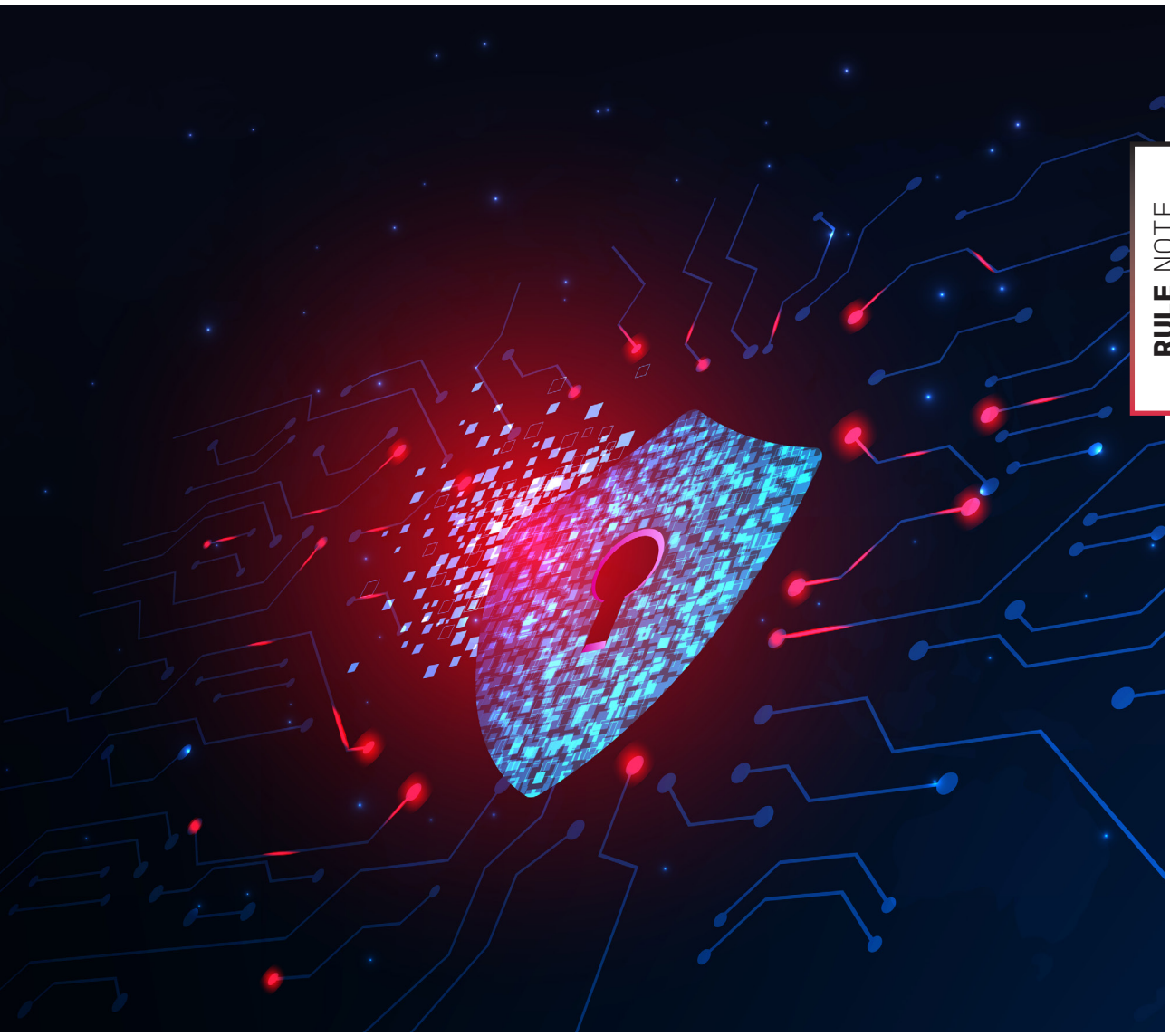
NR659 DT R03 JANUARY 2024

RULES ON CYBER SECURITY FOR THE CLASSIFICATION OF MARINE UNITS

NR659 - JANUARY 2024



RULE NOTE

BUREAU VERITAS

BUREAU VERITAS
RULES, RULE NOTES AND GUIDANCE NOTES

NR659 DT R03 January 2024 takes precedence over previous revision.

The PDF electronic version of this document available on the Bureau Veritas Marine & Offshore website https://marine-offshore.bureauveritas.com/ is the official version and shall prevail if there are any inconsistencies between the PDF version and any other available version.

These rules are provided within the scope of the Bureau Veritas Marine & Offshore General Conditions, enclosed at the end of Part A of NR467, Rules for the Classification of Steel Ships. The latest version of these General Conditions is available on the Bureau Veritas Marine & Offshore website.

