Tasneef
هيئة الإمارات للتصنيف
Emirates Classification Society

Guide for the Certification of Cybersecurity Capabilities of Marine Materials and Equipment

Effective from 1 January 2021

INDEX

1 AIM AND PURPOSE

The aim of this guide is to provide indications and evaluation criteria for the certification of cybersecurity capabilities of marine materials and equipment.

The purpose is to address safety aspects related to cyber issues potentially affecting such materials and equipment according to the principles and criteria of the IMO Standards and/or other international standards such as ISA/IEC 62443.

2 SCOPE OF APPLICABILITY

This guide applies to all marine materials and equipment used to control or monitor physical processes that can be vulnerable to cyber incidents and, if compromised, could lead to dangerous situations for human safety, safety of the vessel and/or threat to the environment.

3 FUNCTIONALITY AND PERFORMANCE OF MARINE MATERIALS AND EQUIPMENT

Marine materials and equipment should demonstrate functionality and performance according to the checklists provided in Annex 1.

4 STATEMENT OF COMPLIANCE

In order to obtain a Statement of Compliance to this guide, the materials or equipment should fulfil the requirements listed in Annex 1.

Compliance shall be assessed by means of:
- test sessions to be carried out on such materials or equipment, witnessed by the Society
- examination of documentation.

The Statement of Compliance – issued using the format in Annex 2 - has validity of 5 years. If the Manufacturer intends to modify the product, Tasneef is to be informed of all the contemplated modifications. If such alterations are such as to affect the conformance of the product with the criteria required in accordance with this guide, a new certification procedure will be considered by Tasneef for the modified product.

If the modifications do not affect those aspects which are ruled by the Standards applied for the certification, an approval extension may be granted by Tasneef as a supplement to the original statement of compliance, if applicable.

Annex 1 - Checklists for the verification of compliance to the "Guide for the certification of Cybersecurity capabilities of Marine materials and equipment"

Introduction

The aim of these checklists is to provide a means for the verification of compliance to the "Guide for the certification of cybersecurity capabilities of marine materials and equipment" (see par. 3 and 4 therein).

The checklists are based on the ISA/IEC 62443 series of standards and to some extent reflect their structure and organization.

Numbering of items is intended to be consistent with ISA/IEC 62443 for easy reference.

Description of checklists

Checklist #1 – Establishing a Cyber Security Management System (CSMS): This check list is based on the ISA/IEC 62443-2-1 standard, "Industrial communication networks –Network and system security – Part 2-1: Establishing an industrial automation and control system security program". This part of IEC 62443 defines the elements necessary to establish a cyber security management system (CSMS) for industrial automation and control systems. The elements of a CSMS described in ISA/IEC 62443-2-1 and, consequently, the items in this check list, are mostly policy, procedure, practice and personnel related, describing what shall or should be included in the final CSMS for the organization.

Checklist #2 – System Security Requirements: This check list is based on the ISA/IEC 62443-3-3 standard, "Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels". This part of the IEC 62443 series provides detailed technical control system requirements (SRs) associated with the seven foundational requirements (FRs) described in IEC 62443‑1‑1[1] including defining the requirements for control system capability security levels, SL-C (control system).

Checklist #3 – Secure product development lifecycle requirements: This check list is based on the ISA/IEC 62443-4-1 standard, "Security for industrial automation and control systems – Part 4-1: Secure product development lifecycle requirements". This part of IEC 62443 specifies process requirements for the secure development of products used in industrial automation and control systems. It defines a secure development lifecycle (SDL) for the purpose of developing and maintaining secure products. This lifecycle includes security requirements definition, secure design, secure implementation (including coding guidelines), verification and validation, defect management, patch management and product end-of-life. These requirements can be applied to new or existing processes for developing, maintaining and retiring hardware, software or firmware for new or existing products. These requirements apply to the developer and maintainer of the product, but not to the integrator or user of the product.

Checklist #4 – Technical security requirements for OT components: This check list is based on the ISA/IEC 62443-4-2 standard, "Security for industrial automation and control systems – Part 4-2: Technical security requirements for Industrial Automation and Control Systems components". This part of IEC 62443 provides detailed technical control system component requirements (CRs) associated with the seven foundational requirements (FRs) described in IEC TS 62443-1-1[2] including defining the requirements for control system capability security levels and their components, SL-C (component).

[1] As defined in IEC TS 62443-1-1 the seven foundational requirements (FRs) are:
a) identification and authentication control (IAC),
b) use control (UC),
c) system integrity (SI),
d) data confidentiality (DC),
e) restricted data flow (RDF),
f) timely response to events (TRE), and
g) resource availability (RA).
These seven FRs are the foundation for defining control system security capability levels.

[2] See Note 1

Annex 1 - Checklists for the verification of compliance to the "Guide for the certification of Cybersecurity capabilities of Marine materials and equipment"

Checklist #1 – Establishing a Cyber Security Management System (CSMS)

Numbering of items is intended to be consistent with ISA/IEC 62443-2-1 for easy reference.

Item	Requirement	Result	Notes
4.2	**Category: Risk analysis**		
4.2.2	**Element: Business rationale**		
4.2.2.1	The organization should develop a high-level business rationale as a basis for its effort to manage OT systems cyber security, which addresses the unique dependence of the organization on OT systems.		
4.2.3	**Element: Risk identification, classification, and assessment Objective:**		
4.2.3.1	The organization shall select a particular risk assessment and analysis approach and methodology that identifies and prioritizes risks based upon security threats, vulnerabilities and consequences related to its OT systems assets.		
4.2.3.2	The organization should provide participants in the risk assessment activity with appropriate information including methodology training, before beginning to identify the risks.		
4.2.3.3	A high-level system risk assessment shall be performed to understand the financial and HSE consequences in the event that availability, integrity or confidentiality of the OT systems is compromised.		
4.2.3.4	The organization shall identify the various OT systems, gather data about the devices to characterize the nature of the security risk, and group the devices into logical systems.		
4.2.3.5	The organization shall develop simple network diagrams for each of the logically integrated systems showing the major devices, network types, and general locations of the equipment.		
4.2.3.6	The organization shall develop the criteria and assign a priority rating for mitigating the risk of each logical control system.		
4.2.3.7	The organization shall perform a detailed vulnerability assessment of its individual logical OT systems, which may be scoped based on the high-level risk assessment results and prioritization of OT systems subject to these risks.		
4.2.3.8	The organization's risk assessment methodology shall include methods for prioritizing detailed vulnerabilities identified in the detailed vulnerability assessment.		
4.2.3.9	The organization shall conduct a detailed risk assessment incorporating the vulnerabilities identified in the detailed vulnerability assessment.		
4.2.3.10	The organization shall identify the risk and vulnerability reassessment frequency as well as any reassessment triggering criteria based on technology, organization, or industrial operation changes.		
4.2.3.11	The results of physical, HSE and cyber security risk assessments shall be integrated to understand the assets' overall risk.		
4.2.3.12	Risk assessments shall be conducted through all stages of the technology lifecycle including development, implementation, changes, and retirement.		
4.2.3.13	The risk assessment methodology and the results of the risk assessment shall be documented.		

Annex 1 - Checklists for the verification of compliance to the "Guide for the certification of Cybersecurity capabilities of Marine materials and equipment"

Item	Requirement	Result	Notes
4.2.3.14	Up-to-date vulnerability assessment records should be maintained for all assets comprising the OT systems.		
4.3	**Category: Addressing risk with the CSMS**		
4.3.2.2	**Element: CSMS scope**		
4.3.2.2.1	The organization shall develop a formal written scope for the cyber security program.		
4.3.2.2.2	The scope should explain the strategic goals, process, and timing for the CSMS.		
4.3.2.3	**Element: Organizing for security**		
4.3.2.3.1	The organization shall obtain senior management support for a cyber security program.		
4.3.2.3.2	There shall be an organization, structure or network of stakeholders established (or chosen) under management leadership, with the responsibility to provide clear direction and oversight for the cyber aspects of the OT systems		
4.3.2.3.3	Organizational responsibilities shall be clearly defined for cyber security and related physical security activities.		
4.3.2.3.4	The core team of stakeholders should be cross- functional in nature to bring together the skills necessary to address security in all parts of the OT systems.		
4.3.2.4	**Element: Staff training and security awareness**		
4.3.2.4.1	The organization shall design and implement a cyber security training program.		
4.3.2.4.2	All personnel (including employees, contract employees, and third-party contractors) shall be trained initially and periodically thereafter in the correct security procedures and the correct use of information processing facilities.		
4.3.2.4.3	All personnel that perform risk management, OT systems engineering, system administration/maintenance and other tasks that impact the CSMS should be trained on the security objectives and industrial operations for these tasks.		
4.3.2.4.4	The training program should be validated on an on- going basis to ensure that personnel understand the security program and that they are receiving the proper training.		
4.3.2.4.5	The cyber security training program shall be revised, as necessary, to account for new or changing threats and vulnerabilities.		
4.3.2.4.6	Records of employee training and schedules for training updates should be maintained and reviewed on a regular basis.		
4.3.2.5	**Element: Business continuity plan**		
4.3.2.5.1	Prior to creating a business continuity plan, the organization shall specify recovery objectives for the systems involved based on business needs.		
4.3.2.5.2	The organization should determine the impact to each system due to a significant disruption and the consequences associated with loss of one or more of the systems.		

Annex 1 - Checklists for the verification of compliance to the "Guide for the certification of Cybersecurity capabilities of Marine materials and equipment"

Item	Requirement	Result	Notes
4.3.2.5.3	Continuity plans shall be developed and implemented to ensure that business processes can be restored in accordance with recovery objectives.		
4.3.2.5.4	A business continuity team should be formed including OT systems and other process owners. In the event of a significant disruption, this team should determine the priority of critical business and OT systems to re-establish operations.		
4.3.2.5.5	The business continuity plan shall define and communicate the specific roles and responsibilities for each part of the plan.		
4.3.2.5.6	The organization shall create backup and restore procedures (see 4.3.4.3.9) that support the business continuity plan.		
4.3.2.5.7	The business continuity plan shall be tested on a regular basis and updated as necessary.		
4.3.2.6	**Element: Security policies and procedures**		
4.3.2.6.1	The organization shall develop high-level cyber security policies for the OT systems environment which are approved by management.		
4.3.2.6.2	The organization shall develop and approve cyber security procedures, based on the cyber security policies, and provide guidance in how to meet the policies.		
4.3.2.6.3	Cyber security policies and procedures that deal with OT systems risks should be consistent with or extensions of policies created by other risk management systems.		
4.3.2.6.4	Cyber security policies and procedures for the OT systems environment shall include compliance requirements.		
4.3.2.6.5	The organization shall determine and document its risk tolerance as a basis for creation of policy and risk management activities.		
4.3.2.6.6	Cyber security policies and procedures for the OT systems environment shall be communicated to all appropriate personnel.		
4.3.2.6.7	The cyber security policies and procedures shall be reviewed regularly, validated to confirm that they are up-to-date and being followed, and updated as required to ensure that they remain appropriate.		
4.3.2.6.8	Senior leadership shall demonstrate commitment to cyber security by endorsing the cyber security policies.		
4.3.3.2	**Element: Personnel security**		
4.3.3.2.1	There shall be a personnel security policy established, clearly stating the organization's commitment to security and the security responsibilities of personnel. (Personnel include employees, prospective employees, contract employees, and third-party contractors.)		
4.3.3.2.2	Unless government regulation prohibits it, all personnel with access to the OT systems (both physical and cyber), including new hires and internal transfers to sensitive positions, shall be screened, including validation of their identity and background checks, during the job application process.		
4.3.3.2.3	Personnel should also be subject to ongoing scrutiny for changes that might indicate a conflict of interest or concern for performing the job in an appropriate manner.		

Annex 1 - Checklists for the verification of compliance to the "Guide for the certification of Cybersecurity capabilities of Marine materials and equipment"

Item	Requirement	Result	Notes
4.3.3.2.4	The personnel security policy should address security responsibilities from recruitment through the end of employment, especially for sensitive positions.		
4.3.3.2.5	Security expectations and responsibilities shall be clearly documented and regularly communicated to personnel.		
4.3.3.2.6	Terms and conditions of employment shall clearly state an employee's responsibility for cyber security. These responsibilities shall extend for a reasonable period of time after employment ceases.		
4.3.3.2.7	Duties should be segregated among personnel to maintain appropriate checks and balances, so that no single individual has total control over actions that change the functional operation of the OT systems.		
4.3.3.3	**Element: Physical and environmental security**		
4.3.3.3.1	Security policies and procedures shall be established that address both physical and cyber security in the protection of assets.		
4.3.3.3.2	One or more physical security perimeters shall be established to provide barriers to unauthorized access to protected assets.		
4.3.3.3.3	Appropriate entry controls shall be provided at each barrier or boundary.		
4.3.3.3.4	Assets shall be protected against environmental damage from threats such as fire, water, smoke, dust, radiation, corrosion, and impact.		
4.3.3.3.5	Employees shall be required to follow and enforce the physical security procedures that have been established.		
4.3.3.3.6	All connections under the control of the organization shall be adequately protected from tampering or damage.		
4.3.3.3.7	All equipment assets, including auxiliary environmental equipment, shall be properly maintained to ensure proper operation.		
4.3.3.3.8	Procedures shall be established for monitoring and alarming when physical or environmental security is compromised.		
4.3.3.3.9	Procedures should be established and audited with respect to the addition, removal, and disposal of all assets.		
4.3.3.3.10	Procedures shall be established to ensure the protection of critical components during the interruption of operations, for example, due to fire, water ingress, security breach, interruption, or natural or any other type of disaster.		
4.3.3.4	**Element: Network segmentation**		
4.3.3.4.1	A network segmentation countermeasure strategy employing security zones shall be developed for OT systems devices based upon the risk level of the OT systems.		
4.3.3.4.2	High-risk OT systems shall be isolated from or employ a barrier device to separate it from other zones with different security levels or risks.		
4.3.3.4.3	Barrier devices shall block all non-essential communications in and out of the security zone containing critical control equipment.		

Item	Requirement	Result	Notes
4.3.3.5	**Element: Access control: Account administration**		
4.3.3.5.1	Access privileges for access account shall be established in accordance with the organization's security policy (see 4.3.3.7.1)		
4.3.3.5.2	As for all cyber security controls, the choice of access accounts for individuals versus access accounts for a crew shall be determined by considering threats, risks, and vulnerabilities. In this case, considerations include HSE risks of individual controls, mitigation using complementary physical security controls, requirement for accountability, and administrative/operational need.		
4.3.3.5.3	Access shall be granted, changed, or terminated on the authority of an appropriate manager.		
4.3.3.5.4	A record shall be maintained of all access accounts, including details of the individual(s) and devices authorized to use the account, their permissions, and the authorizing manager.		
4.3.3.5.5	Access accounts shall be suspended or removed as soon as they are no longer needed (for example, job change).		
4.3.3.5.6	All established access accounts shall be reviewed regularly to ensure that the individual(s) and devices have only the minimum required permissions.		
4.3.3.5.7	Default passwords for access accounts shall be changed before the OT systems is put into service.		
4.3.3.5.8	Periodic reviews of compliance to the account administration policy should be performed.		
4.3.3.6	**Element: Access control: Authentication**		
4.3.3.6.1	Companies shall have an authentication strategy or approach that defines the method(s) of authentication to be used.		
4.3.3.6.2	All users shall be authenticated before using the requested application, unless there are compensating combinations of entrance control technologies and administrative practices.		
4.3.3.6.3	Strong authentication practices (such as requiring strong passwords) shall be used on all system administrator and application configuration access accounts.		
4.3.3.6.4	Log files should record all access attempts to critical systems and should be reviewed for successful and failed access attempts.		
4.3.3.6.5	The organization shall employ an authentication scheme with an appropriate level of strength to positively identify a remote interactive user.		
4.3.3.6.6	The organization shall develop a policy addressing remote login by a user and/or remote connections (for example, task-to-task connections) to the control system which defines appropriate system responses to failed login attempts and periods of inactivity.		
4.3.3.6.7	After some number of failed login attempts by a remote user, the system should disable the access account for a certain amount of time.		
4.3.3.6.8	After a defined period of inactivity, a remote user should be required to re-authenticate before he or she can re-access the system.		
4.3.3.6.9	Systems should employ appropriate authentication schemes for task-to-task communication between applications and devices.		

Annex 1 - Checklists for the verification of compliance to the "Guide for the certification of Cybersecurity capabilities of Marine materials and equipment"

Item	Requirement	Result	Notes
4.3.3.7	**Element: Access control: Authorization**		
4.3.3.7.1	Rules that define the privileges authorized under access accounts for personnel in various job roles shall be defined in an authorization security policy that is clearly documented and applied to all personnel upon authentication.		
4.3.3.7.2	The permission to access OT systems devices shall be logical (rules that grant or deny access to known users based on their roles), physical (locks, cameras, and other controls that restrict access to an active computer console), or both.		
4.3.3.7.3	Access accounts should be role based to manage access to appropriate information or systems for that user's role. Safety implications shall be considered when defining roles.		
4.3.4.2	**Element: Risk management and implementation**		
4.3.4.2.1	The organization shall adopt a risk management framework that includes selection and implementation of OT systems devices and countermeasures to manage risk to an acceptable level over the life of the facility.		
4.3.4.2.2	A common defined set of countermeasures (technical and administrative) to address both physical and cyber security risks should be defined and applied across the organization wherever a specific risk is identified.		
4.3.4.3	**Element: System development and maintenance**		
4.3.4.3.1	The security functions and capabilities of each new component of the OT systems shall be defined up front, developed or achieved via procurement, and tested together with other components so that the entire system meets the desired security profile.		
4.3.4.3.2	A change management system for the OT systems environment shall be developed and implemented. The change management process shall follow separation of duty principles to avoid conflicts of interest.		
4.3.4.3.3	Using clearly defined criteria, proposed changes to the OT systems shall be reviewed for their potential impact to HSE risks and cyber security risks by individuals technically knowledgeable about the industrial operation and the OT systems system.		
4.3.4.3.4	The security requirements of a new system being installed in the OT systems environment in an existing zone shall meet the security policies and procedures required for that zone/environment. Similarly, maintenance upgrades or changes shall meet the security requirements for the zone.		
4.3.4.3.5	Cyber security change management procedures should be integrated with existing PSM procedures.		
4.3.4.3.6	The operations and change management policies and procedures shall be reviewed and kept current to ensure that security changes do not increase risks to safety or business continuity.		
4.3.4.3.7	A procedure for patch management shall be established, documented, and followed.		
4.3.4.3.8	A procedure for antivirus/malware management shall be established, documented, and followed.		

