHAPTER 2 TYPE APPROVAL OF CYBER SECURITY **Section 1 General** **101. General** Cyber-physical systems to be applicable in this Guidance are categorized as follows. (1) - (2) 〈same as the present Rules〉 (3) Forwarder : Network devices, software application and host devices (4) Gateway : Network devices, software application and host devices **Section 2 〈same as the present Rules〉**	**CHAPTER 2 TYPE APPROVAL OF CYBER SECURITY** **Section 1 General** **101. General** Cyber-physical systems to be applicable in this Guidance are categorized as follows. (1) - (2) 〈same as the present Rules〉 (3) Forwarder : Network devices~~, software application and host devices~~ *(2021)* (4) Gateway : Network devices~~, software application and host devices~~ *(2021)* **Section 2 〈same as the present Rules〉**	(Amended) - In accordance with the terminology definition of IEC 61162-460, classifications for software applications and host equipment of (3) and (4) have been deleted.

Present	Amendment	Remark
# CHAPTER 3 REQUIREMENTS FOR CYBER SECURITY ## Section 1 General **101. 〈same as the present Rules〉** ## Section 2 Identification and authentication **201. Human user identification and authentication** 1. Components should provide the capability to identify and authenticate all human users according to ISA 62443-4-2 CR 1.1 on all interfaces capable of human user access. 2. User identification and authentication should not hamper fast, local emergency actions. 3. Components should provide the capability to employ multifactor authentication for all human user access to the component. 4. Components should provide the capability to uniquely identify and authenticate all human users. 5. Requirements for SLs (1) SL 1 : **201. 2** (2) SL 2 : **201. 3** (3) SL 3 : **201. 4** (4) SL 4 : **201. 4**	# CHAPTER 3 REQUIREMENTS FOR CYBER SECURITY ## Section 1 General **101. 〈same as the present Rules〉** ## Section 2 Identification and authentication **201. Human user identification and authentication *(2021)*** 1. Components should provide the capability to identify and authenticate all human users according to ~~ISA 62443-4-2 CR 1.1~~ ISA 62443-3-3 SR 1.1 on all interfaces capable of human user access. ~~2.~~ However, User identification and authentication should not hamper fast, local emergency actions. ~~3.~~2. ~~Components should provide the capability to employ multifactor authentication for all human user access to the component.~~ Components should provide the capability to uniquely identify and authenticate all human users. ~~4.~~3. ~~Components should provide the capability to uniquely identify and authenticate all human users.~~ Components should provide the capability to employ multifactor authentication for all human user access to the component. ~~5.~~4. Requirements for SLs (1) SL 1 : **201. ~~2~~1** (2) SL 2 : **201. ~~3~~2** (3) SL 3 : **201. ~~4~~3** (4) SL 4 : **201. ~~4~~3**	(Amended) - Amended according to the original text of IEC 62443 4-2.

Present	Amendment	Remark
202. Software process and device identification and authentication	**202. Software process and device identification and authentication**	
1. Components should provide the capability to identify itself and authenticate to any other component (software application, embedded devices, host devices and network devices), according to ISA-62443-4-2 CR 1.2.	1. Components should provide the capability to identify itself and authenticate to any other component (software application, embedded devices, host devices and network devices), according to ~~ISA-62443-4-2 CR 1.2.~~ ISA-62443-3-3 SR 1.2. *(2021)*	(Amended) - Amended according to the original text of IEC 62443 4-2.
2. - 3. 〈same as the present Rules〉	2. - 3. 〈same as the present Rules〉	
203. Account management	**203. Account management**	(Amended) - Amended according to the original text of IEC 62443 4-2.
1. Components should provide the capability to support the management of all accounts directly or integrated into a system that manages accounts according to ISA 62443-4-2 CR 1.3.	1. Components should provide the capability to support the management of all accounts directly or integrated into a system that manages accounts according to ~~ISA 62443-4-2 CR 1.3~~ ISA 62443-3-3 SR 1.3. *(2021)*	
2. 〈same as the present Rules〉	2. 〈same as the present Rules〉	
204. Identifier management	**204. Identifier management**	(Amended) - Amended according to the original text of IEC 62443 4-2.
1. Components should provide the capability to integrate into a system that supports the management of identifiers and/or provide the capability to support the management of identifiers directly according to ISA 62443-4-2 CR 1.4.	1. Components should provide the capability to integrate into a system that supports the management of identifiers and/or provide the capability to support the management of identifiers directly according to ~~ISA 62443-4-2 CR 1.4.~~ ISA 62443-3-3 SR 1.4. *(2021)*	
2. 〈same as the present Rules〉	2. 〈same as the present Rules〉	
205. - 206. 〈same as the present Rules〉	**205. - 206. 〈same as the present Rules〉**	

Present	Amendment	Remark
207. Public key infrastructure certificates 1. When public key infrastructure (PKI) is utilized, the component should provide or integrate into a system that provides the capability to interact and operate in accordance with ISA 62443-4-2 CR 1.8. 2. 〈same as the present Rules〉	**207. Public key infrastructure certificates** 1. When public key infrastructure (PKI) is utilized, the component should provide or integrate into a system that provides the capability to interact and operate in accordance with ~~ISA 62443-4-2 CR 1.8~~ ISA 62443-3-3 SR 1.8. *(2021)* 2. 〈same as the present Rules〉	(Amended) - Amended according to the original text of IEC 62443 4-2.
208. - 212. 〈same as the present Rules〉	**208. - 212. 〈same as the present Rules〉**	
Section 3 〈same as the present Rules〉	**Section 3 〈same as the present Rules〉**	
Section 4 System Integrity	**Section 4 System Integrity**	
401. 〈same as the present Rules〉	**401. 〈same as the present Rules〉**	
402. Security functionality verification 1. Components should provide the capability to support verification of the intended operation of security functions according to ISA 62443-4-2 CR 3.3. 2. - 3. 〈same as the present Rules〉	**402. Security functionality verification** 1. Components should provide the capability to support verification of the intended operation of security functions according to ~~ISA 62443-4-2 CR 3.3~~ ISA 62443-3-3 SR 3.3. ***(2021)*** 2. - 3. 〈same as the present Rules〉	(Amended) - Amended according to the original text of IEC 62443 4-2.

Present	Amendment	Remark
Section 5 Data Confidentiality	**Section 5 Data Confidentiality**	
501. Communication integrity	**501. Communication integrity**	(Amended) - Amended according to the original text of IEC 62443 4-2.
1. Components should provide the capability to protect the confidentiality of information at rest for which explicit read authorization is supported and support the protection of the confidentiality of information in transit as defined in ISA 62443-4-2 CR 4.1.	1. Components should provide the capability to protect the confidentiality of information at rest for which explicit read authorization is supported and support the protection of the confidentiality of information in transit as defined in ~~ISA 62443-4-2 CR 4.1~~ ISA 62443-3-3 SR 4.1. *(2021)*	
2. 〈same as the present Rules〉	2. 〈same as the present Rules〉	
502. - 503 〈same as the present Rules〉	**502. - 503 〈same as the present Rules〉**	
Section 6 - Section 12 〈same as the present Rules〉	**Section 6 - Section 12 〈same as the present Rules〉**	