BUREAU VERITAS MARINE & OFFSHORE

Tour Alto
4 place des Saisons
92400 Courbevoie - France
+33 (0)1 55 24 70 00

marine-offshore.bureauveritas.com/rules-guidelines

NR659

RULES ON CYBER SECURITY FOR THE CLASSIFICATION OF MARINE UNITS

January 2024

Table of Content

Table of Content

Table of Content

Chapter 4 Additional Class Notation CYBER SECURE

Section 1 CYBER SECURE Notation

Section 2 On Board to On Shore Connections

Section 3 Ship Networks

Section 4 Operational Technologies Interconnections

Table of Content

Chapter 6 Survey Operations

Section 1 General

Section 2 Monitoring Procedures Survey

Section 3 Checking Infrastructure Cybersecurity

Section 4 Equipment Survey

Section 5 Checking Maintenance Procedures

Table of Content

CHAPTER 1
GENERAL PRINCIPLES

Section 1 General Requirements

1 Scope and application

1.1 General

1.1.1 Application

These rules apply to design, construction, installation and maintenance of Computer Based System (CBS) which rely on software for the achievement of their functions. The requirements focus on the functionality of the software and on the hardware supporting the software. These requirements apply to the use of IT (Information Technologies) and OT (Operational Technologies), see [2.3.2], item g), CBSs which provide, communicate or transport control, alarm, monitoring, safety or internal communication functions which are subject to classification requirements.

In addition, the Shipowner may specify other IT or OT systems to be included in the scope of the classification.

These rules apply to either new ships or existing ships as detailed in [1.2].

1.1.2 Assignment and maintenance of a classification notation

A ship may be assigned one of the following additional class notations, as defined in [1.2]:

- **CYBER MANAGED** when found in compliance with the requirements of Chapter 2
- **CYBER RESILIENT**, when found in compliance with the requirements of Chapter 3
- **CYBER SECURE** when found in compliance with the requirements of Chapter 4.

The scope of surveys and the requirements to be complied with for the maintenance of the additional class notations **CYBER MANAGED** and **CYBER SECURE** are detailed in Chapter 6.

The scope of surveys and the requirements to be complied with for the maintenance of the additional class notation **CYBER RESILIENT** are detailed in Ch 3, Sec 2, [10.4] and Chapter 6.

1.1.3 Type Approval of equipment and systems

The certification requirements for equipment and system are detailed in Chapter 5.

1.2 Classification notations

1.2.1 General

The following additional class notations may be assigned, as applicable, to ships fitted with equipment and networks which comply with the requirements of this Rule Note:

- The additional class notation **CYBER MANAGED**, defined in [1.2.2] may be assigned to existing ships only (**CYBER MANAGED** applies when a crew is on board).
- The additional class notation **CYBER RESILIENT**, defined in [1.2.3], may be assigned to new ships and existing ships.
- The additional class notation **CYBER SECURE**, defined in [1.2.4], may be assigned to new ships and existing ships.

1.2.2 CYBER MANAGED

The additional class notation **CYBER MANAGED** corresponds to a first level of cyber security for existing ships only. It requires human awareness, human organization and procedures.

Note 1: Requirements for the additional class notation **CYBER MANAGED** seeks to support IMO Resolution MSC.428(98) (June 2017): "Maritime Cyber Risk Management in Safety Management Systems", which requires cyber-risks to be addressed in safety management systems by 1 January 2021, based on MSCFAL.1/Circ.3 (June 2017): "Guidelines on Maritime Cyber Risk Management".

The additional class notation **CYBER MANAGED** corresponds to compliance with a set of requirements defined in Chapter 2 and dealing with:

- critical equipment
- cyber management (policy and procedures)
- crew training.

1.2.3 CYBER RESILIENT

The additional class notation **CYBER RESILIENT** may be assigned to ships complying with the requirements defined in Chapter 3 regarding ships resilience when dealing with cyber-attacks.

The additional class notation **CYBER SECURE** is completed with a construction mark in accordance with NR467 Rules for the Classification of Steel Ships, Pt A, Ch 1, Sec 2, [6.1.3].

1.2.4 CYBER SECURE

The additional class notation **CYBER SECURE** is defined for ships secured by design.

Note 1: Ships assigned the additional class notation **CYBER SECURE** comply with the requirements specified for the additional class notation **CYBER RESILIENT**.

For new ships, the requirements for the additional class notation **CYBER SECURE** are defined in Chapter 4 and dealing with:

- OT/IT ship architecture secured by design
- equipment hardening.

The additional class notation **CYBER SECURE** is completed with a construction mark in accordance with Ch 4, Sec 1, [1.1.3] and NR467 Rules for the Classification of Steel Ships, Pt A, Ch 1, Sec 2, [6.1.3].