Annex 1 - Checklists for the verification of compliance to the "Guide for the certification of Cybersecurity capabilities of Marine materials and equipment"

Item	Requirement	Result	Notes
4.3.4.3.9	A procedure for backing up and restoring computer systems and protecting backup copies shall be established, used, and verified by appropriate testing.		
4.3.4.4	**Element: Information and document management**		
4.3.4.4.1	A lifecycle document management process shall be developed and maintained for OT systems information.		
4.3.4.4.2	Information classification levels (for example, company confidential, restricted, or public) shall be defined for access and control, including sharing, copying, transmitting, and distributing appropriate for the level of protection required.		
4.3.4.4.3	All logical assets within the scope of the CSMS (that is, control system design information, vulnerability assessments, network diagrams, and industrial operations programs) shall be classified to indicate the protection required commensurate with the consequences of unauthorized disclosure or modification.		
4.3.4.4.4	Policies and procedures should be developed detailing retention, physical and integrity protection, destruction, and disposal of all assets based on their classifications, including written and electronic records, equipment and other media containing information, with consideration for legal or regulatory requirements.		
4.3.4.4.5	Appropriate measures should be employed to ensure long-term records can be retrieved (that is, converting the data to a newer format or retaining older equipment that can read the data).		
4.3.4.4.6	Information that requires special control or handling should be reviewed on a periodic basis to validate that special handling is still required.		
4.3.4.4.7	Periodic reviews of compliance to the information and document management policy should be performed.		
4.3.4.5	**Element: Incident planning and response**		
4.3.4.5.1	The organization shall implement an incident response plan that identifies responsible personnel and defines actions to be performed by designated individuals.		
4.3.4.5.2	The incident response plan shall be communicated to all appropriate organizations.		
4.3.4.5.3	The organization should establish a reporting procedure to communicate unusual activities and events that may actually be cyber security incidents.		
4.3.4.5.4	Employees should be educated on their responsibility to report cyber security incidents and the methods of reporting these incidents.		
4.3.4.5.5	The organization should report cyber security incidents in a timely manner.		
4.3.4.5.6	If an incident is identified, the organization shall promptly respond in accordance with the established procedures.		
4.3.4.5.7	The organization should have procedures in place to identify failed and successful cyber security breaches.		
4.3.4.5.8	The details of an identified incident shall be documented to record the incident, the response, the lessons learned, and any actions taken to modify the CSMS in light of this incident.		

Annex 1 - Checklists for the verification of compliance to the “Guide for the certification of Cybersecurity capabilities of Marine materials and equipment”

Item	Requirement	Result	Notes
4.3.4.5.9	The documented details of an incident shall be communicated to all appropriate organizations (that is, management, IT, process safety, automation and control engineering, security and manufacturing) in a timely manner.		
4.3.4.5.10	The organization shall have a business methodology in place to address issues discovered and ensure they are corrected.		
4.3.4.5.11	Drills should be conducted to test the incident response program on a routine basis.		
4.4	**Category: Monitoring and improving the CSMS**		
4.4.2	**Element: Conformance**		
4.4.2.1	The audit program shall specify the methodology of the audit process.		
4.4.2.2	Validate that the OT systems conform to the CSMS. The CSMS shall include periodic audits of the OT systems to validate that the security policies and procedures are performing as intended and meet the security objectives for the zone.		
4.4.2.3	The organization should define performance indicators and success criteria to monitor conformance to the CSMS. The results from each periodic audit should be expressed in the form of performance against these metrics to display security performance and security trends.		
4.4.2.4	A list of documents and reports required to establish an audit trail shall be developed.		
4.4.2.5	The organization shall state what non-conformance with the CSMS means, and any related punitive measures shall also be defined.		
4.4.2.6	The required competency for auditing the specific systems that are in scope should be specified. The level of independence required should be determined as part of the governance.		
4.4.3	**Element: Review, improve, and maintain the CSMS**		
4.4.3.1	An organization shall be assigned to manage and coordinate the refinement and implementation of the CSMS changes and use a defined method in making and implementing changes.		
4.4.3.2	The managing organization shall periodically evaluate the overall CSMS to ensure the security objectives are being met.		
4.4.3.3	The organization should establish a list of triggers with set thresholds, which would result in a review of related elements of the CSMS and perhaps a change. These triggers include at a minimum: occurrence of serious security incidents, legal and regulatory changes, changes in risk, and major changes to the OT systems. The thresholds should be based on the organization’s risk tolerance.		
4.4.3.4	The organization shall identify and implement appropriate corrective and preventive actions that modify the CSMS to meet security objectives.		
4.4.3.5	A review of the organization’s tolerance for risk should be initiated when there are major changes to the organization, technology, business objectives, internal business, and external events, including identified threats and changes in social climate.		
4.4.3.6	Management system owners should monitor the industry for CSMS best practices for risk assessment and risk mitigation and evaluate their applicability.		
4.4.3.7	The organization shall identify applicable and changing legislation relevant to cyber security.		

Annex 1 - Checklists for the verification of compliance to the "Guide for the certification of Cybersecurity capabilities of Marine materials and equipment"

Item	Requirement	Result	Notes
4.4.3.8	Employee feedback on security suggestions should be actively sought and reported back to senior management as appropriate on performance shortcomings and opportunities.		

Annex 1 - Checklists for the verification of compliance to the “Guide for the certification of Cybersecurity capabilities of Marine materials and equipment”

Checklist #2 – System Security Requirements

Numbering of items is intended to be consistent with ISA/IEC 62443-3-3 for easy reference.

Item	Requirement	Result	Notes
5	**FR 1 – Identification and authentication control** **Purpose and SL-C(IAC) descriptions** Identify and authenticate all users (humans, software processes and devices) before allowing them to access to the control system. **SL 1 –** Identify and authenticate all users (humans, software processes and devices) by mechanisms which protect against casual or coincidental access by unauthenticated entities. **SL 2 –** Identify and authenticate all users (humans, software processes and devices) by mechanisms which protect against intentional unauthenticated access by entities using simple means with low resources, generic skills and low motivation. **SL 3 –** Identify and authenticate all users (humans, software processes and devices) by mechanisms which protect against intentional unauthenticated access by entities using sophisticated means with moderate resources, OT systems specific skills and moderate motivation. **SL 4 –** Identify and authenticate all users (humans, software processes and devices) by mechanisms which protect against intentional unauthenticated access by entities using sophisticated means with extended resources, OT systems specific skills and high motivation.		
5.3	**SR 1.1 – Human user identification and authentication**		
5.3.1	**Requirement**		
	The control system shall provide the capability to identify and authenticate all human users. This capability shall enforce such identification and authentication on all interfaces which provide		
5.3.3	**Requirement enhancements**		
(1)	Unique identification and authentication The control system shall provide the capability to uniquely identify and authenticate all human users.		
(2)	Multifactor authentication for untrusted networks The control system shall provide the capability to employ multifactor authentication for human user access to the control system via an untrusted network (see 5.15, SR 1.13 – Access via untrusted networks).		
(3)	Multifactor authentication for all networks The control system shall provide the capability to employ multifactor authentication for all human user access to the control system.		
5.3.4	**Security levels**		
	The requirements for the four SL levels that relate to SR 1.1 – Human user identification and authentication are:		
SL-C-1	SR 1.1		
SL-C-2	SR 1.1 (1)		
SL-C-3	SR 1.1 (1) (2)		
SL-C-4	SR 1.1 (1) (2) (3)		

Item	Requirement	Result	Notes
5.4	**SR 1.2 – Software process and device identification and authentication**		
5.4.1	**Requirement**		
	The control system shall provide the capability to identify and authenticate all software processes and devices. This capability shall enforce such identification and authentication on all interfaces which provide access to the control system to support least privilege in accordance with applicable security policies and procedures.		
5.4.3	**Requirement enhancements**		
(1)	Unique identification and authentication The control system shall provide the capability to uniquely identify and authenticate all software processes and devices.		
5.4.4	**Security levels**		
	The requirements for the four SL levels that relate to SR 1.2 – Software process and device identification and authentication are:		
SL-C-1	Not Selected		
SL-C-2	SR 1.2		
SL-C-3	SR 1.2 (1)		
SL-C-4	SR 1.2 (1)		
5.5	**SR 1.3 – Account management**		
5.5.1	**Requirement**		
	The control system shall provide the capability to support the management of all accounts by authorized users, including adding, activating, modifying, disabling and removing accounts.		
5.5.3	**Requirement enhancements**		
(1)	Unified account management		
	The control system shall provide the capability to support unified account management.		
5.5.4	**Security levels**		
	The requirements for the four SL levels that relate to SR 1.3 – Account management are:		
SL-C-1	SR 1.3		
SL-C-2	SR 1.3		
SL-C-3	SR 1.3 (1)		
SL-C-4	SR 1.3 (1)		
5.6	**SR 1.4 – Identifier management**		
5.6.1	**Requirement**		
	The control system shall provide the capability to support the management of identifiers by user, group, role or control system interface.		
5.6.3	**Requirement enhancements**		
	None		

Item	Requirement	Result	Notes
5.6.4	**Security levels**		
	The requirements for the four SL levels that relate to SR 1.4 – Identifier management are:		
SL-C-1	SR 1.4		
SL-C-2	SR 1.4		
SL-C-3	SR 1.4		
SL-C-4	SR 1.4		
5.7	**SR 1.5 – Authenticator management**		
5.7.1	**Requirement**		
	The control system shall provide the capability to: a) initialize authenticator content; b) change all default authenticators upon control system installation; c) change/refresh all authenticators; and d) protect all authenticators from unauthorized disclosure and modification when stored and transmitted.		
5.7.3	**Requirement enhancements**		
(1)	Hardware security for software process identity credentials For software process and device users, the control system shall provide the capability to protect the relevant authenticators via hardware mechanisms.		
5.7.4	**Security levels**		
	The requirements for the four SL levels that relate to SR 1.5 – Authenticator management are:		
SL-C-1	SR 1.5		
SL-C-2	SR 1.5		
SL-C-3	SR 1.5 (1)		
SL-C-4	SR 1.5 (1)		
5.8	**SR 1.6 – Wireless access management**		
5.8.1	**Requirement**		
	The control system shall provide the capability to identify and authenticate all users (humans, software processes or devices) engaged in wireless communication.		
5.8.3	**Requirement enhancements**		
(1)	Unique identification and authentication The control system shall provide the capability to uniquely identify and authenticate all users (humans, software processes or devices) engaged in wireless communication.		
5.8.4	**Security levels**		
	The requirements for the four SL levels that relate to SR 1.6 – Wireless access management are:		
SL-C-1	SR 1.6		
SL-C-2	SR 1.6 (1)		
SL-C-3	SR 1.6 (1)		
SL-C-4	SR 1.6 (1)		

Annex 1 - Checklists for the verification of compliance to the "Guide for the certification of Cybersecurity capabilities of Marine materials and equipment"

Item	Requirement	Result	Notes
5.9	**SR 1.7 – Strength of password-based authentication**		
5.9.1	**Requirement**		
	For control systems utilizing password-based authentication, the control system shall provide the capability to enforce configurable password strength based on minimum length and variety of character types.		
5.9.3	**Requirement enhancements**		
(1)	Password generation and lifetime restrictions for human users The control system shall provide the capability to prevent any given human user account from reusing a password for a configurable number of generations. In addition, the control system shall provide the capability to enforce password minimum and maximum lifetime restrictions for human users. These capabilities shall conform with commonly accepted security industry practices. NOTE The control system should provide the capability to prompt the user to change his password upon a configurable time prior to expiration.		
(2)	Password lifetime restrictions for all users The control system shall provide the capability to enforce password minimum and maximum lifetime restrictions for all users.		
5.9.4	**Security levels**		
	The requirements for the four SL levels that relate to SR 1.7 – Strength of password-based authentication are:		
SL-C-1	SR 1.7		
SL-C-2	SR 1.7		
SL-C-3	SR 1.7 (1)		
SL-C-4	SR 1.7 (1) (2)		
5.10	**SR 1.8 – Public key infrastructure (PKI) certificates**		
5.10.1	**Requirement**		
	Where PKI is utilized, the control system shall provide the capability to operate a PKI according to commonly accepted best practices or obtain public key certificates from an existing PKI.		
5.10.3	**Requirement enhancements**		
	None		
5.10.4	**Security levels**		
	The requirements for the four SL levels that relate to SR 1.8 – Public key infrastructure (PKI) certificates are:		
SL-C-1	Not Selected		
SL-C-2	SR 1.8		
SL-C-3	SR 1.8		
SL-C-4	SR 1.8		

Annex 1 - Checklists for the verification of compliance to the "Guide for the certification of Cybersecurity capabilities of Marine materials and equipment"

Item	Requirement	Result	Notes
5.11	**SR 1.9 – Strength of public key authentication**		
5.11.1	**Requirement**		
	For control systems utilizing public key authentication, the control system shall provide the capability to: a) validate certificates by checking the validity of the signature of a given certificate; b) validate certificates by constructing a certification path to an accepted CA or in the case of self-signed certificates by deploying leaf certificates to all hosts which communicate with the subject to which the certificate is issued; c) validate certificates by checking a given certificate's revocation status; d) establish user (human, software process or device) control of the corresponding private key; and e) map the authenticated identity to a user (human, software process or device).		
5.11.3	**Requirement enhancements**		
(1)	Hardware security for public key authentication The control system shall provide the capability to protect the relevant private keys via hardware mechanisms according to commonly accepted security industry practices and recommendations.		
5.11.4	**Security levels**		
	The requirements for the four SL levels that relate to SR 1.9 – Strength of public key authentication are:		
SL-C-1	Not Selected		
SL-C-2	SR 1.9		
SL-C-3	SR 1.9 (1)		
SL-C-4	SR 1.9 (1)		
5.12	**SR 1.10 – Authenticator feedback**		
5.12.1	**Requirement**		
	The control system shall provide the capability to obscure feedback of authentication information during the authentication process.		
5.12.3	**Requirement enhancements**		
	None		
5.12.4	**Security levels**		
	The requirements for the four SL levels that relate to SR 1.10 – Authenticator feedback are:		
SL-C-1	SR 1.10		
SL-C-2	SR 1.10		
SL-C-3	SR 1.10		
SL-C-4	SR 1.10		

Item	Requirement	Result	Notes
5.13	**SR 1.11 – Unsuccessful login attempts**		
5.13.1	**Requirement**		
	The control system shall provide the capability to enforce a limit of a configurable number of consecutive invalid access attempts by any user (human, software process or device) during a configurable time period. The control system shall provide the capability to deny access for a specified period of time or until unlocked by an administrator when this limit has been exceeded. For system accounts on behalf of which critical services or servers are run, the control system shall provide the capability to disallow interactive logons.		
5.13.3	**Requirement enhancements**		
	None		
5.13.4	**Security levels**		
	The requirements for the four SL levels that relate to SR 1.11 – Unsuccessful login attempts are:		
SL-C-1	SR 1.11		
SL-C-2	SR 1.11		
SL-C-3	SR 1.11		
SL-C-4	SR 1.11		
5.14	**SR 1.12 – System use notification**		
5.14.1	**Requirement**		
	The control system shall provide the capability to display a system use notification message before authenticating. The system use notification message shall be configurable by authorized personnel.		
5.14.3	**Requirement enhancements**		
	None		
5.14.4	**Security levels**		
	The requirements for the four SL levels that relate to SR 1.12 – System use notification are:		
SL-C-1	SR 1.12		
SL-C-2	SR 1.12		
SL-C-3	SR 1.12		
SL-C-4	SR 1.12		
5.15	**SR 1.13 – Access via untrusted networks**		
5.15.1	**Requirement**		
	The control system shall provide the capability to monitor and control all methods of access to the control system via untrusted networks.		
5.15.3	**Requirement enhancements**		
(1)	Explicit access request approval The control system shall provide the capability to deny access requests via untrusted networks unless approved by an assigned role.		

Annex 1 - Checklists for the verification of compliance to the "Guide for the certification of Cybersecurity capabilities of Marine materials and equipment"

Item	Requirement	Result	Notes
5.15.4	**Security levels**		
	The requirements for the four SL levels that relate to SR 1.13 – Access via untrusted networks are:		
SL-C-1	SR 1.13		
SL-C-2	SR 1.13 (1)		
SL-C-3	SR 1.13 (1)		
SL-C-4	SR 1.13 (1)		
6	**FR 2 – Use control**		
	Purpose and SL-C(UC) descriptions Enforce the assigned privileges of an authenticated user (human, software process or device) to perform the requested action on the OT systems and monitor the use of these privileges. **SL 1 –** Restrict use of the OT systems according to specified privileges to protect against casual or coincidental misuse. **SL 2 –** Restrict use of the OT systems according to specified privileges to protect against circumvention by entities using simple means with low resources, generic skills and low motivation. **SL 3 –** Restrict use of the OT systems according to specified privileges to protect against circumvention by entities using sophisticated means with moderate resources, OT systems specific skills and moderate motivation. **SL 4 –** Restrict use of the OT systems according to specified privileges to protect against circumvention by entities using sophisticated means with extended resources, OT systems specific skills and high motivation.		
6.3	**SR 2.1 – Authorization enforcement**		
6.3.1	**Requirement**		
	On all interfaces, the control system shall provide the capability to enforce authorizations assigned to all human users for controlling use of the control system to support segregation of duties and least privilege.		
6.3.3	**Requirement enhancements**		
(1)	Authorization enforcement for all users On all interfaces, the control system shall provide the capability to enforce authorizations assigned to all users (humans, software processes and devices) for controlling use of the control system to support segregation of duties and least privilege.		
(2)	Permission mapping to roles The control system shall provide the capability for an authorized user or role to define and modify the mapping of permissions to roles for all human users. NOTE 1 Roles should not be limited to fixed nested hierarchies in which a higher level role is a super set of a lesser privileged role. For example, a system administrator should not necessarily encompass operator privileges.		