2 Definitions

2.1 Global terms

2.1.1 The following general terms are used within this Rule Note:

a) Society means the Classification Society with which the ship is classed

b) Ship Rules includes Rules for the Classification of Steel Ships (NR467) as well as documents issued by the Society serving the same purpose

c) Surveyor means technical staff acting on behalf of the Society to perform tasks in relation to classification and survey duties

d) Survey means an intervention by the Surveyor for assignment or maintenance of class as defined in Chapter 6, or interventions by the Surveyor within the limits of the tasks delegated by the Administrations

e) Approval means the review by the Society of documents, procedures or other items related to classification, verifying solely their compliance with the relevant Rules.

2.2 Roles

2.2.1 The definitions in [2.2.2] to [2.2.8] are used in this Rule Note to describe roles and responsibilities.

2.2.2 Master

The Master is in ultimate command of the ship. The Master is responsible for safe and efficient cyber operations of the ship.

2.2.3 Cyber security officer

The cyber security officer is the head of IT and OT security, driving the IT and OT security strategy and implementation forward whilst protecting the Shipowner from security threats and cyber-hacking. Operational compliance to standards and regulations is the responsibility of the cyber security officer. This is a senior role and will commonly involve directing a team and taking a seat on the management board. The cyber security officer is appointed by the Shipowner and his responsibilities are described in the Cyber Security Policy.

2.2.4 Cyber security responsible

The cyber security responsible is, aboard, the officer responsible for establishing and maintaining the compliance with the class notation requirements. This includes the entire scope of cyber security access controls, procedures application, registry consistency, documentation updates, events detection, emergency responses, change management and follow-up indicators. For example this role could be held by the Chief Engineer after being trained or certified. The cyber security responsible is appointed by the Shipowner and his responsibilities are described in the Cyber Security Policy.

2.2.5 Shipowner

The Shipowner is responsible for contracting the ship and owns the systems at ship delivery. After ship delivery, the Shipowner may delegate some responsibilities to the ship operating company.

2.2.6 Shipyard

The Shipyard is responsible for systems installation and all the documents to be delivered from the shipyard regarding the systems identification and design assessment.

2.2.7 System integrator

For new construction, the system integrator is in charge of the cyber security. He is responsible for the integration of systems and equipment ordered by both Shipyard and Shipowner. The system integrator is to be nominated by the Shipyard and introduced to the Society with which he is to stay in contact until the commissioning of the ship. The scope of his responsibilities covers OT, IT and computer networks. If there are multiple parties proposing pre-integrated systems (as many OT Suppliers generally do), the system integrator must pay attention to connections, compatibilities, network tunnels, remote accesses, vulnerability monitoring and equipment approvals. In accordance with the risk assessment he has the authority to accept or refuse equipment, a connection or a software. The system integrator shall coordinate operations during the first stages of the ship's life: from design to commissioning.

2.2.8 Supplier

The supplier is any contracted or subcontracted provider of system components or equipment (hardware or software). The supplier is responsible for providing programmable devices, sub-systems or systems to the Shipyard.

2.3 Systems and equipment - terms and abbreviations

2.3.1 Abbreviations/ acronyms

APT : Advanced Persistent Threat
CSR : Compliance and Software Registry
DMZ : Demilitarized Zone
ELR : Events and Logs Recorder
HTTP : Hypertext Transfer Protocol
HTTPS : Hypertext Transfer Protocol Secure
ICS : Industrial Control Systems
IDG : Inspection and Decontamination Gate
IDS : Intrusion Detection System
IP : Internet Protocol
IPS : Intrusion Prevention System
IPSec : Internet Protocol Security
MAC : Media Access Control Address
NGFW : New Generation Firewall
OSI : Open Systems Interconnection model
PLC : Programmable Logic Controller
SNMP : Simple Network Management Protocol
SPI : State-full Packet Inspection
SSH : Secure Shell
SSL : Secure Sockets Layer
TCP : Transmission Control Protocol
VLAN : Virtual Local Area Network
VPN : Virtual Private Networks
WPA : Wi-Fi Protected Access.

2.3.2 Aboard equipment

Aboard equipment refers to any IT and OT systems and equipment installed on the ship.

2.3.3 Administration workstation

Administration workstations are industrial systems (OT) of Category A (Cat. A) dedicated to administration of industrial systems, servers, firewalls, switches, etc.

2.3.4 Ashore equipment

Ashore equipment refers to systems and equipment not present on the ship but used from on ground premises to communicate, monitor or control on-board systems and equipment, including airtime providers intermediate equipment.

2.3.5 Category of equipment (Cat. A, Cat. B or Cat. C)

Categories (Cat. A, Cat. B or Cat. C) define the nature of the equipment:

- Cat. A are equipment operated thanks to a standard operating system like Windows, Linux, Android or macOS. For example, Cat. A are servers, virtual machines, calculators, blade servers, workstations, terminals, tablets, smartphones and, generally, any endpoint.

  Cat. A equipment used into OT systems (Operational Technology) are inventoried and labelled in one of the three following categories:
  - engineering workstation (mostly stationary computers dedicated to industrial system process engineering)
  - operator console (mostly mobile systems involved in industrial system process engineering and maintenance)
  - administration workstation (dedicated to administration of industrial system, servers, firewalls, switches, etc.)
- Cat. B are equipment operated thanks to a dedicated operating system, linked to a dedicated firmware, under the form of a specific appliance. Examples of Cat. B equipment could be network equipment for TCP/IP routing, firewalls or network security equipment.
- Cat. C are industrial automation and control systems (IACS) operated thanks to a firmware. Cat C examples are programmable devices (DCS, PLC, SCADA) or Safety Instrumented Systems (SIS).

In this document, we will refer to Category with the following wording: Cat. A, Cat. B or Cat. C.

2.3.6 Engineering workstation

Engineering workstations are industrial systems (OT) of Category A (Cat. A) mostly stationary computers dedicated to industrial system process engineering.

2.3.7 Equipment

Equipment is part of a system, which may perform a specific function or a set of functions. Equipment may be software only, hardware only or a combination of both. Equipment may be a computer, a laptop, an automation, a programmable logic controller, a software, a virtual environment with networks and software, a network firewall, a physical switch, a diode, a connected object or a mobile phone, etc. In this document, the word equipment will be exclusively considered.

2.3.8 Hardening of a system

Hardening of a system means the process of securing a system by reducing its surface of attack, which is larger when a system performs more functions; in principle a single-function system is more secure than a multi-purpose one. Reducing available ways of attack typically includes changing default passwords, the removal of unnecessary software, unnecessary user names or logins, and the disabling or removal of unnecessary services.

2.3.9 Industrial system

Industrial systems are known as using OT (Operational Technologies). IT (Information Technologies) and OT are two traditional areas used to distinguish equipment. The requirements of this Rule Note apply to both world and rules are globally written for both environments. As OT systems contain Cat. A and Cat B. equipment which come from IT world, rules have been unified and are still exhaustive. As Cat. C equipment are more OT system oriented, Cat. C rules will mostly apply to OT world. The borderline between IT and OT tends to fall down because of interconnections, manufacturers remote accesses, and internet of things industry. For all those reasons, rules have been designed in order to be used for both OT and IT. For very specific cases, OT is stated in the rule.

2.3.10 Monitoring

Monitoring refers to human procedures used to monitor events related to cyber security of equipment and systems.

2.3.11 Operator console

Operator consoles are industrial systems (OT) of Category A (Cat. A) mostly mobile systems involved in industrial system process engineering and maintenance.

2.3.12 System

Systems are a combination of interacting programmable devices and/or sub-systems organized to achieve one or more specified purposes. Systems are generally connected through a dedicated network or a dedicated VLAN. They are generally dedicated to a well-defined mission and localized in a distinct room space. However, systems may be distributed with distant location, or sites, and connected through networks tunnels. Systems may also be interconnected to other systems. A system is generally pre-integrated in that sense where it is developed, delivered and maintained by an individual supplier. Of course, systems may also be a group of elements integrated by the Shipyard or the Shipowner to fill out a specific mission, service or function. Systems may regroup different Categories of equipment. For example, a typical industrial controlled system regroups Cat. C equipment like safety instrumented systems, Cat B. network switch and Cat. A workstation for Supervisory Control And Data Acquisition (SCADA). In this document, the word system will be exclusively considered.

Note 1: Sub-systems are subcategories of systems. For the requirements application, sub-systems are considered like systems. This is due to the fact that cyber security looks at connection point between different levels of risks. Sub-systems wording is not used in this document.

3 Documentation management

3.1 General

3.1.1 Roles

Depending on context, all the documents are to be delivered under a defined responsible which is in charge to identify them, collect them and keep the collection up to date.

3.1.2 Documentation format

Documentation is provided in an electronic file with a human readable format.

3.1.3 Application

The Shipyard, Shipowner or supplier delivering the documentation is in charge of communicating its protection policy to relevant parties. However each relevant party is responsible for the application of the protection policy.

3.1.4 Technical tests file format

Tests are provided in an electronic file in a human readable format (e.g. describing a survey procedure, documentation to present, registry to read, command line test or step-by-step procedure to follow in a screen interface). Tests can result with the usage of scripts or tools (in this case, they shall be explained in the electronic document). Corresponding results shall be described and explained. For example, a way to detect generic logical accounts may be to use a command line with grep or awk command-line utilities.