Annex 1 - Checklists for the verification of compliance to the “Guide for the certification of Cybersecurity capabilities of Marine materials and equipment”

Item	Requirement	Result	Notes
	NOTE 2 This RE should be applicable to software processes and devices as well.		
(3)	Supervisor override The control system shall support supervisor manual override of the current human user authorizations for a configurable time or event sequence. NOTE Implementation of a controlled, audited and manual override of automated mechanisms in the event of emergencies or other serious events is often needed. This allows a supervisor to enable an operator to quickly react to unusual conditions without closing the current session and establishing a new session as a higher privilege human user.		
(4)	Dual approval The control system shall support dual approval where an action can result in serious impact on the industrial process. NOTE Dual approval should be limited to actions which require a very high level of confidence that they will be performed reliably and correctly. Requiring dual approval provides emphasis to the seriousness of consequences that would result from failure of a correct action. An example of a situation in which dual approval is required would be a change to a set point of a critical industrial process. Dual approval mechanisms should not be employed when an immediate response is necessary to safeguard HSE consequences, for example, emergency shutdown of an industrial process.		
6.3.4	**Security levels**		
	The requirements for the four SL levels that relate to SR 2.1 – Authorization enforcement are:		
SL-C-1	2.1		
SL-C-2	2.1 (1) (2)		
SL-C-3	2.1 (1) (2) (3)		
SL-C-4	2.1 (1) (2) (3) (4)		
6.4	**SR 2.2 – Wireless use control**		
6.4.1	**Requirement**		
	The control system shall provide the capability to authorize, monitor and enforce usage restrictions for wireless connectivity to the control system according to commonly accepted security industry practices.		
6.4.3	**Requirement enhancements**		
(1)	Identify and report unauthorized wireless devices The control system shall provide the capability to identify and report unauthorized wireless devices transmitting within the control system physical environment.		
6.4.4	**Security levels**		
	The requirements for the four SL levels that relate to SR 2.2 – Wireless use control are:		
SL-C-1	SR 2.2		
SL-C-2	SR 2.2		
SL-C-3	SR 2.2 (1)		
SL-C-4	SR 2.2 (1)		

Annex 1 - Checklists for the verification of compliance to the “Guide for the certification of Cybersecurity capabilities of Marine materials and equipment”

Item	Requirement	Result	Notes
6.5	**SR 2.3 – Use control for portable and mobile devices**		
6.5.1	**Requirement**		
	The control system shall provide the capability to automatically enforce configurable usage restrictions that include: a) preventing the use of portable and mobile devices; b) requiring context specific authorization; and c) restricting code and data transfer to/from portable and mobile devices.		
6.5.3	**Requirement enhancements**		
(1)	Enforcement of security status of portable and mobile devices The control system shall provide the capability to verify that portable or mobile devices attempting to connect to a zone comply with the security requirements of that zone.		
6.5.4	**Security levels**		
	The requirements for the four SL levels that relate to SR 2.3 – Use control for portable and mobile devices are:		
SL-C-1	SR 2.3		
SL-C-2	SR 2.3		
SL-C-3	SR 2.3 (1)		
SL-C-4	SR 2.3 (1)		
6.6	**SR 2.4 – Mobile code**		
6.6.1	**Requirement**		
	The control system shall provide the capability to enforce usage restrictions for mobile code technologies based on the potential to cause damage to the control system that include: a) preventing the execution of mobile code; b) requiring proper authentication and authorization for origin of the code; c) restricting mobile code transfer to/from the control system; and d) monitoring the use of mobile code.		
6.6.3	**Requirement enhancements**		
(1)	Mobile code integrity checks The control system shall provide the capability to verify integrity of the mobile code before allowing code execution.		
6.6.4	**Security levels**		
	The requirements for the four SL levels that relate to SR 2.4 – Mobile code are:		
SL-C-1	SR 2.4		
SL-C-2	SR 2.4		
SL-C-3	SR 2.4 (1)		
SL-C-4	SR 2.4 (1)		

Annex 1 - Checklists for the verification of compliance to the "Guide for the certification of Cybersecurity capabilities of Marine materials and equipment"

Item	Requirement	Result	Notes
6.7	**SR 2.5 – Session lock**		
6.7.1	**Requirement**		
	The control system shall provide the capability to prevent further access by initiating a session lock after a configurable time period of inactivity or by manual initiation. The session lock shall remain in effect until the human user who owns the session, or another authorized human user, re-establishes access using appropriate identification and authentication procedures.		
6.7.3	**Requirement enhancements**		
	None		
6.7.4	**Security levels**		
SL-C-1	SR 2.5		
SL-C-2	SR 2.5		
SL-C-3	SR 2.5		
SL-C-4	SR 2.5		
6.8	**SR 2.6 – Remote session termination**		
6.8.1	**Requirement**		
	The control system shall provide the capability to terminate a remote session either automatically after a configurable time period of inactivity or manually by the user who initiated the session.		
6.8.3	**Requirement enhancements**		
	None		
6.8.4	**Security levels**		
	The requirements for the four SL levels that relate to SR 2.6 – Remote session termination are:		
SL-C-1	Not Selected		
SL-C-2	SR 2.6		
SL-C-3	SR 2.6		
SL-C-4	SR 2.6		
6.9	**SR 2.7 – Concurrent session control**		
6.9.1	**Requirement**		
	The control system shall provide the capability to limit the number of concurrent sessions per interface for any given user (human, software process or device) to a configurable number of sessions.		
6.9.3	**Requirement enhancements**		
	None		
6.9.4	**Security levels**		
	The requirements for the four SL levels that relate to SR 2.7 – Concurrent session control are:		
SL-C-1	Not Selected		
SL-C-2	Not Selected		

Annex 1 - Checklists for the verification of compliance to the "Guide for the certification of Cybersecurity capabilities of Marine materials and equipment"

Item	Requirement	Result	Notes
SL-C-3	SR 2.7		
SL-C-4	SR 2.7		
6.10	**SR 2.8 – Auditable events**		
6.10.1	**Requirement**		
	The control system shall provide the capability to generate audit records relevant to security for the following categories: access control, request errors, operating system events, control system events, backup and restore events, configuration changes, potential reconnaissance activity and audit log events. Individual audit records shall include the timestamp, source (originating device, software process or human user account), category, type, event ID and event result.		
6.10.3	**Requirement enhancements**		
(1)	Centrally managed, system-wide audit trail The control system shall provide the capability to centrally manage audit events and to compile audit records from multiple components throughout the control system into a system-wide (logical or physical), time-correlated audit trail. The control system shall provide the capability to export these audit records in industry standard formats for analysis by standard commercial log analysis tools, for example, security information and event management (SIEM).		
6.10.4	**Security levels**		
	The requirements for the four SL levels that relate to SR 2.8 – Auditable events are:		
SL-C-1	SR 2.8		
SL-C-2	SR 2.8		
SL-C-3	SR 2.8 (1)		
SL-C-4	SR 2.8 (1)		
6.11	**SR 2.9 – Audit storage capacity**		
6.11.1	**Requirement**		
	The control system shall allocate sufficient audit record storage capacity according to commonly recognized recommendations for log management and system configuration. The control system shall provide auditing mechanisms to reduce the likelihood of such capacity being exceeded.		
6.11.3	**Requirement enhancements**		
(1)	Warn when audit record storage capacity threshold reached The control system shall provide the capability to issue a warning when the allocated audit record storage volume reaches a configurable percentage of maximum audit record storage capacity.		
6.11.4	**Security levels**		
	The requirements for the four SL levels that relate to SR 2.9 – Audit storage capacity are:		
SL-C-1	SR 2.9		
SL-C-2	SR 2.9		

Annex 1 - Checklists for the verification of compliance to the "Guide for the certification of Cybersecurity capabilities of Marine materials and equipment"

Item	Requirement	Result	Notes
SL-C-3	SR 2.9 (1)		
SL-C-4	SR 2.9 (1)		
6.12	**SR 2.10 – Response to audit processing failures**		
6.12.1	**Requirement**		
	The control system shall provide the capability to alert personnel and prevent the loss of essential services and functions in the event of an audit processing failure. The control system shall provide the capability to support appropriate actions in response to an audit processing failure according to commonly accepted industry practices and recommendations.		
6.12.3	**Requirement enhancements**		
	None		
6.12.4	**Security levels**		
	The requirements for the four SL levels that relate to SR 2.10 – Response to audit processing failures are:		
SL-C-1	SR 2.10		
SL-C-2	SR 2.10		
SL-C-3	SR 2.10		
SL-C-4	SR 2.10		
6.13	**SR 2.11 – Timestamps**		
6.13.1	**Requirement**		
	The control system shall provide timestamps for use in audit record generation		
6.13.3	**Requirement enhancements**		
(1)	Internal time synchronization The control system shall provide the capability to synchronize internal system clocks at a configurable frequency.		
(2)	Protection of time source integrity The time source shall be protected from unauthorized alteration and shall cause an audit event upon alteration.		
6.13.4	**Security levels**		
	The requirements for the four SL levels that relate to SR 2.11 – Timestamps are:		
SL-C-1	Not selected		
SL-C-2	SR 2.11		
SL-C-3	SR 2.11 (1)		
SL-C-4	SR 2.11 (1) (2)		
6.14	**SR 2.12 – Non-repudiation**		
6.14.1	**Requirement**		
	The control system shall provide the capability to determine whether a given human user took a particular action.		

Annex 1 - Checklists for the verification of compliance to the "Guide for the certification of Cybersecurity capabilities of Marine materials and equipment"

Item	Requirement	Result	Notes
6.14.3	**Requirement enhancements**		
(1)	Non-repudiation for all users The control system shall provide the capability to determine whether a given user (human, software process or device) took a particular action.		
6.14.4	**Security levels**		
	The requirements for the four SL levels that relate to SR 2.12 – Non-repudiation are:		
SL-C-1	Not Selected		
SL-C-2	Not Selected		
SL-C-3	SR 2.12		
SL-C-4	SR 2.12 (1)		
7	**FR 3 – System integrity** **Purpose and SL-C(SI) descriptions** Ensure the integrity of the OT systems to prevent unauthorized manipulation. **SL 1 –** Protect the integrity of the OT systems against casual or coincidental manipulation. **SL 2 –** Protect the integrity of the OT systems against manipulation by someone using simple means with low resources, generic skills and low motivation. **SL 3 –** Protect the integrity of the OT systems against manipulation by someone using sophisticated means with moderate resources, OT systems specific skills and moderate motivation. **SL 4 –** Protect the integrity of the OT systems against manipulation by someone using sophisticated means with extended resources, OT systems specific skills and high motivation.		
7.3	**SR 3.1 – Communication integrity**		
7.3.1	**Requirement**		
	The control system shall provide the capability to protect the integrity of transmitted information.		
7.3.3	**Requirement enhancements**		
(1)	Cryptographic integrity protection The control system shall provide the capability to employ cryptographic mechanisms to recognize changes to information during communication. NOTE The use of cryptographic mechanisms to provide message authentication and integrity should be determined after careful consideration of the security needs and the potential ramifications on system performance and capability to recover from system failure.		
7.3.4	**Security levels**		
	The requirements for the four SL levels that relate to SR 3.1 – Communication integrity are:		
SL-C-1	SR 3.1		
SL-C-2	SR 3.1		
SL-C-3	SR 3.1 (1)		
SL-C-4	SR 3.1 (1)		

Annex 1 - Checklists for the verification of compliance to the "Guide for the certification of Cybersecurity capabilities of Marine materials and equipment"

Item	Requirement	Result	Notes
7.4	**SR 3.2 – Malicious code protection**		
7.4.1	**Requirement**		
	The control system shall provide the capability to employ protection mechanisms to prevent, detect, report and mitigate the effects of malicious code or unauthorized software. The control system shall provide the capability to update the protection mechanisms.		
7.4.3	**Requirement enhancements**		
(1)	Malicious code protection on entry and exit points The control system shall provide the capability to employ malicious code protection mechanisms at all entry and exit points. NOTE Mechanisms at this level may include removable media, firewalls, unidirectional gateways, web servers, proxy servers and remote-access servers.		
(2)	Central management and reporting for malicious code protection The control system shall provide the capability to manage malicious code protection mechanisms. NOTE Such mechanisms may be provided by endpoint infrastructure centralized management and SIEM solutions.		
7.4.4	**Security levels**		
	The requirements for the four SL levels that relate to SR 3.2 – Malicious code protection are:		
SL-C-1	SR 3.2		
SL-C-2	SR 3.2 (1)		
SL-C-3	SR 3.2 (1) (2)		
SL-C-4	SR 3.2 (1) (2)		
7.5	**SR 3.3 – Security functionality verification**		
7.5.1	**Requirement**		
	The control system shall provide the capability to support verification of the intended operation of security functions and report when anomalies are discovered during FAT, SAT and scheduled maintenance. These security functions shall include all those necessary to support the security requirements specified in this standard.		
7.5.3	**Requirement enhancements**		
(1)	Automated mechanisms for security functionality verification The control system shall provide the capability to employ automated mechanisms to support management of security verification during FAT, SAT and scheduled maintenance.		
(2)	Security functionality verification during normal operation The control system shall provide the capability to support verification of the intended operation of security functions during normal operations. NOTE This RE needs to be carefully implemented to avoid detrimental effects. It may not be suitable for safety systems.		

Annex 1 - Checklists for the verification of compliance to the "Guide for the certification of Cybersecurity capabilities of Marine materials and equipment"

Item	Requirement	Result	Notes
7.5.4	**Security levels**		
	The requirements for the four SL levels that relate to SR 3.3 – Security functionality verification are:		
SL-C-1	SR 3.3		
SL-C-2	SR 3.3		
SL-C-3	SR 3.3 (1)		
SL-C-4	SR 3.3 (1) (2)		
7.6	**SR 3.4 – Software and information integrity**		
7.6.1	**Requirement**		
	The control system shall provide the capability to detect, record, report and protect against unauthorized changes to software and information at rest.		
7.6.3	**Requirement enhancements**		
(1)	Automated notification about integrity violations The control system shall provide the capability to use automated tools that provide notification to a configurable set of recipients upon discovering discrepancies during integrity verification.		
7.6.4	**Security levels**		
	The requirements for the four SL levels that relate to SR 3.4 – Software and information integrity are:		
SL-C-1	Not Selected		
SL-C-2	SR 3.4		
SL-C-3	SR 3.4 (1)		
SL-C-4	SR 3.4 (1)		
7.7	**SR 3.5 – Input validation**		
7.7.1	**Requirement**		
	The control system shall validate the syntax and content of any input which is used as an industrial process control input or input that directly impacts the action of the control system.		
7.7.3	**Requirement enhancements**		
	None		
7.7.4	**Security levels**		
	The requirements for the four SL levels that relate to SR 3.5 – Input validation are:		
SL-C-1	SR 3.5		
SL-C-2	SR 3.5		
SL-C-3	SR 3.5		
SL-C-4	SR 3.5		
7.8	**SR 3.6 – Deterministic output**		
7.8.1	**Requirement**		
	The control system shall provide the capability to set outputs to a predetermined state if normal operation cannot be maintained as a result of an attack.		

Annex 1 - Checklists for the verification of compliance to the “Guide for the certification of Cybersecurity capabilities of Marine materials and equipment”

Item	Requirement	Result	Notes
7.8.3	**Requirement enhancements**		
	None		
7.8.4	**Security levels**		
	The requirements for the four SL levels that relate to SR 3.6 – Deterministic output are:		
SL-C-1	SR 3.6		
SL-C-2	SR 3.6		
SL-C-3	SR 3.6		
SL-C-4	SR 3.6		
7.9	**SR 3.7 – Error handling**		
7.9.1	**Requirement**		
	The control system shall identify and handle error conditions in a manner such that effective remediation can occur. This shall be done in a manner which does not provide information that could be exploited by adversaries to attack the OT systems unless revealing this information is necessary for the timely troubleshooting of problems.		
7.9.3	**Requirement enhancements**		
	None		
7.9.4	**Security levels**		
	The requirements for the four SL levels that relate to SR 3.7 – Error handling are:		
SL-C-1	Not Selected		
SL-C-2	SR 3.7		
SL-C-3	SR 3.7		
SL-C-4	SR 3.7		
7.10	**SR 3.8 – Session integrity**		
7.10.1	**Requirement**		
	The control system shall provide the capability to protect the integrity of sessions. The control system shall reject any usage of invalid session IDs.		
7.10.3	**Requirement enhancements**		
(1)	Invalidation of session IDs after session termination The control system shall provide the capability to invalidate session IDs upon user logout or other session termination (including browser sessions).		
(2)	Unique session ID generation The control system shall provide the capability to generate a unique session ID for each session and treat all unexpected session IDs as invalid.		
(3)	Randomness of session IDs The control system shall provide the capability to generate unique session IDs with commonly accepted sources of randomness. NOTE Session hijacking and other man-in-the-middle attacks or injections of false information often take advantage of easy-to-guess session IDs (keys or other		

Item	Requirement	Result	Notes
	shared secrets) or use of session IDs which were not properly invalidated after session termination. Therefore the validity of a session authenticator needs to be tightly connected to the lifetime of a session. Employing randomness in the generation of unique session IDs helps to protect against brute-force attacks to determine future session IDs.		
7.10.4	**Security levels**		
	The requirements for the four SL levels that relate to SR 3.8 – Session integrity are:		
SL-C-1	Not Selected		
SL-C-2	SR 3.8		
SL-C-3	SR 3.8 (1) (2)		
SL-C-4	SR 3.8 (1) (2) (3)		
7.11	**SR 3.9 – Protection of audit information**		
7.11.1	**Requirement**		
	The control system shall protect audit information and audit tools (if present) from unauthorized access, modification and deletion.		
7.11.3	**Requirement enhancements**		
(1)	Audit records on write-once media The control system shall provide the capability to produce audit records on hardware-enforced write-once media.		
7.11.4	**Security levels**		
	The requirements for the four SL levels that relate to SR 3.9 – Protection of audit information are:		
SL-C-1	Not selected		
SL-C-2	SR 3.9		
SL-C-3	SR 3.9		
SL-C-4	SR 3.9 (1)		
8	**FR 4 – Data confidentiality** **Purpose and SL-C(DC) descriptions** Ensure the confidentiality of information on communication channels and in data repositories to prevent unauthorized disclosure. **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, OT systems 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, OT systems specific skills and high motivation.		

Annex 1 - Checklists for the verification of compliance to the "Guide for the certification of Cybersecurity capabilities of Marine materials and equipment"

Item	Requirement	Result	Notes
8.3	**SR 4.1 – Information confidentiality**		
8.3.1	**Requirement**		
	The control system shall provide the capability to protect the confidentiality of information for which explicit read authorization is supported, whether at rest or in transit.		
8.3.3	**Requirement enhancements**		
(1)	Protection of confidentiality at rest or in transit via untrusted networks The control system shall provide the capability to protect the confidentiality of information at rest and remote access sessions traversing an untrusted network.		
(2)	Protection of confidentiality across zone boundaries The control system shall provide the capability to protect the confidentiality of information traversing any zone boundary.		
8.3.4	**Security levels**		
	The requirements for the four SL levels that relate to SR 4.1 – Information confidentiality are:		
SL-C-1	SR 4.1		
SL-C-2	SR 4.1 (1)		
SL-C-3	SR 4.1 (1)		
SL-C-4	4: SR 4.1 (1) (2)		
8.4	**SR 4.2 – Information persistence**		
8.4.1	**Requirement**		
	The control system shall provide the capability to purge all information for which explicit read authorization is supported from components to be released from active service and/or decommissioned.		
8.4.3	**Requirement enhancements**		
(1)	Purging of shared memory resources The control system shall provide the capability to prevent unauthorized and unintended information transfer via volatile shared memory resources.		
8.4.4	**Security levels**		
	The requirements for the four SL levels that relate to SR 4.2 – Information persistence are:		
SL-C-1	Not Selected		
SL-C-2	SR 4.2		
SL-C-3	SR 4.2 (1)		
SL-C-4	SR 4.2 (1)		
8.5	**SR 4.3 – Use of cryptography**		
8.5.1	**Requirement**		
	If cryptography is required, the control system shall use cryptographic algorithms, key sizes and mechanisms for key establishment and management according to commonly accepted security industry practices and recommendations.		