4 Deliverables

4.1 CYBER MANAGED deliverables

4.1.1 Shipowner

The following steps are to be implemented by the Shipowner when the additional class notation **CYBER MANAGED** is assigned:

a) Basic Cyber Inventory, as defined in Sec 2

b) Criticality Assessment of each system, as defined in Sec 3

c) Cyber Risk Assessment based on the levels of criticality, as defined in Sec 5

d) Cyber Security Policy, as defined in Ch 2, Sec 2

e) Cyber Handbook with respect to Cyber Security Policy and the Cyber Risk Assessment output (Level 3: critical systems/equipment).

4.2 CYBER RESILIENT deliverables

4.2.1 Shipowner and/or Shipyard

The following steps are to be implemented by:

- the Shipowner for existing ships,
- the Shipyard for new ships,

as applicable when the additional class notation **CYBER RESILIENT** is assigned:

a) Basic, Intermediate and Detailed Inventory, as defined in Sec 2.

b) Criticality Assessment of each system, as defined in Sec 3

c) Design Assessment, as defined in Sec 4

d) Cyber Risk Assessment based on the levels of criticality, as defined in Sec 5

e) For existing ships only: Cyber Security Policy, as defined in Ch 2, Sec 2

f) Cyber Handbook with respect to:
   - Cyber Risk Assessment output (Level 3: critical systems/equipment)
   - for existing ships only: Cyber Security Policy.

4.3 CYBER SECURE deliverables

4.3.1 Shipyard and/or Shipowner

The following steps are to be implemented by:

- the Shipowner for existing ships,
- the Shipyard for new ships,

as applicable when the additional class notation **CYBER SECURE** is assigned:

a) Basic, Intermediate and Detailed Inventory, as defined in Sec 2

b) Criticality Assessment of each system, as defined in Sec 3

c) Design Assessment, as defined in Sec 4, including the list of rules applicable to the design of the ship

d) Cyber Risk Assessment based on the levels of criticality, as defined Sec 5

e) For existing ships only: Cyber Security Policy, as defined in Ch 2, Sec 2

f) Cyber Handbook with respect to:
   - Cyber Risk Assessment output (Level 3: critical systems/equipment)
   - for existing ships only: Cyber Security Policy.

4.4 Type approval of systems and equipment

4.4.1 Systems and equipment suppliers

The following steps are to be implemented by the systems and equipment suppliers applying to type approval:

a) The first step is to provide a Basic, Intermediate and Detailed Cyber Inventory document: equipment, networks, interconnections, connections, equipment, software, security mechanisms and components.

   The design and integration phases may interfere with the Cyber Inventory preparation. The assessment of the levels of criticality and the design assessment may require to modify the design and thus, lead to update the Cyber Inventory with revised systems, equipment and relevant networks.

b) The second step is to assess the levels of criticality of every equipment included in the system. High-risk assets, equipment or component will highlight the scope of systems to focus on. This scope is defined by the qualification of the levels of criticality of systems and equipment, as defined in Sec 3.

c) The third step is dedicated to the Design Assessment where:
   - Rules applied on equipment hardening, as detailed in Ch 5, Sec 3, Ch 5, Sec 4 and Ch 5, Sec 5 are to submitted. Rules depend on the level of criticality calculated during the second step. The proof of implementation is to be delivered by the supplier, including extended tests, which are to be performed during factory acceptance tests to verify both functional requirements and security mechanisms implementation
   - the surface of attack of equipment is evaluated in accordance with Sec 4, [2].

d) The fourth and last step consists of collecting information about the functioning of systems and equipment, such as guides and procedure, as explained in Sec 6. The gathered information shall constitute the Cyber Handbook document. The Cyber Handbook shall include extended tests, which are to be performed during annual surveys to verify both functional requirements and security mechanisms implementation.

5 Deliverables description

5.1 Definitions

5.1.1 Cyber Inventory

Quick view: The Cyber Inventory contains systems and equipment inventories and details on network architecture. Three levels of inventory may be submitted: Basic Inventory, Intermediate Inventory and Detailed Inventory.

Main outputs:

- Systems inventory
- Network inventory.

Responsibility: For new ships, the Inventory is under the responsibility of the Shipyard. For existing ships, the document is under the responsibility of the Shipowner. For systems and equipment, the document is under the responsibility of the supplier.

Service life: During the ship service life, the Cyber Inventory is under the responsibility of the Shipowner. The Shipowner must keep it updated and he must ensure the pertinence, quality and exhaustiveness of information.

Management: The Cyber Inventory is to be stored and managed on shore.

5.1.2 Criticality assessment

Quick view: The Criticality Assessment document contains, for each system and equipment, an assessment of impact in case of cyber attack. This assessment is based on technical and human factors.

Output: Levels of Criticality

Responsibility: This document is under the responsibility of the Shipyard for new ships and under the responsibility of the Shipowner for existing ships. For systems and equipment, the document is under the responsibility of the supplier.

Service life: During the service life of the ship, this document is to be updated by the Shipowner in case of modification of any system or equipment aboard.

Management: The Criticality Assessment is to be stored and managed on shore. It is not to be stored on board.

5.1.3 Design Assessment

Quick view: The Design Assessment document contains informations on the ship or system design. Applied rules are detailed and the surfaces of attack are calculated for each system and equipment.

Output:

- Design review
- Surfaces of Attack

Responsibility: The design assessment is under the responsibility of the Shipyard for new ships and under the responsibility of the suppliers for system and equipment. The design assessment is not applicable to existing ships.

Service life: During the service life of the ship, this document is to be updated by the Shipowner in case of major modification of the ship architecture.

Management: The Design Assessment is stored and managed on shore. It is not to be stored on board.

5.1.4 Cyber Risk Assessment

Quick view: The Cyber Risk Assessment allows the Shipowner to consider the equipment in its future maritime environment and take into account all of his operational and organisational priorities, the specific features of some ships, and the particular threats the Shipowner might already face or anticipate. The cyber risks are to be managed by the Shipowner as any other risks covered by ISM Code which requires to assess all risks.

Output: Cyber Risk Assessment in compliance with IMO resolution.

Responsibility: The Cyber Risk Assessment is under the responsibility of the Shipowner.

Service life: This document is to be updated during the whole service life of the ship and, in particular, during major maintenance phase like system upgrades.

Management: The Cyber Risk Assessment is to be stored and managed on shore.

5.1.5 Cyber Security Policy

Quick view: Cyber Security Policy describes the governance of cyber security by the Shipowner. This document, to be enforced on the whole fleet, details roles and rules. It is used as a reference for any action on systems and equipment by crew members.

Output: Cyber Security Policy

Responsibility: The Cyber Security Policy is under the responsibility of the Shipowner.

Service life: The cyber security responsible is in charge of checking and verifying that the Cyber Security Policy is in place and applied by crew members and external partners.

Management: The Cyber Security Policy is to be shared and implemented by with officers and crew members. The document is to be on board.

5.1.6 Cyber Handbook

Quick view: The Cyber Handbook contains procedures regarding cyber security management of systems and equipment. It is used to maintain the ship in a proper cyber state.

Output: Procedures to include inside the ISM.

Responsibility/ Service life: The Shipowner is in charge of updating the document and of ensuring that the handbook is in place and applied by crew members.

Management: The Cyber Handbook is to be used by officers and crew members. It is part of the ISM procedures.

5.2 Documentation to be submitted

5.2.1 Documentation to be submitted for notations CYBER MANAGED, CYBER SECURE and CYBER RESILIENT

The Documentation to be submitted for approval is detailed in the following chapters:

- Chapter 2 for the additional class notation **CYBER MANAGED**:
- Chapter 3 for the additional class notation **CYBER RESILIENT**:
- Chapter 4 for the additional class notation **CYBER SECURE**:.

A sum-up of the required documentation is detailed in Tab 1.

5.2.2 Documentation to be submitted for type approval of systems and equipment

The documentation to be submitted for approval is detailed in Chapter 5.

A summary of the required documentation is detailed in Tab 2.

Table 1 : Documentation to be submitted for notations CYBER MANAGED, CYBER RESILIENT and CYBER SECURE

	CYBER MANAGED	CYBER RESILIENT	CYBER SECURE
Basic Inventory	yes	yes	yes
Intermediate Inventory	–	yes	yes
Detailed Inventory	–	yes	yes
Criticality Assessment	yes	yes	yes
Design Assessment	–	yes	yes
Cyber Risk Assessment	yes	yes	yes
Cyber Handbook	yes	yes	yes
Security Policy	yes	yes	yes

Table 2 : Documentation to be submitted for Type Approval of system and equipement

	Type Approval Certificate
Basic Inventory	yes
Intermediate Inventory	yes
Detailed Inventory	yes
Criticality Assessment	yes
Design Assessment	yes
Cyber Risk Assessment	**(1)**
Cyber Handbook	yes
Security Policy	–
(1) Optional	

6 Regulations and standards

6.1

6.1.1 Purpose

For the purpose of application of this Rule Note, the standards listed in [6.1.2] could be used for:

- the development of hardware or software of CBSs
- the connection between systems and the global ship integration
- the design of the Cyber Risk Analysis
- the management of the and the crew members.