Annex 1 - Checklists for the verification of compliance to the "Guide for the certification of Cybersecurity capabilities of Marine materials and equipment"

Item	Requirement	Result	Notes
8.5.3	**Requirement enhancements**		
	None		
8.5.4	**Security levels**		
	The requirements for the four SL levels that relate to SR 4.3 – Use of cryptography are:		
SL-C-1	SR 4.3		
SL-C-2	SR 4.3		
SL-C-3	SR 4.3		
SL-C-4	SR 4.3		
9	**FR 5 – Restricted data flow** **Purpose and SL-C(RDF) descriptions** Segment the control system via zones and conduits to limit the unnecessary flow of data. **SL 1 –** Prevent the casual or coincidental circumvention of zone and conduit segmentation. **SL 2 –** Prevent the intended circumvention of zone and conduit segmentation by entities using simple means with low resources, generic skills and low motivation. **SL 3 –** Prevent the intended circumvention of zone and conduit segmentation by entities using sophisticated means with moderate resources, OT systems specific skills and moderate motivation. **SL 4 –** Prevent the intended circumvention of zone and conduit segmentation by entities using sophisticated means with extended resources, OT systems specific skills and high motivation.		
9.3	**SR 5.1 – Network segmentation**		
9.3.1	**Requirement**		
	The control system shall provide the capability to logically segment control system networks from non-control system networks and to logically segment critical control system networks from other control system networks.		
9.3.3	**Requirement enhancements**		
(1)	Physical network segmentation The control system shall provide the capability to physically segment control system networks from non-control system networks and to physically segment critical control system networks from non-critical control system networks.		
(2)	Independence from non-control system networks The control system shall have the capability to provide network services to control system networks, critical or otherwise, without a connection to non-control system networks.		
(3)	Logical and physical isolation of critical networks The control system shall provide the capability to logically and physically isolate critical control system networks from non-critical control system networks.		
9.3.4	**Security levels**		
	The requirements for the four SL levels that relate to SR 5.1 – Network segmentation are:		
SL-C-1	SR 5.1		
SL-C-2	SR 5.1 (1)		

Annex 1 - Checklists for the verification of compliance to the “Guide for the certification of Cybersecurity capabilities of Marine materials and equipment”

Item	Requirement	Result	Notes
SL-C-3	SR 5.1 (1) (2)		
SL-C-4	SR 5.1 (1) (2) (3)		
9.4	**SR 5.2 – Zone boundary protection**		
9.4.1	**Requirement**		
	The control system shall provide the capability to monitor and control communications at zone boundaries to enforce the compartmentalization defined in the risk-based zones and conduits model.		
9.4.3	**Requirement enhancements**		
(1)	Deny by default, allow by exception The control system shall provide the capability to deny network traffic by default and allow network traffic by exception (also termed deny all, permit by exception).		
(2)	Island mode The control system shall provide the capability to prevent any communication through the control system boundary (also termed island mode).		
(3)	Fail close The control system shall provide the capability to prevent any communication through the control system boundary when there is an operational failure of the boundary protection mechanisms (also termed fail close). This ‘fail close’ functionality shall be designed such that it does not interfere with the operation of a SIS or other safety-related functions.		
9.4.4	**Security levels**		
	The requirements for the four SL levels that relate to SR 5.2 – Zone boundary protection are:		
SL-C-1	SR 5.2		
SL-C-2	SR 5.2 (1)		
SL-C-3	SR 5.2 (1) (2)		
SL-C-4	SR 5.2 (1) (2) (3)		
9.5	**SR 5.3 – General purpose person-to-person communication restrictions**		
9.5.1	**Requirement**		
	The control system shall provide the capability to prevent general purpose person-to-person messages from being received from users or systems external to the control system.		
9.5.3	**Requirement enhancements**		
(1)	Prohibit all general-purpose person-to-person communications The control system shall provide the capability to prevent both transmission and receipt of general-purpose person-to-person messages.		
9.5.4	**Security levels**		
	The requirements for the four SL levels that relate to SR 5.3 – Zone boundary protection are:		
SL-C-1	SR 5.3		
SL-C-2	SR 5.3		

Annex 1 - Checklists for the verification of compliance to the "Guide for the certification of Cybersecurity capabilities of Marine materials and equipment"

Item	Requirement	Result	Notes
SL-C-3	SR 5.3 (1)		
SL-C-4	SR 5.3 (1)		
9.6	**SR 5.4 – Application partitioning**		
9.6.1	**Requirement**		
	The control system shall provide the capability to support partitioning of data, applications and services based on criticality to facilitate implementing a zoning model.		
9.6.3	**Requirement enhancements**		
	None		
9.6.4	**Security levels**		
	The requirements for the four SL levels that relate to SR 5.4 – Zone boundary protection are:		
SL-C-1	SR 5.4		
SL-C-2	SR 5.4		
SL-C-3	SR 5.4		
SL-C-4	SR 5.4		
10	**FR 6 – Timely response to events** **Purpose and SL-C(TRE) descriptions** Respond to security violations by notifying the proper authority, reporting needed evidence of the violation and taking timely corrective action when incidents are discovered. **SL 1 –** Monitor the operation of the OT systems and respond to incidents when they are discovered by collecting and providing the forensic evidence when queried. **SL 2 –** Monitor the operation of the OT systems and respond to incidents when they are discovered by actively collecting and periodically reporting forensic evidence. **SL 3 –** Monitor the operation of the OT systems and respond to incidents when they are discovered by actively collecting and pushing forensic evidence to the proper authority. **SL 4 –** Monitor the operation of the OT systems and respond to incidents when they are discovered by actively collecting and pushing forensic evidence to the proper authority in near real-time.		
10.3	**SR 6.1 – Audit log accessibility**		
10.3.1	**Requirement**		
	The control system shall provide the capability for authorized humans and/or tools to access audit logs on a read-only basis.		
10.3.3	**Requirement enhancements**		
(1)	Programmatic access to audit logs The control system shall provide programmatic access to audit records using an application programming interface (API).		
10.3.4	**Security levels**		
	The requirements for the four SL levels that relate to SR 6.1 – Audit log accessibility are:		
SL-C-1	SR 6.1		
SL-C-2	SR 6.1		

Item	Requirement	Result	Notes
SL-C-3	SR 6.1 (1)		
SL-C-4	SR 6.1 (1)		
10.4	**SR 6.2 – Continuous monitoring**		
10.4.1	**Requirement**		
	The control system shall provide the capability to continuously monitor all security mechanism performance using commonly accepted security industry practices and recommendations to detect, characterize and report security breaches in a timely manner.		
10.4.3	**Requirement enhancements**		
	None		
10.4.4	**Security levels**		
	The requirements for the four SL levels that relate to SR 6.2 – Continuous monitoring are:		
SL-C-1	SR 6.2		
SL-C-2	SR 6.2		
SL-C-3	SR 6.2		
SL-C-4	SR 6.2		
11	**FR 7 – Resource availability** **Purpose and SL-C(RA) descriptions** Ensure the availability of the control system against the degradation or denial of essential services. **SL 1 –** Ensure that the control system operates reliably under normal production conditions and prevents DoS situations caused by the casual or coincidental actions of an entity. **SL 2 –** Ensure that the control system operates reliably under normal and abnormal production conditions and prevents DoS situations by entities using simple means with low resources, generic skills and low motivation. **SL 3 –** Ensure that the control system operates reliably under normal, abnormal, and extreme production conditions and prevents DoS situations by entities using sophisticated means with moderate resources, OT systems specific skills and moderate motivation. **SL 4 –** Ensure that the control system operates reliably under normal, abnormal, and extreme production conditions and prevents DoS situations by entities using sophisticated means with extended resources, OT systems specific skills and high motivation.		
11.3	**SR 7.1 – Denial of service protection**		
11.3.1	**Requirement**		
	The control system shall provide the capability to operate in a degraded mode during a DoS event.		
11.3.3	**Requirement enhancements**		
(1)	Manage communication loads The control system shall provide the capability to manage communication loads (such as using rate limiting) to mitigate the effects of information flooding types of DoS events.		

Annex 1 - Checklists for the verification of compliance to the "Guide for the certification of Cybersecurity capabilities of Marine materials and equipment"

Item	Requirement	Result	Notes
(2)	Limit DoS effects to other systems or networks The control system shall provide the capability to restrict the ability of all users (humans, software processes and devices) to cause DoS events which affect other control systems or networks.		
11.3.4	**Security levels**		
	The requirements for the four SL levels that relate to SR 7.1 – Denial of service protection are:		
SL-C-1	SR 7.1		
SL-C-2	SR 7.1 (1)		
SL-C-3	SR 7.1 (1) (2)		
SL-C-4	SR 7.1 (1) (2)		
11.4	**SR 7.2 – Resource management**		
11.4.1	**Requirement**		
	The control system shall provide the capability to limit the use of resources by security functions to prevent resource exhaustion.		
11.4.3	**Requirement enhancements**		
	None		
11.4.4	**Security levels**		
	The requirements for the four SL levels that relate to SR 7.2 – Resource management are:		
SL-C-1	SR 7.2		
SL-C-2	SR 7.2		
SL-C-3	SR 7.2		
SL-C-4	SR 7.2		
11.5	**SR 7.3 – Control system backup**		
11.5.1	**Requirement**		
	The identity and location of critical files and the ability to conduct backups of user-level and system-level information (including system state information) shall be supported by the control system without affecting normal plant operations.		
11.5.3	**Requirement enhancements**		
(1)	Backup verification The control system shall provide the capability to verify the reliability of backup mechanisms.		
(2)	Backup automation The control system shall provide the capability to automate the backup function based on a configurable frequency.		
11.5.4	**Security levels**		
	The requirements for the four SL levels that relate to SR 7.3 – Control system backup are:		
SL-C-1	SR 7.3		
SL-C-2	SR 7.3 (1)		
SL-C-3	SR 7.3 (1) (2)		
SL-C-4	SR 7.3 (1) (2)		

Annex 1 - Checklists for the verification of compliance to the "Guide for the certification of Cybersecurity capabilities of Marine materials and equipment"

Item	Requirement	Result	Notes
11.6	**SR 7.4 – Control system recovery and reconstitution**		
11.6.1	**Requirement**		
	The control system shall provide the capability to recover and reconstitute to a known secure state after a disruption or failure.		
11.6.3	**Requirement enhancements**		
	None		
11.6.4	**Security levels**		
	The requirements for the four SL levels that relate to SR 7.4 – Control system recovery and reconstitution are:		
SL-C-1	SR 7.4		
SL-C-2	SR 7.4		
SL-C-3	SR 7.4		
SL-C-4	SR 7.4		
11.7	**SR 7.5 – Emergency power**		
11.7.1	**Requirement**		
	The control system shall provide the capability to switch to and from an emergency power supply without affecting the existing security state or a documented degraded mode.		
11.7.3	**Requirement enhancements**		
	None		
11.7.4	**Security levels**		
	The requirements for the four SL levels that relate to SR 7.5 – Emergency power are:		
SL-C-1	SR 7.5		
SL-C-2	SR 7.5		
SL-C-3	SR 7.5		
SL-C-4	SR 7.5		
11.8	**SR 7.6 – Network and security configuration settings**		
11.8.1	**Requirement**		
	The control system shall provide the capability to be configured according to recommended network and security configurations as described in guidelines provided by the control system supplier. The control system shall provide an interface to the currently deployed network and security configuration settings.		
11.8.3	**Requirement enhancements**		
(1)	Machine-readable reporting of current security settings The control system shall provide the capability to generate a report listing the currently deployed security settings in a machine-readable format.		

Annex 1 - Checklists for the verification of compliance to the "Guide for the certification of Cybersecurity capabilities of Marine materials and equipment"

Item	Requirement	Result	Notes
11.8.4	**Security levels**		
	The requirements for the four SL levels that relate to SR 7.6 – Network and security configuration settings are:		
SL-C-1	SR 7.6		
SL-C-2	SR 7.6		
SL-C-3	SR 7.6 (1)		
SL-C-4	SR 7.6 (1)		
11.9	**SR 7.7 – Least functionality**		
11.9.1	**Requirement**		
	The control system shall provide the capability to specifically prohibit and/or restrict the use of unnecessary functions, ports, protocols and/or services.		
11.9.3	**Requirement enhancements**		
	None		
11.9.4	**Security levels**		
	The requirements for the four SL levels that relate to SR 7.7 – Least functionality are:		
SL-C-1	SR 7.7		
SL-C-2	SR 7.7		
SL-C-3	SR 7.7		
SL-C-4	SR 7.7		
11.10	**SR 7.8 – Control system component inventory**		
11.10.1	**Requirement**		
	The control system shall provide the capability to report the current list of installed components and their associated properties.		
11.10.3	**Requirement enhancements**		
	None		
11.10.4	**Security levels**		
	The requirements for the four SL levels that relate to SR 7.8 – Control system component inventory are:		
SL-C-1	SR 7.8		
SL-C-2	SR 7.8		
SL-C-3	SR 7.8		
SL-C-4	SR 7.8		

Annex 1 - Checklists for the verification of compliance to the "Guide for the certification of Cybersecurity capabilities of Marine materials and equipment"

Checklist #3 – Secure product development lifecycle requirements

Numbering of items is intended to be consistent with ISA/IEC 62443-4-1 for easy reference.

Item	Requirement	Result	Notes
5	**Practice 1 – Security management**		
5.2	**SM-1: Development process**		
5.2.1	**Requirement**		
	A general product development/maintenance/support process shall be documented and enforced that is consistent and integrated with commonly accepted product development processes that include, but are not limited to:		
	a) configuration management with change controls and audit logging;		
	b) product description and requirements definition with requirements traceability;		
	c) software or hardware design and implementation practices, such as modular design;		
	d) repeatable testing verification and validation process;		
	e) review and approval of all development process records; and		
	f) life-cycle support.		
5.3	**SM-2: Identification of responsibilities**		
5.3.1	**Requirement**		
	A process shall be employed that identifies the organizational roles and personnel responsible for each of the processes required by this standard.		
5.4	**SM-3: Identification of applicability**		
5.4.1	**Requirement**		
	A process shall be employed for identifying products (or parts of products) to which this standard applies.		
5.5	**SM-4: Security expertise**		
5.5.1	**Requirement**		
	A process shall be employed for identifying and providing security training and assessment programs to ensure that personnel assigned to the organizational roles and duties specified in 5.3, SM-2: Identification of responsibilities, have demonstrated security expertise appropriate for those processes.		

Annex 1 - Checklists for the verification of compliance to the "Guide for the certification of Cybersecurity capabilities of Marine materials and equipment"

Item	Requirement	Result	Notes
5.6	**SM-5: Process scoping**		
5.6.1	**Requirement**		
	A process, that includes justification by documented security analysis, shall be employed to identify the parts of this standard that are applicable to a selected product development project. Justification for scoping the level of compliance of a project to this standard shall be subject to review and approval by personnel with the appropriate security expertise (see SM-4: Security expertise).		
5.7	**SM-6: File integrity**		
5.7.1	**Requirement**		
	A process shall be employed to provide an integrity verification mechanism for all scripts, executables and other important files included in a product.		
5.8	**SM-7: Development environment security**		
5.8.1	**Requirement**		
	A process that includes procedural and technical controls shall be employed for protecting the product during development, production and delivery. This includes protecting the product or product update (patch) during design, implementation, testing and release.		
5.9	**SM-8: Controls for private keys**		
5.9.1	**Requirement**		
	The supplier shall have procedural and technical controls in place to protect private keys used for code signing from unauthorized access or modification.		
5.10	**SM-9: Security requirements for externally provided components**		
5.10.1	**Requirement**		
	A process shall be employed to identify and manage the security risks of all externally provided components used within the product.		
5.11	**SM-10: Custom developed components from third-party suppliers**		
5.11.1	**Requirement**		
	A process shall be employed to ensure that product development life-cycle processes for components from a third-party supplier conform to the requirements used in this document when they meet the following criteria:		
	a) the components are developed specifically for a single supplier for a specific purpose; and		
	b) the components can have an impact on security.		
5.12	**SM-11: Assessing and addressing security-related issues**		
5.12.1	**Requirement**		
	A process shall be employed for verifying that a product or a patch is not released until its security- related issues have been addressed and tracked to closure (see 10.5,		

Annex 1 - Checklists for the verification of compliance to the "Guide for the certification of Cybersecurity capabilities of Marine materials and equipment"

Item	Requirement	Result	Notes
	DM-4: Addressing security- related issues). This includes issues associated with:		
	a) requirements (see Clause 6, Practice 2 – Specification of security requirements);		
	b) secure by design (see Clause 7, Practice 3 – Secure by design);		
	c) implementation (see Clause 8, Practice 4 – Secure implementation);		
	d) verification/validation (see Clause 9, Practice 5 – Security verification and validation testing); and		
	e) defect management (see Clause 10, Practice 6 – Management of security-related issues).		
5.13	**SM-12: Process verification**		
5.13.1	**Requirement**		
	A process shall be employed for verifying that, prior to product release, all applicable security- related processes required by this specification (see SM-5: Process scoping) have been completed with records documenting the completion of each process.		
5.14	**SM-13: Continuous improvement**		
5.14.1	**Requirement**		
	A process shall be employed for continuously improving the SDL. This process shall include the analysis of security defects in component/subsystem/system technologies that escape to the field.		
6	**Practice 2 – Specification of security requirements**		
6.2	**SR-1: Product security context**		
6.2.1	**Requirement**		
	A process shall be employed to ensure that the intended product security context is documented		
6.3	**SR-2: Threat model**		
6.3.1	**Requirement**		
	A process shall be employed to ensure that all products shall have a threat model specific to the current development scope of the product with the following characteristics (where applicable):		
	a) correct flow of categorized information throughout the system;		
	b) trust boundaries;		
	c) processes;		
	d) data stores;		
	e) interacting external entities;		
	f) internal and external communication protocols implemented in the product;		
	g) externally accessible physical ports including debug ports ;		

Annex 1 - Checklists for the verification of compliance to the "Guide for the certification of Cybersecurity capabilities of Marine materials and equipment"

Item	Requirement	Result	Notes
	h) circuit board connections such as Joint Test Action Group (JTAG) connections or debug headers which might be used to attack the hardware;		
	i) potential attack vectors including attacks on the hardware, if applicable;		
	j) potential threats and their severity as defined by a vulnerability scoring system (for example, CVSS);		
	k) mitigations and/or dispositions for each threat;		
	l) security-related issues identified; and		
	m) external dependencies in the form of drivers or third-party applications (code that is not developed by the supplier) that are linked into the application.		
	The threat model shall be reviewed and verified by the development team to ensure that it is correct and understood. The threat model shall be reviewed periodically (at least once a year) for released products and updated if required in response to the emergence of new threats to the product even if the design does not change. Any issues identified in the threat model shall be addressed as defined in 10.4, DM-3: Assessing security-related issues, and 10.5, DM-4: Addressing security-related issues.		
6.4	**SR-3: Product security requirements**		
6.4.1	**Requirement**		
	A process shall be employed for ensuring that security requirements are documented for the product/feature under development including requirements for security capabilities related to installation, operation, maintenance and decommissioning.		
6.5	**SR-4: Product security requirements content**		
6.5.1	**Requirement**		
	A process shall be employed for ensuring that security requirements include the following information:		
	a) the scope and boundaries of the component or system, in general terms in both a physical and a logical way; and		
	b) the required capability security level (SL-C) of the product.		
6.6	**SR-5: Security requirements review**		
6.6.1	**Requirement**		
	A process shall be employed to ensure that security requirements are reviewed, updated as necessary and approved to ensure clarity, validity, alignment with the threat model (discussed in 6.3 SR-2: Threat model), and their ability to be verified. Each of the following representative disciplines shall participate in this process. Personnel may be assigned to more than one discipline except for testers, who shall remain independent.		
	a) architects/developers (those who will implement the requirements);		
	b) testers (those who will validate that the requirements have been met);		

Annex 1 - Checklists for the verification of compliance to the "Guide for the certification of Cybersecurity capabilities of Marine materials and equipment"

Item	Requirement	Result	Notes
	c) customer advocate (such as sales, marketing, product management or customer support); and		
	d) security advisor		
7	**Practice 3 – Secure by design**		
7.2	**SD-1: Secure design principles**		
7.2.1	**Requirement**		
	A process shall be employed for developing and documenting a secure design that identifies and characterizes each interface of the product, including physical and logical interfaces, to include:		
	a) an indication of whether the interface is externally accessible (by other products), or internally accessible (by other components of the product), or both;		
	b) security implications of the product security context (see Clause 6, Practice 2 – Specification of security requirements) on the external interface;		
	c) potential users of the interface and the assets that can be accessed through it (directly or indirectly);		
	d) a determination of whether access to the interface crosses a trust boundary;		
	e) security considerations, assumptions and/or constraints associated with the use of the interface within the product security context, including applicable threats;		
	f) the security roles, privileges/rights and access control permissions needed to use the interface and to access the assets defined in c) above;		
	g) the security capabilities and/or compensating mechanisms used to safeguard the interface and the assets defined in c) above, including input validation as well as output and error handling;		
	h) the use of third-party products to implement the interface and their security capabil ities;		
	i) documentation that describes how to use the interface if it is externally accessible ; and		
	j) description of how the design mitigates the threats identified in the threat model.identified in the threat model.		
7.3	**SD-2: Defense in depth design**		
7.3.1	**Requirement**		
	A process shall be employed to implement multiple layers of defense using a risk based approach based on the threat model. This process shall be employed for assigning responsibilities to each layer of defense.		
7.4	**SD-3: Security design review**		
7.4.1	**Requirement**		
	A process shall be employed for conducting design reviews to identify, characterize and track to closure security-related issues associated with each significant revision of the secure design including but not limited to:		
	a) security requirements (see Clause 6, Practice 2 – Specification of security requirements) that were not		

Annex 1 - Checklists for the verification of compliance to the “Guide for the certification of Cybersecurity capabilities of Marine materials and equipment”

Item	Requirement	Result	Notes
	adequately addressed by the design;.		
	b) threats and their ability to exploit product interfaces, trust boundaries, and assets (see 7.2, SD-1: Secure design principles); and		
	c) identification of secure design practices (see 7.5, SD-4: Secure design best practices) that were not followed (for example, failure to apply principle of least privilege).		
7.5	**SD-4: Secure design best practices**		
7.5.1	**Requirement**		
	A process shall be employed to ensure that secure design best practices are documented and applied to the design process. These practices shall be periodically reviewed and updated. Secure design practices include but are not be limited to:		
	a) least privilege (granting only the privileges to users/software necessary to perform intended operations);		
	b) using proven secure components/designs where possible;		
	c) economy of mechanism (striving for simple designs);		
	d) using secure design patterns;		
	e) attack surface reduction;		
	f) all trust boundaries are documented as part of the design; and		
	g) removing debug ports, headers and traces from circuit boards used during development from production hardware or documenting their presence and the need to protect them from unauthorized access.		
8	**Practice 4 – Secure implementation**		
8.3	**SI-1: Security implementation review**		
8.3.1	**Requirement**		
	A process shall be employed to ensure that implementation reviews are performed for identifying, characterizing and tracking to closure security-related issues associated with the implementation of the secure design including:		
	a) identification of security requirements (see Clause 6, Practice 2 – Specification of security requirements) that were not adequately addressed by the implementation;		
	b) identification of secure coding standards (see 8.4, SI-2: Secure coding standards) that were not followed (for example, use of banned functions or failure to apply principle of least privilege);		
	c) Static Code Analysis (SCA) for source code to determine security coding errors such as buffer overflows, null pointer dereferencing, etc. using the secure coding standard for the supported programming language. SCA shall be done using a tool if one is available for the language used. In addition, static code analysis shall be done on all source code changes including new source code.		

Annex 1 - Checklists for the verification of compliance to the "Guide for the certification of Cybersecurity capabilities of Marine materials and equipment"

Item	Requirement	Result	Notes
	d) review of the implementation and its traceability to the security capabilities defined to support the security design (see Clause 7, Practice 3 – Secure by design); and		
	e) examination of threats and their ability to exploit implementation interfaces, trust boundaries and assets (see 7.2, SD-1: Secure design principles, and 7.3, SD-2: Defense in depth design).		
8.4	**SI-2: Secure coding standards**		
8.4.1	**Requirement**		
	The implementation processes shall incorporate security coding standards that are periodically reviewed and updated and include at a minimum:		
	a) avoidance of potentially exploitable implementation constructs – implementation design patterns that are known to have security weaknesses;		
	b) avoidance of banned functions and coding constructs/design patterns – software functions and design patterns that should not be used because they have known security weaknesses;		
	c) automated tool use and settings (for example, for static analysis tools);		
	d) secure coding practices;		
	e) validation of all inputs that cross trust boundary.		
	f) error handling		
9	**Practice 5 – Security verification and validation testing**		
9.2	**SVV-1: Security requirements testing**		
8.2.1	**Requirement**		
	A process shall be employed for verifying the product security functions meet the security requirements and that the product handles error scenarios and invali d input correctly. Types of testing shall include:		
	a) functional testing of security requirements;		
	b) performance and scalability testing; and		
	c) boundary/edge condition, stress and malformed or unexpected input tests not specifically targeted at security;		
9.3	**SVV-2: Threat mitigation testing**		
9.3.1	**Requirement**		
	A process shall be employed for testing the effectiveness of the mitigation for the threats identified and validated in the threat model. Activities shall include:		
	a) creating and executing plans to ensure that each mitigation implemented to address a specific threat has been adequately tested to ensure the mitigation works as designed and		
	b) creating and executing plans for attempting to thwart each mitigation.		
9.4	**SVV-3: Vulnerability testing**		
9.4.1	**Requirement**		

Annex 1 - Checklists for the verification of compliance to the "Guide for the certification of Cybersecurity capabilities of Marine materials and equipment"

Item	Requirement	Result	Notes
	A process shall be employed for performing tests that focus on identifying and characterizing potential security vulnerabilities in the product. Known vulnerability testing shall be based upon, at a minimum, recent contents of an established, industry-recognized, public source for known vulnerabilities. Testing shall include:		
	a) abuse case or malformed or unexpected input testing focused on uncovering security issues. This shall include manual or automated abuse case testing and specialized types of abuse case testing on all external interfaces and protocols for which tools exist. Examples include fuzz testing and network traffic load testing and capacity testing.		
	b) attack surface analysis to determine all avenues of ingress and egress to and from the system, common vulnerabilities including but not limited to week ACLs, exposed ports and services running with elevated privileges.		
	c) black box known vulnerability scanning focused on detecting known vulnerabilities in the product hardware, host or software components. For example, this could be a network based known vulnerability scan.		
	d) for compiled software, software composition analysis on all binary executable files, including embedded firmware, delivered by the supplier to be installed for a product. This analysis shall detect the following types of problems at a minimum:		
	1) known vulnerabilities in the product software components;		
	2) linking to vulnerable libraries;		
	3) security rule violations; and		
	4) compiler settings that can lead to vulnerabilities.		
	e) dynamic runtime resource management testing that detects flaws not visible under static code analysis, including but not limited to denial of service conditions due to failing to releas e runtime handles, memory leaks and accesses made to shared memory without authentication. This testing shall be applied if such tools are available.		
9.5	**SVV-4: Penetration testing**		
9.5.1	**Requirement**		
	A process shall be employed to identify and characterize security-related issues via tests that focus on discovering and exploiting security vulnerabilities in the product.		
9.6	**SVV-5: Independence of testers**		
9.6.1	**Requirement**		
	A process shall be employed to ensure that individuals performing testing are independent from the developers who designed and implemented the product.		
10	**Practice 6 – Management of security-related issues**		
10.2	**DM-1: Receiving notifications of security-related issues**		
10.2.1	**Requirement**		

Item	Requirement	Result	Notes
	A process shall exist for receiving and tracking to closure security-related issues in the product reported by internal and external sources including at a minimum:		
	a) security verification and validation testers;		
	b) suppliers of third-party components used in the product;		
	c) product developers and testers; and		
	d) product users including integrators, asset owners, and maintenance personnel.		
10.4	**DM-3: Assessing security-related issues**		
10.4.1	**Requirement**		
	A process shall be employed for analysing security-related issues in the product to include:		
	a) assessing their impact with respect to:		
	1) the actual security context in which they were discovered;		
	2) the product's security context (see Clause 6, Practice 2 – Specification of security requirements); and		
	3) the product's defense in depth strategy (see Clause 7, Practice 3 – Secure by design);		
	b) severity as defined by a vulnerability scoring system (for example, CVSS);		
	c) identifying all other products/product versions containing the security-related issue (if any);		
	d) identifying the root causes of the issue; and		
	e) identifying related security issues.		
	For root cause analysis, a methodical approach such as that described in IEC 62740 [23] may be employed.		
10.5	**DM-4: Addressing security-related issues**		
10.5.1	**Requirement**		
	A process shall be employed for addressing security-related issues and determining whether to report them based on the results of the impact assessment (see 10.4, DM-3: Assessing security- related issues). The supplier shall establish an acceptable level of residual risk that shall be applied when determining appropriate way to address each issue. Options include one or more of the following:		
	a) fixing the issue through one or more of the following:		
	1) defense in depth strategy or design change;		
	2) addition of one or more security requirements and/or capabilities;		
	3) use of compensating mechanisms; and/or		
	4) disabling or removing features;		
	b) creating a remediation plan to fix the problem;		
	c) deferring the problem for future resolution (reapply this requirement at some time in the future) and specifying the reason(s) and associated risk(s);		
	d) not fixing the problem if the residual risk is below the established acceptable level of residual risk.		
	In all cases the following shall be done as well:		

Annex 1 - Checklists for the verification of compliance to the “Guide for the certification of Cybersecurity capabilities of Marine materials and equipment”

Item	Requirement	Result	Notes
	a) inform other processes of the issue or related issue(s), including processes for o ther products/product revisions; and		
	b) Inform third parties if problems found in included third-party source code		
	When security-related issues are resolved recommendations to prevent similar errors from occurring in the future shall be evaluated.		
	This process shall include a periodic review of open security-related issues to ensure that issues are being addressed appropriately. This periodic review shall at a minimum occur during each release or iteration cycle.		
10.6	**DM-5: Disclosing security-related issues**		
10.6.1	**Requirement**		
	A process shall be employed for informing product users about reportable security-related issues (see 10.5, DM-4: Addressing security-related issues) in supported products in a timely manner with content that includes but is not limited to the following information:		
	a) issue description, vulnerability score as per CVSS or a similar system for ranking vulnerabilities, and affected product version(s); and		
	b) description of the resolution.		
	The strategy for handling third-party component vulnerabilities discovered by the product developer should take into account the possibility of premature public disclosure by the third -party component supplier.		
10.7	**DM-6: Periodic review of security defect management practice**		
10.7.1	**Requirement**		
	A process shall be employed for conducting periodic reviews of the security-related issue management process. Periodic reviews of the process shall, at a minimum, examine security- related issues managed through the process since the last periodic review to determine if the management process was complete, efficient, and led to the resolution of each security-related issue. Periodic reviews of the security-related issue management process shall be conducted at least annually.		
11	**Practice 7 – Security update management**		
11.2	**SUM-1: Security update qualification**		
11.2.1	**Requirement**		
	A process shall be employed for verifying		
	1) security updates created by the product developer address the intended security vulnerabilities		
	2) security updates do not introduce regressions, including but not limited to patches created by:		
	a) the product developer;		
	b) suppliers of components used in the product; and		
	c) suppliers of components or platforms on which the product depends .		

Item	Requirement	Result	Notes
	The process should include a confirmation that update is not contradicting other operational, safety or legal constraints.		
11.3	**SUM-2: Security update documentation**		
11.3.1	**Requirement**		
	A process shall be employed to ensure that documentation about product security updates is made available to product users that includes but is not limited to:		
	a) the product version number(s) to which the security patch applies;		
	b) instructions on how to apply approved patches manually and via an automated process;		
	c) description of any impacts that applying the patch to the product, including reboot;		
	d) instructions on how to verify that an approved patch has been applied; and		
	e) risks of not applying the patch and mediations that can be used for patches that are not approved or deployed by the asset owner.		
11.4	**SUM-3: Dependent component or operating system security update documentation**		
11.4.1	**Requirement**		
	A process shall be employed to ensure that documentation about dependent component or operating system security updates is made available to product users that includes but is not limited to:		
	a) stating whether the product is compatible with the dependent component or operating system security update; and		
	b) for security updates that are unapproved by the product vendor, the mitigations that can be used in lieu of not applying the update.		
11.5	**SUM-4: Security update delivery**		
11.5.1	**Requirement**		
	A process shall be employed to ensure that security updates for all supported products and product versions are made available to product users in a manner that facilitates verification that the security patch is authentic.		
11.5	**SUM-5: Timely delivery of security patches**		
11.5.1	**Requirement**		
	A process shall be employed to define a policy that specifies the timeframes for delivering and qualifying (see SUM-1: Security update qualification) security updates to product users and to ensure that this policy is followed. At a minimum, this policy shall consider the following factors:		
	a) The potential impact of the vulnerability;		
	b) Public knowledge of the vulnerability;		
	c) Whether published exploits exist for the vulnerability;		

Item	Requirement	Result	Notes
	d) The volume of deployed products that are affected; and		
	e) The availability of an effective mitigation in lieu of the patch.		

Checklist #4 – Technical security requirements for OT components

Numbering of items is intended to be consistent with ISA/IEC 62443-4-2 for easy reference.

Item	Requirement	Resul t	Notes
5	**FR 1 – Identification and authentication control** **Purpose and SL-C(IAC) descriptions** Identify and authenticate all users (humans, software processes and devices), prior to allowing them access to the system or assets. **SL 1 –** Identify and authenticate all users (humans, software processes and devices) by mechanisms that protect against casual or coincidental access by unauthenticated entities. **SL 2 –** Identify and authenticate all users (humans, software processes and devices) by mechanisms that protect against intentional unauthenticated access by entities using simple means with low resources, generic skills and low motivation. **SL 3 –** Identify and authenticate all users (humans, software processes and devices) by mechanisms that protect against intentional unauthenticated access by entities using sophisticated means with moderate resources, OT systems specific skills and moderate motivation. **SL 4 –** Identify and authenticate all users (humans, software processes and devices) by mechanisms that protect against intentional unauthenticated access by entities using sophisticated means with extended resources, OT systems specific skills and high motivation.		
5.3	**CR 1.1 – Human user identification and authentication**		
5.3.1	**Requirement**		
	Components shall provide the capability to identify and authenticate all human users according to ISA-62443-3-3 [11] SR 1.1 on all interfaces capable of human user access. This capability shall enforce such identification and authentication on all interfaces that provide human user access to the component to support segregation of duties and least privilege in accordance with applicable security policies and procedures. This capability may be provided locally by the component or by integration into a system level identification and authentication system.		
5.3.3	**Requirement enhancements**		
(1)	Unique identification and authentication: Components shall provide the capability to uniquely identify and authenticate all human users.		
(2)	Multifactor authentication for all interfaces Components shall provide the capability to employ multifactor authentication for all human user access to the component.		
5.3.4	**Security levels**		
	The requirements for the four security levels that relate to CR 1.2 are:		
SL-C -1	CR 1.1		
SL-C-2	CR 1.1 (1)		
SL-C-3	CR 1.1 (1) (2)		

Annex 1 - Checklists for the verification of compliance to the “Guide for the certification of Cybersecurity capabilities of Marine materials and equipment”

Item	Requirement	Result	Notes
SL-C-4	CR 1.1 (1) (2)		
5.4	**CR 1.2 – Software process and device identification and authentication**		
5.4.1	**Requirement**		
	Components shall provide the capability to identify itself and authenticate to any other component (software application, embedded devices, host devices and network devices), according to ISA-62443-3-3 [11] SR1.2. If the component, as in the case of an application, is running in the context of a human user, in addition, the identification and authentication of the human user according to ISA-62443-3-3 [11] SR1.1 may be part of the component identification and authentication process towards the other components.		
5.4.3	**Requirement enhancements**		
(1)	Unique identification and authentication Components shall provide the capability to uniquely identify and authenticate itself to any other component.		
5.4.4	**Security levels**		
	The requirements for the four security levels that relate to CR 1.3 are:		
SL-C-1	Not Selected		
SL-C-2	CR 1.2		
SL-C-3	CR 1.2 (1)		
SL-C-4	CR 1.2 (1)		
5.5	**CR 1.3 – Account management**		
5.5.1	**Requirement**		
	Components shall provide the capability to support the management of all accounts directly or integrated into a system that manages accounts according to ISA-62443-3-3 [11] SR 1.3.		
5.5.3	**Requirement enhancements**		
	None		
5.5.4	**Security levels**		
	The requirements for the four security levels that relate to CR 1.3 are:		
SL-C 1	CR 1.3		
SL-C-2	CR 1.3		
SL-C-3	CR 1.3		
SL-C-4	CR 1.3		
5.6	**CR 1.4 – Identifier management**		
5.6.1	**Requirement**		
	Components shall 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-62443-3-3 [11] SR 1.4.		

Annex 1 - Checklists for the verification of compliance to the "Guide for the certification of Cybersecurity capabilities of Marine materials and equipment"

Item	Requirement	Result	Notes
5.6.3	**Requirement enhancements**		
	None		
5.6.4	**Security levels**		
	The requirements for the four security levels that relate to CR 1.4 are:		
SL-C 1	CR 1.4		
SL-C-2	CR 1.4		
SL-C-3	CR 1.4		
SL-C-4	CR 1.4		
5.7	**CR 1.5 – Authenticator management**		
5.7.1	**Requirement**		
	Components shall provide the capability to:		
	a) support the use of initial authenticator content;		
	b) support the recognition of changes to default authenticators made at installation time;		
	c) function properly with periodic authenticator change/refresh operation; and		
	d) protect authenticators from unauthorized disclosure and modification when stored, used and transmitted.		
5.7.3	**Requirement enhancements**		
(1)	Hardware security for authenticators The authenticators on which the component rely shall be protected via hardware mechanisms.		
5.7.4	**Security levels**		
	The requirements for the four security levels that relate to CR 1.5 are:		
SL-C 1	CR 1.5		
SL-C-2	CR 1.5		
SL-C-3	CR 1.5 (1)		
SL-C-4	CR 1.5 (1)		
5.8	**CR 1.6 – Wireless access management**		
	The wireless access management requirements are network-component-specific and can be located as requirements for network-components in Clause 15.		
5.9	**CR 1.7 – Strength of password-based authentication**		
5.9.1	**Requirement**		
	For components that utilize password-based authentication, those components shall provide or integrate into a system that provides the capability to enforce configurable password strength according to internationally recognized and proven password guidelines		

Annex 1 - Checklists for the verification of compliance to the "Guide for the certification of Cybersecurity capabilities of Marine materials and equipment"

Item	Requirement	Resul t	Notes
5.9.3	**Requirement enhancements**		
(1)	Password generation and lifetime restrictions for human users Components shall provide, or integrate into a system that provides, the capability to protect against any given human user account from reusing a password for a configurable number of generations. In addition, the component shall provide the capability to enforce password minimum and maximum lifetime restrictions for human users. These capabilities shall conform to commonly accepted security industry practices.		
(2)	Password lifetime restrictions for all users (human, software process, or device) Components shall provide, or integrate into a system that provides, the capability to enforce password minimum and maximum lifetime restrictions for all users.		
5.9.4	**Security levels**		
	The requirements for the four security levels that relate to CR 1.7 are:		
SL-C 1	CR 1.7		
SL-C-2	CR 1.7		
SL-C-3	CR 1.7 (1)		
SL-C-4	CR 1.7 (1) (2)		
5.10	**CR 1.8 – Public key infrastructure certificates**		
5.10.1	**Requirement**		
	When public key infrastructure (PKI) is utilized, the component shall provide or integrate into a system that provides the capability to interact and operate in accordance with ISA-62443-3-3 [11] SR1.8.		
5.10.3	**Requirement enhancements**		
	None		
5.10.4	**Security levels**		
	The requirements for the four security levels that relate to CR 1.8 are:		
SL-C 1	Not selected		
SL-C-2	CR 1.8		
SL-C-3	CR 1.8		
SL-C-4	CR 1.8		
5.11	**CR 1.9 – Strength of public key-based authentication**		
5.11.1	**Requirement**		
	For components that utilize public-key-based authentication, those components shall provide directly or integrate into a system that provides the capability within the same OT systems environment to:		
	a) validate certificates by checking the validity of the signature of a given certificate;		