6.1.2 List of standards

- ANSSI Cybersecurity for Industrial Control Systems: Classification + Detailed Measures
- ANSSI EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité)
- ANSSI-DAT-NT-003-EN/ANSSI/SDE/NP: Recommendations for securing networks with IPsec
- ANSSI-PA-046: Cartographie du système d'information - Novembre 2018
- CIS-Benchmarks: Centre for Internet Security guidelines to protect systems & platforms
- ENISA Port Security (Good practices for cybersecurity in maritime) - November 2019
- IACS UR E22 Rev.3 : On board use and application of computer based systems
- IACS UR E26 Rev.1: Cyber resilience of ships
- IACS UR E27Rev.1: Cyber resilience of on-board systems and equipment
- IACS Rec. 171: Recommendation on incorporating cyber risk management into Safety Management Systems
- IEC 62443 series: Industrial communication networks - Network and system security
- IMO Resolution MSC.428(98) Maritime Cyber Risk Management in Safety Management Systems
- IMO MSC-FAL.1: International Marine Organization - Guidelines on Maritime Cyber Risk Management - Circ.3 - 5 July 2017
- ISO/IEC 15408 series: Information security, cybersecurity and privacy protection - Evaluation criteria for IT security
- ISO/IEC 27001:2022: Information security, cybersecurity and privacy protection - Information security management systems - Requirements
- NIST Special Publication 800-39: Managing Information Security Risk
- NIST Special Publication 800-137: Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations as part of a directive from the Federal Information Security Management Act (FISMA).

Section 2 Cyber Inventory

1 General

1.1 Framework

1.1.1 Objective

The Cyber Inventory document is dedicated to information gathering regarding assets, systems and equipment.

The objective is to have a list of information in accordance with the requirements of the notation as detailed in [1.4.1].

The identification is definitely the entry point of every methodology and regulation.

1.2 Applicability

1.2.1 The requirements of this Section are to be complied with:

- by Shipowners for new or existing ships assigned the additional class notation **CYBER MANAGED**
- by Shipyards for new or existing ships assigned the additional class notation **CYBER SECURE**
- by Shipyards (before ship commissioning) and by Shipowners (after ship commissioning) for new or existing ships assigned the additional class notation **CYBER RESILIENT**.

The requirements of this Section are to be complied with by equipment suppliers for systems or equipment to be type approved.

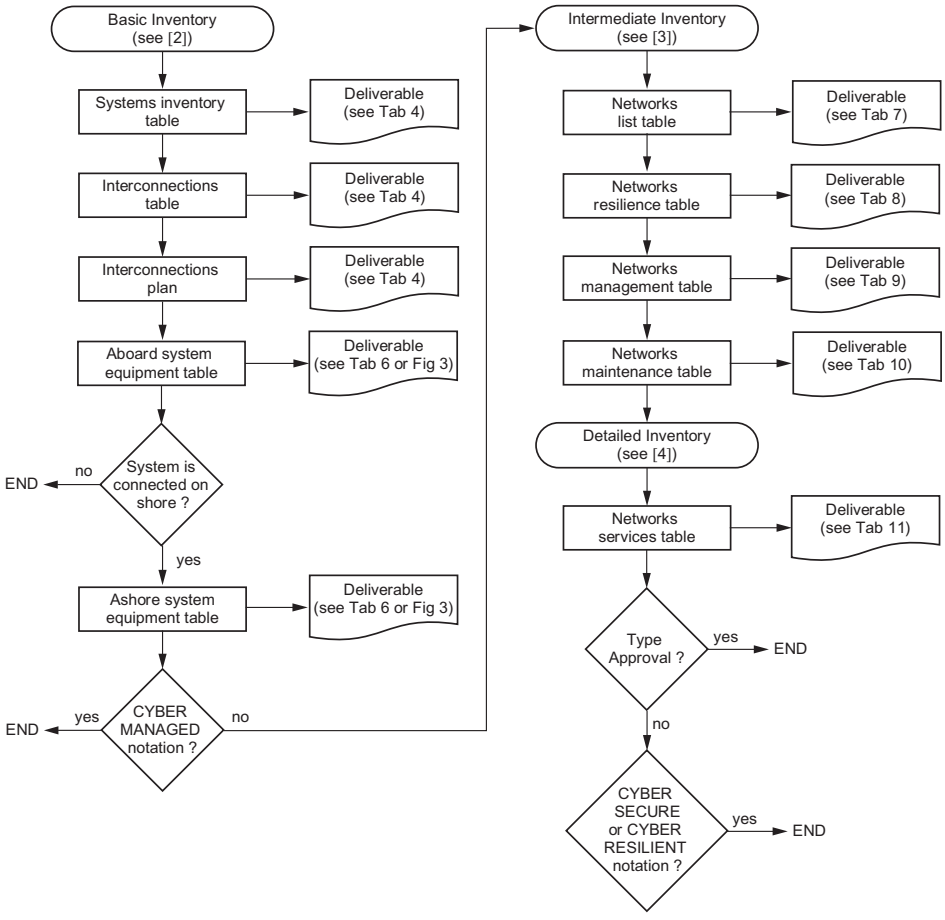
1.3 Methodology

1.3.1 Overview

The suggested methodology is a step by step identification of assets of the ship.