Item	Requirement	Result	Notes
	b) validate the certificate chain or, in the case of self-signed certificates, by deploying leaf certificates to all hosts that communicate with the subject to which the certificate is issued;		
	c) validate certificates by checking a given certificate's revocation status;		
	d) establish user (human, software process or device) control of the corresponding private key;		
	e) map the authenticated identity to a user (human, software process or device); and		
	f) ensure that the algorithms and keys used for the public key authentication comply with 8.5 CR 4.3 – Use of cryptography.		
5.11.3	**Requirement enhancements**		
(1)	Hardware security for public key-based authentication Components shall provide the capability to protect critical, long-lived private keys via hardware mechanisms.		
5.11.4	**Security levels**		
	The requirements for the four security levels that relate to CR 1.9 are:		
SL-C 1	Not selected		
SL-C-2	CR 1.9		
SL-C-3	CR 1.9 (1)		
SL-C-4	CR 1.9 (1)		
5.12	**CR 1.10 – Authenticator feedback**		
5.12.1	**Requirement**		
	When a component provides an authentication capability the component shall provide the capability to obscure feedback of authenticator information during the authentication process.		
5.12.3	**Requirement enhancements**		
	None		
5.12.4	**Security levels**		
	The requirements for the four security levels that relate to CR 1.10 are:		
SL-C 1	CR 1.10		
SL-C-2	CR 1.10		
SL-C-3	CR 1.10		
SL-C-4	CR 1.10		
5.13	**CR 1.11 – Unsuccessful login attempts**		
5.13.1	**Requirement**		
	When a component provides an authentication capability the component shall provide the capability to:		
	a) enforce a limit of a configurable number of consecutive invalid access attempts by any user (human, software process or device) during a configurable time period; and		

Annex 1 - Checklists for the verification of compliance to the "Guide for the certification of Cybersecurity capabilities of Marine materials and equipment"

Item	Requirement	Result	Notes
	b) deny access for a specified period of time or until unlocked by an administrator when this limit has been reached.		
5.13.3	**Requirement enhancements**		
	None		
5.13.4	**Security levels**		
	The requirements for the four security levels that relate to CR 1.11 are:		
SL-C 1	CR 1.11		
SL-C-2	CR 1.11		
SL-C-3	CR 1.11		
SL-C-4	CR 1.11		
5.14	**CR 1.12 – System use notification**		
5.14.1	**Requirement**		
	When a component provides local human user access/HMI, it shall provide the capability to display a system use notification message before authenticating. The system use notification message shall be configurable by authorized personnel.		
5.14.3	**Requirement enhancements**		
	None		
5.14.4	**Security levels**		
	The requirements for the four security levels that relate to CR 1.12 are:		
SL-C 1	CR 1.12		
SL-C-2	CR 1.12		
SL-C-3	CR 1.12		
SL-C-4	CR 1.12		
5.15	**CR 1.13 – Access via untrusted networks**		
	The access via untrusted networks requirements are component-specific and can be located as requirements for each specific component type in Clauses 12 through 15.		
5.16	**CR 1.14 – Strength of symmetric key-based authentication**		
5.16.1	**Requirement**		
	For components that utilize symmetric keys, the component shall provide the capability to:		
	a) establish the mutual trust using the symmetric key;		
	b) store securely the shared secret (the authentication is valid as long as the shared secret remains secret);		
	c) restrict access to the shared secret; and		
	d) ensure that the algorithms and keys used for the symmetric key authentication comply with CR 4.3 – Use of cryptography Subclause 8.5.		

Annex 1 - Checklists for the verification of compliance to the "Guide for the certification of Cybersecurity capabilities of Marine materials and equipment"

Item	Requirement	Result	Notes
5.16.3	**Requirement enhancements**		
(1)	Hardware security for symmetric key-based authentication Components shall provide the capability to protect critical, long lived symmetric keys via hardware mechanisms.		
5.16.4	**Security levels**		
	The requirements for the four security levels that relate to CR 1.14 are:		
SL-C 1	Not selected		
SL-C-2	CR 1.14		
SL-C-3	CR 1.14 (1)		
SL-C-4	CR 1.14 (1)		
6	**FR 2 – Use control** **Purpose and SL-C(UC) descriptions** 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. **SL 1** – Restrict use of the OT systems according to specified privileges to protect against casual or coincidental misuse. **SL 2** – Restrict use of the OT systems according to specified privileges to protect against circumvention by entities using simple means with low resources, generic skills and low motivation. **SL 3** – Restrict use of the OT systems according to specified privileges to prot ect against circumvention by entities using sophisticated means with moderate resources, OT systems specific skills and moderate motivation. **SL 4** – Restrict use of the OT systems according to specified privileges to protect against circumvention by entities using sophisticated means with extended resources, OT systems specific skills and high motivation. **Rationale** Once the user is identified and authenticated, the component must restrict the allowed actions to the authorized use of the component. Asset owners and system integrators will have to assign, to each user (human, software process or device), group, role, etc. (see 4.5) , the privileges defining the authorized use of the component. The goal of use control is to protect against unauthorized actions on the component's resources by verifying that the necessary privileges have been granted before allowing a user to perform the actions. Examples of actions are reading or writing data, downloading programs and setting configurations. Recommendations and guidelines should include mechanisms that will operate in mixed modes. For example, some component resources require strong use control protection, such as restrictive privileges, and others do not. By extension, use control requirements must be extended to data at rest. User privileges may vary based on time-of-day/date, location and means by which access is made.		

Annex 1 - Checklists for the verification of compliance to the "Guide for the certification of Cybersecurity capabilities of Marine materials and equipment"

Item	Requirement	Result	Notes
6.3	**CR 2.1 – Human user identification and authentication**		
6.3.1	**Requirement**		
	Components shall provide an authorization enforcement mechanism for all identified and authenticated users based on their assigned responsibilities.		
6.3.2	**Rationale and supplemental guidance**		
	Use control policies (for example, identity-based policies, role-based policies and rule-based policies) and associated read/write access enforcement mechanisms (for example, access con trol lists, access control matrices and cryptography) are employed to control usage between users (humans, software processes and devices) and assets (for example, devices, files, records, software processes, programs and domains). After the control system has verified the identity of a user (human, software process or device) (see 5.3, CR 1.1 – Human user identification and authentication and 5.4, CR 1.2 – Software process and device identification and authentication), it also has to verify that a requested operation is actually permitted according to the defined security policies a nd procedures. For example, in a role-based access control policy, the control system would check which roles are assigned to a verified user or asset and which privileges are assigned to these roles – if the requested operation is covered by the permissions, it is executed, otherwise rejected. This allows the enforcement of segregation of duties and least privileges. Usage enforcement mechanisms should not be allowed to adversely affect the operational performance of the control system. Planned or unplanned changes to control system components can have significant effects on the overall security of the control system. Accordingly, only qualified and authorized individuals should obtain the use of control system components for purposes of initiating changes , including upgrades and modifications.		
6.3.3	**Requirement enhancements**		
(1)	Authorization enforcement for all users (humans, software processes and devices) Components shall provide an authorization enforcement mechanism for all users based on their assigned responsibilities and least privilege.		
(2)	Permission mapping to roles Components shall, directly or through a compensating security mechanism, provide for an authorized role to define and modify the mapping of permissions to roles for all human users.		
(3)	Supervisor override Components shall support a supervisor manual override for a configurable time or sequence of events.		
(4)	Dual approval Components shall support dual approval when action can result in serious impact on the industrial process.		

Item	Requirement	Result	Notes
6.3.4	**Security levels**		
	The requirements for the four security levels that relate to CR 2.1 are:		
SL-C -1	CR 2.1		
SL-C-2	CR 2.1 (1) (2)		
SL-C-3	CR 2.1 (1) (2) (3)		
SL-C-4	CR 2.1 (1) (2) (3) (4)		
6.4	**CR 2.2 – Wireless use control**		
6.4.1	**Requirement**		
	If a component supports usage through wireless interfaces it shall provide the capability to integrate into the system that supports usage authorization, monitoring and restrictions according to commonly accepted industry practices.		
6.4.3	**Requirement enhancements**		
	None		
6.4.4	**Security levels**		
	The requirements for the four security levels that relate to CR 2.2 are:		
SL-C -1	CR 2.2		
SL-C-2	CR 2.2		
SL-C-3	CR 2.2		
SL-C-4	CR 2.2		
6.5	**CR 2.3 – Use control for portable and mobile devices**		
	There is no component level requirement associated with ISA-62443-3-3 SR 2.3.		
6.6	**CR 2.4 – Mobile code**		
	The use control requirements for mobile code are component-specific and can be located as requirements for each specific component type in Clauses 13 through 15.		
6.7	**CR 2.5 – Session lock**		
6.7.1	**Requirement**		
	If a component provides a human user interface, whether accessed locally or via a network, the component shall provide the capability		
	a) to protect against further access by initiating a session lock after a configurable time period of inactivity or by manual initiation by the user (human, software process or device); and		
	b) for the session lock to remain in effect until the human user who owns the session, or another authorized human user, re-establishes access using appropriate identification and authentication procedures.		

Item	Requirement	Resul t	Notes
6.7.3	**Requirement enhancements**		
	None		
6.7.4	**Security levels**		
	The requirements for the four security levels that relate to CR 2.5 are:		
SL-C -1	CR 2.5		
SL-C-2	CR 2.5		
SL-C-3	CR 2.5		
SL-C-4	CR 2.5		
6.8	**CR 2.6 – Remote session termination**		
6.8.1	**Requirement**		
	If a component supports remote sessions, the component shall provide the capability to terminate a remote session either automatically after a configurable time period of inactivity, manually by a local authority, or manually by the user (human, software process or device) who initiated the session.		
6.8.3	**Requirement enhancements**		
	None		
6.8.4	**Security levels**		
	The requirements for the four security levels that relate to CR 2.6 are:		
SL-C -1	Not Selected		
SL-C-2	CR 2.6		
SL-C-3	CR 2.6		
SL-C-4	CR 2.6		
6.9	**CR 2.7 – Concurrent session control**		
6.9.1	**Requirement**		
	Components shall provide the capability to limit the number of concurrent sessions per interface for any given user (human, software process or device)		
6.9.3	**Requirement enhancements**		
	None		
6.9.4	**Security levels**		
	The requirements for the four security levels that relate to CR 2.6 are:		
SL-C -1	Not Selected		
SL-C-2	Not Selected		
SL-C-3	CR 2.7		
SL-C-4	CR 2.7		

Item	Requirement	Resul t	Notes
6.10	**CR 2.8 – Auditable events**		
6.10.1	**Requirement**		
	Components shall provide the capability to generate audit records relevant to security for the following categories:		
	a) access control;		
	b) request errors;		
	c) control system events;		
	d) backup and restore event;		
	e) configuration changes; and		
	f) audit log events.		
	Individual audit records shall include:		
	a) timestamp;		
	b) source (originating device, software process or human user account);		
	c) category;		
	d) type;		
	e) event ID; and		
	f) event result.		
6.10.3	**Requirement enhancements**		
	None		
6.10.4	**Security levels**		
	The requirements for the four security levels that relate to CR 2.8 are:		
SL-C -1	CR 2.8		
SL-C-2	CR 2.8		
SL-C-3	CR 2.8		
SL-C-4	CR 2.8		
6.11	**CR 2.9 – Audit storage capacity**		
6.11.1	**Requirement**		
	Components shall		
	a) provide the capability to allocate audit record storage capacity according to commonly recognized recommendations for log management; and		
	b) provide mechanisms to protect against a failure of the component when it reaches or exceeds the audit storage capacity.		
6.11.3	**Requirement enhancements**		
(1)	Warn when audit record storage capacity threshold reached Components shall provide the capability to issue a warning when the allocated audit record storage reaches a configurable threshold.		

Annex 1 - Checklists for the verification of compliance to the "Guide for the certification of Cybersecurity capabilities of Marine materials and equipment"

Item	Requirement	Result	Notes
6.11.4	**Security levels**		
	The requirements for the four security levels that relate to CR 2.9 are:		
SL-C -1	CR 2.9		
SL-C-2	CR 2.9		
SL-C-3	CR 2.9 (1)		
SL-C-4	CR 2.9 (1)		
6.12	**CR 2.10 – Response to audit processing failures**		
6.12.1	**Requirement**		
	Components shall		
	a) provide the capability to protect against the loss of essential services and functions in the event of an audit processing failure; and		
	b) provide the capability to support appropriate actions in response to an audit processing failure according to commonly accepted industry practices and recommendations.		
6.12.3	**Requirement enhancements**		
	None		
6.12.4	**Security levels**		
	The requirements for the four security levels that relate to CR 2.10 are:		
SL-C -1	CR 2.10		
SL-C-2	CR 2.10		
SL-C-3	CR 2.10		
SL-C-4	CR 2.10		
6.13	**CR 2.11 – Timestamps**		
6.13.1	**Requirement**		
	Components shall provide the capability to create timestamps (including date and time) for use in audit records		
6.13.3	**Requirement enhancements**		
(1)	Time synchronization Components shall provide the capability to create timestamps that are synchronized with a system wide time source.		
(2)	Protection of time source integrity The time synchronization mechanism shall provide the capability to detect unauthorized alteration and cause an audit event upon alteration.		
6.13.4	**Security levels**		
	The requirements for the four security levels that relate to CR 2.11 are:		
SL-C -1	CR 2.11		
SL-C-2	CR 2.11 (1)		

Item	Requirement	Result	Notes
SL-C-3	CR 2.11 (1)		
SL-C-4	CR 2.11 (1) (2)		
6.14	**CR 2.12 – Non-repudiation**		
6.14.1	**Requirement**		
	If a component provides a human user interface, the component shall provide the capability to determine whether a given human user took a particular action. Control elements that are not able to support such capability shall be l isted in component documents.		
6.14.3	**Requirement enhancements**		
(1)	Non-repudiation for all users Components shall provide the capability to determine whether a given user (human, software process or device) took a particular action.		
6.14.4	**Security levels**		
	The requirements for the four security levels that relate to CR 2.12 are:		
SL-C -1	CR 2.12		
SL-C-2	CR 2.12		
SL-C-3	CR 2.12		
SL-C-4	CR 2.12 (1)		
6.15	**CR 2.13 – Use of physical diagnostic and test interfaces**		
	The use of physical diagnostic and test interfaces requirements are component-specific and can be located as requirements for each specific component type in Clauses 12 through 15.		
7	**FR 3 – System integrity** **Purpose and SL-C(Si) descriptions** Ensure the integrity of the component to protect against unauthorized manipulation or modification. SL 1 – Protect the integrity of the OT systems against casual or coincidental manipulation. SL 2 – Protect the integrity of the OT systems against manipulation by someone using simple means with low resources, generic skills and low motivation. SL 3 – Protect the integrity of the OT systems against manipulation by someone using sophisticated means with moderate resources, OT systems specific skills and moderate motivation. SL 4 – Protect the integrity of the OT systems against manipulation by someone using sophisticated means with extended resources, OT systems specific skills and high motivation.		
7.3	**CR 3.1 – Communication integrity**		
7.3.1	**Requirement**		
	Components shall provide the capability to protect integrity of transmitted information		

Annex 1 - Checklists for the verification of compliance to the “Guide for the certification of Cybersecurity capabilities of Marine materials and equipment”

Item	Requirement	Resul t	Notes
7.3.3	**Requirement enhancements**		
(1)	Communication authentication Components shall provide the capability to verify the authenticity of received information during communication.		
7.3.4	**Security levels**		
	The requirements for the four security levels that relate to CR 3.1 are:		
SL-C -1	CR 3.1		
SL-C-2	CR 3.1 (1)		
SL-C-3	CR 3.1 (1)		
SL-C-4	CR 3.1 (1)		
7.4	**CR 3.2 – Protection from malicious code**		
	The protection from malicious code requirements are component-specific and can be located as requirements for each specific component type in Clauses 12 through 15.		
7.5	**CR 3.3 – Security functionality verification**		
7.5.1	**Requirement**		
	Components shall provide the capability to support verification of the intended operation of security functions according to ISA-62443-3-3 [11] SR3.3.		
7.5.3	**Requirement enhancements**		
(1)	Security functionality verification during normal operation Components shall provide the capability to support verification of the intended operation of security functions during normal operations.		
7.5.4	**Security levels**		
	The requirements for the four security levels that relate to CR 3.3 are:		
SL-C -1	CR 3.3		
SL-C-2	CR 3.3		
SL-C-3	CR 3.3		
SL-C-4	CR 3.3 (1)		
7.6	**CR 3.4 – Software and information integrity**		
7.6.1	**Requirement**		
	Components shall provide the capability to perform or support integrity checks on software, configuration and other information as well as the recording and reporting of the results of these checks or be integrated into a system that can perform or support integrity checks		

Annex 1 - Checklists for the verification of compliance to the "Guide for the certification of Cybersecurity capabilities of Marine materials and equipment"

Item	Requirement	Result	Notes
7.6.3	**Requirement enhancements**		
(1)	Authenticity of software and information Components shall provide the capability to perform or support authenticity checks on software, configuration and other information as well as the recording and reporting of the results of these checks or be integrated into a system that can perform or support authenticity checks.		
(2)	Automated notification of integrity violations If the component is performing the integrity check, it shall be capable of automatically providing notification to a configurable entity upon discovery of an attempt to make an unauthorized change.		
7.6.4	**Security levels**		
	The requirements for the four security levels that relate to CR 3.4 are:		
SL-C -1	CR 3.4		
SL-C-2	CR 3.4 (1)		
SL-C-3	CR 3.4 (1) (2)		
SL-C-4	CR 3.4 (1) (2)		
7.7	**CR 3.5 – Input validation**		
7.7.1	**Requirement**		
	Components shall validate the syntax, length and content of any input data that is used as an industrial process control input or input via external interfaces that directly i mpacts the action of the component		
7.7.3	**Requirement enhancements**		
	None		
7.7.4	**Security levels**		
	The requirements for the four security levels that relate to CR 3.5 are:		
SL-C -1	CR 3.5		
SL-C-2	CR 3.5		
SL-C-3	CR 3.5		
SL-C-4	CR 3.5		
7.8	**CR 3.6 – Deterministic output**		
7.8.1	**Requirement**		
	Components that physically or logically connect to an automation process shall provide the capability to set outputs to a predetermined state if normal operation as defined by the component supplier cannot be maintained.		
7.8.3	**Requirement enhancements**		
	None		

Annex 1 - Checklists for the verification of compliance to the "Guide for the certification of Cybersecurity capabilities of Marine materials and equipment"

Item	Requirement	Resul t	Notes
7.8.4	**Security levels**		
	The requirements for the four security levels that relate to CR 3.6 are:		
SL-C -1	CR 3.6		
SL-C-2	CR 3.6		
SL-C-3	CR 3.6		
SL-C-4	CR 3.6		
7.9	**CR 3.7 – Error handling**		
7.9.1	**Requirement**		
	Components shall identify and handle error conditions in a manner that does not provide information that could be exploited by adversaries to attack the OT systems.		
7.9.3	**Requirement enhancements**		
	None		
7.9.4	**Security levels**		
	The requirements for the four security levels that relate to CR 3.7 are:		
SL-C -1	CR 3.7		
SL-C-2	CR 3.7		
SL-C-3	CR 3.7		
SL-C-4	CR 3.7		
7.10	**CR 3.8 – Session integrity**		
7.10.1	**Requirement**		
	Components shall provide mechanisms to protect the integrity of communications sessions including: a) the capability to invalidate session identifiers upon user logout or other session termination (including browser sessions); b) the capability to generate a unique session identifier f or each session and recognize only session identifiers that are system-generated; and c) the capability to generate unique session identifiers with commonly accepted sources of randomness.		
7.10.3	**Requirement enhancements**		
	None		
7.10.4	**Security levels**		
	The requirements for the four security levels that relate to CR 3.7 are:		
SL-C -1	Not selected		
SL-C-2	CR 3.8		
SL-C-3	CR 3.8		
SL-C-4	CR 3.8		

Annex 1 - Checklists for the verification of compliance to the "Guide for the certification of Cybersecurity capabilities of Marine materials and equipment"

Item	Requirement	Resul t	Notes
7.11	**CR 3.9 – Protection of audit information**		
7.11.1	**Requirement**		
	Components shall protect audit information, audit logs, and audit tools (if present) from unauthorized access, modification and deletion.		
7.11.3	**Requirement enhancements**		
(1)	Audit records on write-once media Components shall provide the capability to store audit records on hardware-enforced write- once media.		
7.11.4	**Security levels**		
	The requirements for the four security levels that relate to CR 3.7 are:		
SL-C -1	Not selected		
SL-C-2	CR 3.9		
SL-C-3	CR 3.9		
SL-C-4	CR 3.9 (1)		
7.12	**CR 3.10 – Support for updates**		
	The support for updates requirements is component-specific and can be located as requirements for each specific device type in Clauses 12 through 15.		
7.13	**CR 3.11 – Physical tamper resistance and detection**		
	The physical tamper resistance and detection requirements are component -specific and can be located as requirements for each specific device type in Clauses 12 through 15.		
7.14	**CR 3.12 – Provisioning product supplier roots of trust**		
	The provisioning product supplier roots of trust requirements are component -specific and can be located as requirements for each specific device type in Clauses 12 through 15.		
7.15	**CR 3.13 – Provisioning asset owner roots of trust**		
	The provisioning asset owner roots of trust requirements are component -specific and can be located as requirements for each specific device type in Clauses 12 through 15.		
7.16	**CR 3.14 – Integrity of the boot process**		
	The integrity of the boot process requirements are component-specific and can be located as requirements for each specific device type in Clauses 12 through 15.		

Annex 1 - Checklists for the verification of compliance to the "Guide for the certification of Cybersecurity capabilities of Marine materials and equipment"

Item	Requirement	Resul t	Notes
8	**FR 4 – Data confidentiality** **Purpose and SL-C(DC) descriptions** Ensure the confidentiality of information on communication channels and in data stored in repositories to protect against unauthorized disclosure. 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, OT systems 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, OT systems specific skills and high motivation.		
8.3	**CR 4.1 – Information integrity**		
8.3.1	**Requirement**		
	Components shall		
a)	provide the capability to protect the confidentiality of information at rest for which explicit read authorization is supported; and		
b)	support the protection of the confidentiality of information in transit as defined in ISA-62443-3-3 [11] SR 4.1.		
8.3.3	**Requirement enhancements**		
	None		
8.3.4	**Security levels**		
	The requirements for the four security levels that relate to CR 4.1 are:		
SL-C -1	CR 4.1		
SL-C-2	CR 4.1		
SL-C-3	CR 4.1		
SL-C-4	CR 4.1		
8.4	**CR 4.2 – Information persistence**		
8.4.1	**Requirement**		
	Components shall provide the capability to erase all information, for which explicit read authorization is supported, from components to be released from active service and/or decommissioned.		
8.4.3	**Requirement enhancements**		
(1)	Erase of shared memory resources Components shall provide the capability to protect against unauthorized and unintended information transfer via volatile shared memory resources.		

Annex 1 - Checklists for the verification of compliance to the "Guide for the certification of Cybersecurity capabilities of Marine materials and equipment"

Item	Requirement	Result	Notes
(2)	Erase verification Components shall provide the capability to verify that the erasure of information occurred.		
8.4.4	**Security levels**		
	The requirements for the four security levels that relate to CR 4.2 are:		
SL-C -1	Not Selected		
SL-C-2	CR 4.2		
SL-C-3	CR 4.2 (1) (2)		
SL-C-4	CR 4.2 (1) (2)		
8.5	**CR 4.3 – Use of cryptography**		
8.5.1	**Requirement**		
	If cryptography is required, the component shall use cryptographic security mechanisms according to internationally recognized and proven security practices and recommendations.		
8.5.3	**Requirement enhancements**		
	None		
8.5.4	**Security levels**		
	The requirements for the four security levels that relate to CR 4.3 are:		
SL-C -1	CR 4.3		
SL-C-2	CR 4.3		
SL-C-3	CR 4.3		
SL-C-4	CR 4.3		
9	**FR 5 – Restricted data flow** **Purpose and SL-C(RDF) descriptions** Segment the control system via zones and conduits to limit the unnecessary flow of data. SL 1 – Prevent the casual or coincidental circumvention of zone and conduit segmentation. SL 2 – Prevent the intended circumvention of zone and conduit segmentation by entities using simple means with low resources, generic skills and low motivation. SL 3 – Prevent the intended circumvention of zone and conduit segmentation by entities using sophisticated means with moderate resources, OT systems specific skills and moderate motivation. SL 4 – Prevent the intended circumvention of zone and conduit segmentation by entities using sophisticated means with extended resources, OT systems specific skills and high motivation.		
9.3	**CR 5.1 – Network segmentation**		
9.3.1	**Requirement**		
	Components shall support a segmented network to support zones and conduits, as needed, to support the		

Annex 1 - Checklists for the verification of compliance to the "Guide for the certification of Cybersecurity capabilities of Marine materials and equipment"

Item	Requirement	Result	Notes
	broader network architecture based on logical segment ation and criticality.		
9.3.3	**Requirement enhancements**		
	None		
9.3.4	**Security levels**		
	The requirements for the four security levels that relate to CR 5.1 are:		
SL-C -1	CR 5.1		
SL-C-2	CR 5.1		
SL-C-3	CR 5.1		
SL-C-4	CR 5.1		
9.4	**CR 5.2 – Zone boundary protection**		
	The zone boundary protection requirements are network-component-specific and can be located as requirements for network devices in Clause 15.		
9.5	**CR 5.3 – General-purpose person-to-person communication restrictions**		
	If cryptography is required, the component shall use cryptographic security mechanisms according to internationally recognized and proven security practices and recommendations.		
	CR 5.4 – Application partitioning		
	There is no component level requirement associated with ISA-62443-3-3 SR 5.4.		
10	**FR 6 – Timely response to events** **Purpose and SL-C(TRE) descriptions** Respond to security violations by notifying the proper authorities, reporting needed evidence of the violation and taking timely corrective action when incidents are discovered. SL 1 – Monitor the operation of the components of the OT systems, and respond to incidents when discovered, by collecting and providing the forensic evidence when queried. SL 2 – Monitor the operation of the components of the OT systems, and respond to incidents when discovered, by actively collecting and periodically reporting forensic evidence. SL 3 – Monitor the operation of the components of the OT systems, and respond to incidents when discovered, by actively collecting and pushing forensic evidence to the proper authorities. SL 4 – Monitor the operation of the components of the OT systems, and respond to incidents when discovered, by actively collecting and pushing forensic evidence to the proper authorities in near real-time.		
10.3	**CR 6.1 – Audit log accessibility**		
10.3.1	**Requirement**		
	Components shall provide the capability for authorized humans and/or tools to access audit logs on a read-only basis.		

Item	Requirement	Result	Notes
10.3.3	**Requirement enhancements**		
(1)	Programmatic access to audit logs Components shall provide programmatic access to audit records by either using an application programming interface (API) or sending the audit records to a centralized system		
10.3.4	**Security levels**		
	The requirements for the four security levels that relate to CR 4.1 are:		
SL-C -1	CR 6.1		
SL-C-2	CR 6.1		
SL-C-3	CR 6.1 (1)		
SL-C-4	CR 6.1 (1)		
10.4	**CR 6.2 – Continuous monitoring**		
10.4.1	**Requirement**		
	Components shall provide the capability to be continuously monitored using commonly accepted security industry practices and recommendations to detect, characterize and report security breaches in a timely manner.		
10.4.3	**Requirement enhancements**		
	None		
10.4.4	**Security levels**		
	The requirements for the four security levels that relate to CR 4.2 are:		
SL-C -1	Not Selected		
SL-C-2	CR 6.2		
SL-C-3	CR 6.2		
SL-C-4	CR 6.2		
11	**FR 7 – Resource availability** **Purpose and SL-C(DC) descriptions** Ensure the availability of components against the degradation or denial of essential services. SL 1 – Ensure that the component operates reliably under normal production conditions and prevents denial-of-service situations caused by the casual or coincidental actions of an entity. SL 2 – Ensure that the component operates reliably under normal and abnormal production conditions and prevents denial-of-service situations by entities using simple means with low resources, generic skills and low motivation. SL 3 – Ensure that the component operates reliably under normal, abnormal, and extreme production conditions and prevents denial-of-service situations by entities using sophisticated means with moderate resources, OT systems specific skills and moderate motivation. SL 4 – Ensure that the component operates reliably under normal, abnormal, and extreme production conditions and prevents denial-of-service situations by entities using		

Item	Requirement	Result	Notes
	sophisticated means with extended resources, OT systems specific skills and high motivation.		
11.3	**CR 7.1 – Denial of service protection**		
11.3.1	**Requirement**		
	Components shall provide the capability to maintain essential functions when operating in a degraded mode as the result of a DoS event.		
11.3.3	**Requirement enhancements**		
(1)	Manage communication load from component Components shall provide the capability to mitigate the effects of information and/or message flooding types of DoS events.		
11.3.4	**Security levels**		
	The requirements for the four security levels that relate to CR 4.1 are:		
SL-C -1	CR 7.1		
SL-C-2	CR 7.1 (1)		
SL-C-3	CR 7.1 (1)		□
SL-C-4	CR 7.1 (1)		□
11.4	**CR 7.2 – Resource management**		
11.4.1	**Requirement**		
	Components shall provide the capability to limit the use of resources by security functions to protect against resource exhaustion.		
11.4.3	**Requirement enhancements**		
	None		
11.4.4	**Security levels**		
	The requirements for the four SL levels that relate to CR 7.2 are:		
SL-C -1	CR 7.2		
SL-C-2	CR 7.2		
SL-C-3	CR 7.2		
SL-C-4	CR 7.2		
11.5	**CR 7.3 – Control system backup**		
11.5.1	**Requirement**		
	Components shall provide the capability to participate in system level backup operations in order to safeguard the component state (user- and system-level information). The backup process shall not affect the normal component operations.		
11.5.3	**Requirement enhancements**		
(1)	Backup integrity verification Components shall provide the capability to validate the integrity of backed up information prior to the initiation of a restore of that information.		

Item	Requirement	Result	Notes
11.5.4	**Security levels**		
	The requirements for the four SL levels that relate to CR 7.3 are:		
SL-C -1	CR 7.3		
SL-C-2	CR 7.3 (1)		
SL-C-3	CR 7.3 (1)		
SL-C-4	CR 7.3 (1)		
11.6	**CR 7.4 – Control system recovery and reconstitution**		
	Components shall provide the capability to be recovered and reconstituted to a known secure state after a disruption or failure.		
11.6.3	**Requirement enhancements**		
	None		
11.6.4	**Security levels**		
	The requirements for the four SL levels that relate to CR 7.4 are:		
SL-C -1	CR 7.4		
SL-C-2	CR 7.4		
SL-C-3	CR 7.4		
SL-C-4	CR 7.4		
11.7	**CR 7.5 - Emergency Power**		
	There is no component level requirement associated with ISA-62443-3-3 SR 7.5.		
11.8	**CR 7.6 – Network and security configuration settings**		
11.8.1	**Requirement**		
	Components shall provide the capability to be configured according to recommended network and security configurations as described in guidelines provided by the control system supplier. The component shall provide an interface to the currently deployed network and security configuration settings.		
11.8.3	**Requirement enhancements**		
(1)	Machine-readable reporting of current security settings Components shall provide the capability to generate a report listing the currently deployed security settings in a machine-readable format.		
11.8.4	**Security levels**		
	The requirements for the four security levels that relate to CR 7.6 are:		
SL-C -1	CR 7.6		
SL-C-2	CR 7.6		
SL-C-3	CR 7.6 (1)		□
SL-C-4	CR 7.6 (1)		□

Annex 1 - Checklists for the verification of compliance to the "Guide for the certification of Cybersecurity capabilities of Marine materials and equipment"

Item	Requirement	Result	Notes
11.9	**CR 7.7 – Least functionality**		
11.9.1	**Requirement**		
	Components shall provide the capability to specifically restrict the use of unnecessary functions, ports, protocols and/or services.		
11.9.3	**Requirement enhancements**		
	None		
11.9.4	**Security levels**		
	The requirements for the four SL levels that relate to CR 7.7 are:		
SL-C -1	CR 7.7		
SL-C-2	CR 7.7		
SL-C-3	CR 7.7		
SL-C-4	CR 7.7		
11.10	**CR 7.8 – Control system component inventory**		
11.10.1	**Requirement**		
	Components shall provide the capability to support a control system component inventory according to ISA-62443-3-3 [11] SR 7.8.		
11.10.3	**Requirement enhancements**		
	None		
11.10.4	**Security levels**		
	The requirements for the four SL levels that relate to CR 7.8 are:		
SL-C-1	Not Selected		
SL-C-2	CR 7.8		
SL-C-3	CR 7.8		
SL-C-4	CR 7.8		
12	**Software application requirements** **Purpose** The purpose of this set of requirements is to document requirements that are specific to software applications.		
12.2	**SAR 2.4 – Mobile code**		
12.2.1	**Requirement**		
	In the event that a software application utilizes mobile code technologies, that application shall provide the capability to enforce a security policy for the usage of mobile code technologies. The security policy shall allow, at a minimum, the following actions for each mobile code technology used on the software application:		
a)	Control execution of mobile code;		
b)	Control which users (human, software process, or device) are allowed to transfer mobile code to/from the application;		

Annex 1 - Checklists for the verification of compliance to the "Guide for the certification of Cybersecurity capabilities of Marine materials and equipment"

Item	Requirement	Result	Notes
c)	Control the execution of mobile code based on the results of an integrity check prior to the code being executed.		
12.2.3	**Requirement enhancements**		
(1)	Mobile code authenticity check The application shall provide the capability to enforce a security policy that allows the device to control execution of mobile code based on the results of an authenticity check prior to the code being executed.		
12.2.4	**Security levels**		
	The requirements for the four SL levels that relate to SAR 2.4 are:		
SL-C-1	SAR 2.4		
SL-C-2	SAR 2.4 (1)		
SL-C-3	SAR 2.4 (1)		
SL-C-4	SAR 2.4 (1)		
12.3	**SAR 3.2 – Protection from malicious code**		
12.3.1	**Requirement**		
	The application product supplier shall qualify and document which protection from malicious code mechanisms are compatible with the application and note any special configuration requirements.		
12.3.3	**Requirement enhancements**		
	None		
12.3.4	**Security levels**		
	The requirements for the four SL levels that relate to SAR 3.2 are:		
SL-C-1	SAR 3.2		
SL-C-2	SAR 3.2		
SL-C-3	SAR 3.2		
SL-C-4	SAR 3.2		
13	**Embedded device requirements** **Purpose** The purpose of this set of requirements is to document requirements that are specific to embedded devices.		
13.2	**EDR 2.4 – Mobile code**		
13.2.1	**Requirement**		
	In the event that an embedded device utilizes mobile code technologies, the embedded device shall provide the capability to enforce a security policy for the usage of mobile code technologies. The security policy shall allow, at a minimum, the following actions for each mobile code technology used on the embedded device:		
a)	Control execution of mobile code;		
b)	Control which users (human, software process, or device) are allowed to transfer mobile code to/from the application;		

Item	Requirement	Result	Notes
c)	Control the execution of mobile code based on the results of an integrity check prior to the code being executed.		
13.2.3	**Requirement enhancements**		
(1)	Mobile code authenticity check The embedded device shall provide the capability to enforce a security policy that allows the device to control execution of mobile code based on the results of an authenticity check prior to the code being executed		
13.2.4	**Security levels**		
	The requirements for the four SL levels that relate to SAR 2.4 are:		
SL-C-1	SAR 2.4		
SL-C-2	SAR 2.4 (1)		□
SL-C-3	SAR 2.4 (1)		□
SL-C-4	SAR 2.4 (1)		□
13.3	**EDR 2.13 – Use of physical diagnostic and test interfaces**		□
13.3.1	**Requirement**		
	Embedded devices shall protect against unauthorized use of the physical factory diagnostic and test interface(s) (e.g. JTAG Debugging).		
13.3.3	**Requirement enhancements**		
(1)	Active monitoring Embedded devices shall provide active monitoring of the device’s diagnostic and test interface(s) and generate an audit log entry when attempts to access these interface(s) are detected.		
13.3.4	**Security levels**		
	The requirements for the four SL levels that relate to EDR 2.13 are:		
SL-C-1	Not Selected		
SL-C-2	EDR 2.13		
SL-C-3	EDR 2.13 (1)		
SL-C-4	EDR 2.13 (1)		
13.4	**EDR 3.2 – Protection from malicious code**		
13.4.1	**Requirement**		
	The embedded device shall provide the capability to protect from installation and execution of unauthorized software.		
13.4.3	**Requirement enhancements**		
	None		
13.4.4	**Security levels**		
	The requirements for the four SL levels that relate to EDR 3.2 are:		
SL-C-1	EDR 3.2		

Item	Requirement	Resul t	Notes
SL-C-2	EDR 3.2		
SL-C-3	EDR 3.2		
SL-C-4	EDR 3.2		
13.5	**EDR 3.10 – Support for updates**		**1.5**
13.5.1	**Requirement**		
	The embedded device shall support the ability to be updated and upgraded.		
13.5.3	**Requirement enhancements**		
(1)	Update authenticity and integrity The embedded device shall validate the authenticity and integrity of any software update or upgrade prior to installation.		
13.5.4	**Security levels**		
	The requirements for the four SL levels that relate to EDR 3.10 are:		
SL-C-1	EDR 3.10		
SL-C-2	EDR 3.10 (1)		
SL-C-3	EDR 3.10 (1)		
SL-C-4	EDR 3.10 (1)		□
13.6	**EDR 3.11 – Physical tamper resistance and detection**		
13.6.1	**Requirement**		
	The embedded device shall provide tamper resistance and detection mechanisms to protect against unauthorized physical access into the device		
13.6.3	**Requirement enhancements**		
(1)	Notification of a tampering attempt The embedded device shall be capable of automatically providing notification to a configurable set of recipients upon discovery of an attempt to make an unauthorized physical access. All notifications of tampering shall be logged as part of the overall audit logging function.		
13.6.4	**Security levels**		
	The requirements for the four SL levels that relate to EDR 3.11 are:		
SL-C-1	Not Selected		
SL-C-2	EDR 3.11		
SL-C-3	EDR 3.11 (1)		□
SL-C-4	EDR 3.11 (1)		□
13.7	**EDR 3.12 – Provisioning product supplier roots of trust**		
13.7.1	**Requirement**		
	Embedded devices shall provide the capability to provision and protect the confidentiality, integrity, and authenticity of product supplier keys and data to be used as one or more “roots of trust” at the time of manufacture of the device.		

Item	Requirement	Resul t	Notes
13.7.3	**Requirement enhancements**		
	None		
13.7.4	**Security levels**		
	The requirements for the four SL levels that relate to EDR 3.12 are:		
SL-C-1	Not Selected		
SL-C-2	EDR 3.12		
SL-C-3	EDR 3.12		
SL-C-4	EDR 3.12		
13.8	**EDR 3.13 – Provisioning asset owner roots of trust**		
13.8.1	**Requirement**		
	Embedded devices shall		
a)	provide the capability to provision and protect the confidentiality, integrity, and authenticity of asset owner keys and data to be used as "roots of trust"; and		
b)	support the capability to provision without reliance on components that may be outside of the device's security zone.		
13.8.3	**Requirement enhancements**		
	None		
13.8.4	**Security levels**		
	The requirements for the four SL levels that relate to EDR 3.13 are:		
SL-C-1	Not Selected		
SL-C-2	EDR 3.13		
SL-C-3	EDR 3.13		
SL-C-4	EDR 3.13		
13.9	**EDR 3.14 – Integrity of the boot process**		
13.9.1	**Requirement**		
	Embedded devices shall verify the integrity of the firmware, software, and configuration data needed for the component's boot and runtime processes prior to use.		
13.9.3	**Requirement enhancements**		
(1)	Authenticity of the boot process Embedded devices shall use the component's product supplier roots of trust to veri fy the authenticity of the firmware, software, and configuration data needed for the component's boot process prior to it being used in the boot process.		
13.9.4	**Security levels**		
	The requirements for the four SL levels that relate to EDR 3.14 are:		
SL-C-1	EDR 3.14		
SL-C-2	EDR 3.14 (1)		

Annex 1 - Checklists for the verification of compliance to the "Guide for the certification of Cybersecurity capabilities of Marine materials and equipment"

Item	Requirement	Result	Notes
SL-C-3	EDR 3.14 (1)		
SL-C-4	EDR 3.14 (1)		
14	**Host device requirements** **Purpose** The purpose of this set of requirements is to document requirements that are specific to host devices.		
14.2	**HDR 2.4 – Mobile code**		
14.2.1	**Requirement**		
	In the event that a host device utilizes mobile code technologies, that host device shall provide the capability to enforce a security policy for the usage of mobile code technologies. The security policy shall allow, at a minimum, the following actions for each mobile code technology used on the host device:		
a)	Control execution of mobile code;		
b)	Control which users (human, software process, or device) are allowed to transfer mobile code to/from the application; and		
c)	Control the execution of mobile code based on the results of an integrity check prior to the code being executed.		
14.2.3	**Requirement enhancements**		
(1)	Mobile code authenticity checks The host device shall provide the capability to enforce a security policy that allows the device to control execution of mobile code based on the results of an authenticity check prior to the code being executed.		
14.2.4	**Security levels**		
	The requirements for the four SL levels that relate to HDR 2.4 are:		
SL-C-1	HDR 2.4		
SL-C-2	HDR 2.4 (1)		
SL-C-3	HDR 2.4 (1)		□
SL-C-4	HDR 2.4 (1)		□
14.3	**HDR 2.13 – Use of physical diagnostic and test interfaces**		□
14.3.1	**Requirement**		□
	Host devices shall protect against unauthorized use of the physical factory diagnostic and test interface(s) (e.g. JTAG debugging).		
14.3.3	**Requirement enhancements**		
(1)	Active monitoring Host devices shall provide active monitoring of the device's diagnostic and test interface(s) and generate an audit log entry when attempts to access these interface(s) are detected.		
14.3.4	**Security levels**		
	The requirements for the four SL levels that relate to HDR 2.13 are:		

Item	Requirement	Result	Notes
SL-C-1	Not Selected		
SL-C-2	HDR 2.13		
SL-C-3	HDR 2.13 (1)		□
SL-C-4	HDR 2.13 (1)		□
14.4	**HDR 3.2 – Protection from malicious code**		□
14.4.1	**Requirement**		□
	There shall be mechanisms on host devices that are qualified by the OT systems product supplier to provide protection from malicious code. The OT systems product supplier shall document any special configuration requirements related to protection from malicious code.		
14.4.3	**Requirement enhancements**		
(1)	Report version of code protection The host device shall automatically report the software and file versions of protection from malicious code in use (as part of overall logging function).		
14.4.4	**Security levels**		
	The requirements for the four SL levels that relate to HDR 3.2 are:		
SL-C-1	HDR 3.2		
SL-C-2	HDR 3.2 (1)		
SL-C-3	HDR 3.2 (1)		
SL-C-4	HDR 3.2 (1)		
14.5	**HDR 3.10 – Support for updates**		
14.5.1	**Requirement**		
	Host devices shall support the ability to be updated and upgraded.		□
14.5.3	**Requirement enhancements**		□
(1)	Update authenticity and integrity Host devices shall validate the authenticity and integrity of any software update or upgrade prior to installation.		
14.5.4	**Security levels**		
	The requirements for the four SL levels that relate to HDR 3.10 are:		
SL-C-1	HDR 3.10		
SL-C-2	HDR 3.10 (1)		
SL-C-3	HDR 3.10 (1)		
SL-C-4	HDR 3.10 (1)		
14.6	**HDR 3.11 – Physical tamper resistance and detection**		
14.6.1	**Requirement**		
	Host devices shall provide the capability to support tamper resistance and detection mechanisms to protect against unauthorized physical access into the device.		

Item	Requirement	Result	Notes
14.6.3	**Requirement enhancements**		
(1)	Notification of a tampering attempt Host devices shall be capable of automatically providing notification to a configurable set of recipients upon discovery of an attempt to make an unauthorized physical access. All notifications of tampering shall be logged as part of the overall audit logging function.		
14.6.4	**Security levels**		
	The requirements for the four SL levels that relate to HDR 3.11 are:		
SL-C-1	Not Selected		□
SL-C-2	HDR 3.11		□
SL-C-3	HDR 3.11 (1)		□
SL-C-4	HDR 3.11 (1)		□
14.7	**HDR 3.12 – Provisioning product supplier roots of trust**		
14.7.1	**Requirement**		
	Host devices shall provide the capability to provision and protect the confidentiality, integrity, and authenticity of product supplier keys and data to be used as one or more “roots of trust” at the time of manufacture of the device.		
14.7.3	**Requirement enhancements**		
	None		
14.7.4	**Security levels**		
	The requirements for the four SL levels that relate to HDR 3.12 are:		
SL-C-1	Not Selected		
SL-C-2	HDR 3.12		
SL-C-3	HDR 3.12		
SL-C-4	HDR 3.12		
14.8	**HDR 3.14 – Provisioning asset owner roots of trust**		
14.8.1	**Requirement**		
	Embedded devices shall		
a)	provide the capability to provision and protect the confidentiality, integrity, and authenticity of asset owner keys and data to be used as “roots of trust”; and		
b)	support the capability to provision without reliance on components that may be outside of the device’s security zone.		
14.8.3	**Requirement enhancements**		
	None		
14.8.4	**Security levels**		
	The requirements for the four SL levels that relate to HDR 3.14 are:		
SL-C-1	Not Selected		

Annex 1 - Checklists for the verification of compliance to the “Guide for the certification of Cybersecurity capabilities of Marine materials and equipment”

Item	Requirement	Result	Notes
SL-C-2	HDR 3.14		
SL-C-3	HDR 3.14		
SL-C-4	HDR 3.14		
14.9	**HDR 3.14 – Integrity of the boot process**		
14.9.1	**Requirement**		
	Host devices shall verify the integrity of the firmware, software, and configuration data needed for component’s boot process prior to it being used in the boot process.		
14.9.3	**Requirement enhancements**		
(1)	Authenticity of the boot process Host devices shall use the component’s product supplier roots of trust to verify the authenticity of the firmware, software, and configuration data needed for component’s boot process prior to it being used in the boot process.		
14.9.4	**Security levels**		
	The requirements for the four SL levels that relate to HDR 3.14 are:		
SL-C-1	HDR 3.14		
SL-C-2	HDR 3.14 (1)		
SL-C-3	HDR 3.14 (1)		
SL-C-4	HDR 3.14 (1)		
15	**Network device requirements** **Purpose** The purpose of this set of requirements is to document requirements that are specific to network devices.		
15.2	**NDR 1.6 – Wireless access management**		
15.2.1	**Requirement**		
	A network device supporting wireless access management shall provide the capability to identify and authenticate all users (humans, software processes or devices) engaged in wireless communication.		
15.2.3	**Requirement enhancements**		
(1)	Unique identification and authentication The network device shall provide the capability to uniquely identify and authenticate all users (humans, software processes or devices) engaged in wireless communication.		
15.2.4	**Security levels**		
	The requirements for the four SL levels that relate to NDR 1.6 are:		
SL-C-1	NDR 1.6		
SL-C-2	NDR 1.6 (1)		□
SL-C-3	NDR 1.6 (1)		
SL-C-4	NDR 1.6 (1)		

Annex 1 - Checklists for the verification of compliance to the "Guide for the certification of Cybersecurity capabilities of Marine materials and equipment"

Item	Requirement	Resul t	Notes
15.3	**NDR 1.13 – Access via untrusted networks**		
15.3.1	**Requirement**		
	The network device supporting device access into a network shall provide the capability to monitor and control all methods of access to the network device via untrusted networks.		
15.3.3	**Requirement enhancements**		
(1)	Explicit access request approval The network device shall provide the capability to deny access requests via untrusted networks unless explicitly approved by an assigned role.		
15.3.4	**Security levels**		
	The requirements for the four SL levels that relate to NDR 1.13 are:		
SL-C-1	NDR 1.13		
SL-C-2	NDR 1.13		
SL-C-3	NDR 1.13 (1)		
SL-C-4	NDR 1.13 (1)		
15.4	**NDR 2.4 – Mobile code**		
15.4.1	**Requirement**		
	In the event that a network device utilizes mobile code technologies, the network device shall provide the capability to enforce a security policy for the usage of mobile code technologies. The security policy shall allow, at a minimum, the following actions for each mobile code technology used on the network device:		
a)	Control execution of mobile code;		
b)	Control which users (human, software process, or device) are allowed to transfer mobile code to/from the network device; and		
c)	Control the code execution based upon integrity checks on mobile code and prior to the code being executed		
15.4.3	**Requirement enhancements**		
(1)	Mobile code authenticity check The network device shall provide the capability to enforce a security policy that allows the device to control execution of mobile code based on the results of an authenticity check prior to the code being executed.		
15.4.4	**Security levels**		
	The requirements for the four SL levels that relate to NDR 2.4 are:		
SL-C-1	NDR 2.4		
SL-C-2	NDR 2.4 (1)		
SL-C-3	NDR 2.4 (1)		
SL-C-4	NDR 2.4 (1)		

Item	Requirement	Result	Notes
15.5	**NDR 2.13 – Use of physical diagnostic and test interfaces**		
15.5.1	**Requirement**		
	Network devices shall protect against unauthorized use of the physical factory diagnostic and test interface(s) (e.g. JTAG debugging).		
15.5.3	**Requirement enhancements**		
(1)	Active monitoring Network devices shall provide active monitoring of the device’s diagnostic and test interface(s) and generate an audit log entry when attempts to access these interface(s) are detected.		
15.5.4	**Security levels**		
	The requirements for the four SL levels that relate to NDR 2.13 are:		
SL-C-1	Not Selected		
SL-C-2	NDR 2.13		
SL-C-3	NDR 2.13 (1)		□
SL-C-4	NDR 2.13 (1)		□
15.6	**NDR 3.2 – Protection from malicious code**		
15.6.1	**Requirement**		
	The network device shall provide for protection from malicious code.		
15.6.3	**Requirement enhancements**		
	None		
15.6.4	**Security levels**		
	The requirements for the four SL levels that relate to NDR 3.2 are:		
SL-C-1	NDR 3.2		
SL-C-2	NDR 3.2		
SL-C-3	NDR 3.2		
SL-C-4	NDR 3.2		□
15.7	**NDR 3.10 – Support for updates**		
15.7.1	**Requirement**		
	Network devices shall support the ability to be updated and upgraded.		
15.7.3	**Requirement enhancements**		
(1)	Update authenticity and integrity Network devices shall validate the authenticity and integrity of any software update or upgrade prior to installation.		
15.7.4	**Security levels**		
	The requirements for the four SL levels that relate to NDR 3.10 are:		
SL-C-1	NDR 3.10		

Annex 1 - Checklists for the verification of compliance to the "Guide for the certification of Cybersecurity capabilities of Marine materials and equipment"

Item	Requirement	Result	Notes
SL-C-2	NDR 3.10 (1)		
SL-C-3	NDR 3.10 (1)		
SL-C-4	NDR 3.10 (1)		
15.8	**NDR 3.11 – Physical tamper resistance and detection**		
15.8.1	**Requirement**		
	Network devices shall provide tamper resistance and detection mechanisms to protect against unauthorized physical access into the device		
15.8.3	**Requirement enhancements**		
(1)	Notification of a tampering attempt Network devices shall be capable of automatically providing notification to a configurable set of recipients upon discovery of an attempt to make an unauthorized physical access. All notifications of tampering shall be logged as part of the overall audit logging function.		
15.8.4	**Security levels**		
	The requirements for the four SL levels that relate to NDR 3.11 are:		
SL-C-1	Not Selected		
SL-C-2	NDR 3.11		
SL-C-3	NDR 3.11 (1)		
SL-C-4	NDR 3.11 (1)		
15.9	**NDR 3.12 – Provisioning product supplier roots of trust**		
15.9.1	**Requirement**		
	Network devices shall provide the capability to provision and protect the confidentiality, integrity, and authenticity of product supplier keys and data to be used as one or more "roots of trust" at the time of manufacture of the device.		
15.9.3	**Requirement enhancements**		
	None		
15.9.4	**Security levels**		
	The requirements for the four SL levels that relate to NDR 3.12 are:		
SL-C-1	Not Selected		
SL-C-2	NDR 3.12		
SL-C-3	NDR 3.12		
SL-C-4	NDR 3.12		
15.10	**NDR 3.13 – Provisioning asset owner roots of trust**		
15.10.1	**Requirement**		
	Network devices shall		
a)	provide the capability to provision and protect the confidentiality, integrity, and authenticity of asset owner keys and data to be used as "roots of trust"; and		

Annex 1 - Checklists for the verification of compliance to the “Guide for the certification of Cybersecurity capabilities of Marine materials and equipment”

Item	Requirement	Result	Notes
b)	support the capability to provision without reliance on components that may be outside of the device’s security zone.		
15.10.3	**Requirement enhancements**		
	None		
15.10.4	**Security levels**		
	The requirements for the four SL levels that relate to NDR 3.13 are:		
SL-C-1	Not Selected		
SL-C-2	NDR 3.13		
SL-C-3	NDR 3.13		
SL-C-4	NDR 3.13		
15.11	**NDR 3.14 – Integrity of the boot process**		
15.11.1	**Requirement**		
	Network devices shall verify the integrity of the firmware, software, and configuration data needed for component’s boot process prior to it being used in the boot process.		
15.11.3	**Requirement enhancements**		
(1)	Authenticity of the boot process Network devices shall use the component’s product supplier roots of trust to verity the authenticity of the firmware, software, and configuration data needed for component’s boot process prior to it being used in the boot process.		
15.11.4	**Security levels**		
	The requirements for the four SL levels that relate to NDR 3.14 are:		
SL-C-1	NDR 3.14		
SL-C-2	NDR 3.14 (1)		
SL-C-3	NDR 3.14 (1)		□
SL-C-4	NDR 3.14 (1)		□
15.12	**NDR 3.14 – Integrity of the boot process**		
15.12.1	**Requirement**		
	Network devices shall verify the integrity of the firmware, software, and configuration data needed for component’s boot process prior to it being used in the boot process.		
15.12.3	**Requirement enhancements**		
(1)	Deny all, permit by exception The network component shall provide the capability to deny network traffic by default and allow network traffic by exception (also termed deny all, permit by exception).		
(2)	Island mode The network component shall provide the capability to protect against any communication through the control system boundary (also termed island mode).		

Item	Requirement	Result	Notes
(3)	Fail close The network component shall provide the capability to protect against any communication through the control system boundary when there is an operational failure of the boundary protection mechanisms (also termed fail close).		
15.12.4	**Security levels**		
	The requirements for the four SL levels that relate to NDR 5.2 are:		
SL-C-1	NDR 5.2		□
SL-C-2	NDR 5.2 (1)		□
SL-C-3	NDR 5.2 (1) (2) (3)		□
SL-C-4	NDR 5.2 (1) (2) (3)		□
15.13	**NDR 5.3 – General purpose, person-to-person communication restrictions**		
15.13.1	**Requirement**		
	A network device at a zone boundary shall provide the capability to protect against general purpose, person-to-person messages from being received from users or systems external to the control system.		
15.13.3	**Requirement enhancements**		
	None		
15.13.4	**Security levels**		
	The requirements for the four SL levels that relate to NDR 5.3 are:		
SL-C-1	NDR 5.3		
SL-C-2	NDR 5.3		□
SL-C-3	NDR 5.3		□
SL-C-4	NDR 5.3		□

Annex 2 – Format of Statement of Compliance

Tasneef
هيئة الإمارات للتصنيف
Emirates Classification Society

STATEMENT OF COMPLIANCE

No.

We state that the following device/product is in compliance with Tasneef “Guide for the certification of Cybersecurity capabilities of Marine materials and equipment”

Description
Type
Applicant
Manufacturer
Reference standards
Reference documents

The validity of this Statement is subject to the maintenance of the initial product conditions verified by Tasneef . Any change to initial conditions must be communicated to Tasneef which reserves the right to carry out further verification in order to confirm the validity of this Statement.

Issued at on

This statement is valid until

Insert full name of signing person

____
Tasneef

The rules, surveys and activities performed by Tasneef, reports, certificates and other documents issued by Tasneef are in no way intended to replace the duties and responsibilities of other parties such as Governments, designers, ship builders, manufacturers, repairers, suppliers, contractors or sub-contractors, owners, operators, charterers, underwriters, sellers or intended buyers of a ship or other product or system surveyed.
These documents and activities do not relieve such parties from any fulfillment, warranty, responsibility, duty or obligation (also of a contractual nature) expressed or implied or in any case incumbent on them according to the law, nor do they confer on such parties any right, claim or cause of action against Tasneef. With particular regard to the duties of the ship Owner, the services undertaken by Tasneef do not relieve the Owner of his duty to ensure at all times proper maintenance of the ship and seaworthiness. Likewise, the rules, surveys performed, reports, certificates and other documents issued by Tasneef are intended neither to guarantee the buyers of the ship, its components or any other surveyed or certified item, nor to relieve the seller of the duties arising out of the law or the contract, regarding the quality, commercial value or characteristics of the item which is the subject of transaction.
In providing the services, as well as other correlated information or advice, Tasneef, its surveyors, servants or agents operate with due diligence for the proper execution of the activity. However, considering the nature of the activities performed (see art. 2.4 of the General Conditions), it is not possible to guarantee absolute accuracy, correctness and completeness of any information or advice supplied. Therefore, express and implied warranties are specifically disclaimed.
In providing its services, and also in the case of activities carried out by delegation of Governments, neither Tasneef nor any of its surveyors will be liable for any loss, damage or expense of whatever nature sustained by any person, in tort or in contract, derived from carrying out the services.
However, should any user of Tasneef services prove that he has suffered a loss or damage due to any negligent act or omission of Tasneef, its surveyors, servants or agents, then Tasneef will pay compensation to such person for his proved loss, up to, but not exceeding, five times the amount of the fees charged for the specific services, information or opinions from which the loss or damage derives or, if no fee has been charged, a maximum of one hundred thousand Euro.
Any liability for indirect or consequential loss, damage or expense is specifically excluded. In any case, irrespective of the amount of the fees charged, the maximum damages payable by Tasneef will not be more than 1 million Euro.
No report, statement, notation on a plan, review, class certificate, document or information issued or given as part of the services provided by Tasneef shall have any legal effect or implication other than a representation that, on the basis of the checks made by Tasneef, the ship, structure, materials, equipment, machinery or any other item covered by such document or information meet the rules issued by Tasneef. Therefore, Tasneef cannot be held liable for any act made or document issued by other parties on the basis of the statements or information given by Tasneef.

Enclosures

Product description

Test carried out

Field of Application