Those steps are linked to classification notation to be assigned and Type Approval Certification as detailed in Fig 1 and divided in three main bricks: the Basic Inventory, [2], the Intermediate Inventory, Article [3] and the Detailed Inventory, Article [4].

Figure 1 : Cyber Inventory deliverable workflow



1.3.2 Basic Inventory

The Basic Inventory (described in Article [2]) is to gather information through an inventory of assets identifying:

a) Every aboard system (identifying each group of equipment supplied as a whole and dedicated to a function) as explained in [2.3]

b) Systems interconnections (through a general architecture scheme containing connected systems) as explained in [2.4]

c) Architecture of the systems (implementation detailed in [2.5.1]) containing, as explained in [2.5]:

- a list of connected equipment
- a list of ashore equipment when ashore equipment are involved in ship monitoring, ship operations, ship management or equipment administration
- a scheme explaining the architecture of the system with a description of:
  - connections between aboard equipment
  - connections from aboard equipment to ashore equipment, when relevant
  - interconnections of the system of any other system.

Table 1 : Basic Inventory

Topic	Reference	Deliverable
Systems inventory table	[2.3]	Tab 4
Interconnections table Interconnections plan	[2.4.2] [2.4.3]	Tab 5 Fig 2
Aboard system equipment table Ashore system equipment table Equipment plan	[2.5.2] [2.5.3] [2.5.4]	Tab 6 Tab 6 Fig 3
On shore processing plan	[2.6]	Fig 4

1.3.3 Intermediate Inventory

The Intermediate Inventory (described in Article [3]) is dedicated to network identification:

- networks are to be detailed with identification information (VLAN, VPN), physical layers and location as described in [3.2.1]
- network resilience is to identify measures applied to contribute to the partitioning of networks, the safety of operations, the confidentiality of information, the availability of equipment and the integrity of data as detailed in [3.2.2]
- network management is to identify equipment involved in the configuration, monitoring of network equipment as detailed in [3.2.3]
- network maintenance is to identify on board and on shore equipment involved in the maintenance of on board system (e.g. OT laptops, system administration from on shore premises) as detailed in [3.2.4].

Table 2 : Intermediate Inventory

Topic	Reference	Deliverable
Networks list table	[3.2.1]	Tab 7
Network resilience table	[3.2.2]	Tab 8
Network management table	[3.2.3]	Tab 9
Network maintenance table	[3.2.4]	Tab 10

1.3.4 Detailed Inventory

The Detailed Inventory (described in Article [4]) is focused on data flows and implemented network services.

Listening, connecting or broadcasting services are to be detailed as explained in [4.2.1].

Table 3 : Detailed Inventory

Topic	Reference	Deliverable
Network services table	[4.2.1]	Tab 11

1.4 Deliverables

1.4.1 The Cyber Inventory document is to be submitted to the Society for approval in accordance with Sec 1, Tab 1.

1.4.2 Maintenance

The Cyber Inventory document is to be updated should any change occur regarding the infrastructure, the architecture, the networks, the physical implementation of any system and equipment.

The update procedure of the Cyber Inventory document is to be integrated to the Change Management Plan (as required in Ch 2, Sec 2, [6.1.1]).

The maintenance policy of the Cyber Inventory document is to be specified in the Cyber Security Policy document as requested in Ch 2, Sec 2, [3.2.1].

2 Basic Inventory

2.1 Definitions

2.1.1 Systems

Systems are groups of equipment delivered and installed as a standalone asset of the ship by a supplier. Systems may contain different kind of equipment (e.g. workstations, network equipment, automation, firewalls, automation) which are not to be detailed at this point. A system always refers to one or more piece of equipment delivering functions.

2.1.2 Target of evaluation

The Target of Evaluation defines any asset, systems or equipment to be considered by the classification notation:

- for the ship to be assigned the classification notation
- for the systems or equipment to be type approved.

2.2 Applicability

2.2.1 New ships

For new ships, the inventory of assets as detailed in [2] is to be delivered by Shipyards when one of the additional class notations **CYBER RESILIENT** or **CYBER SECURE** is to be assigned to the ship.

2.2.2 Existing ships

For existing ships, the inventory of assets as detailed in [2] is to be delivered by Shipowner when one of the additional class notations **CYBER MANAGED**, **CYBER RESILIENT** or **CYBER SECURE** is to be assigned to the ship.

2.3 Systems inventory

2.3.1 Categorisation

Aboard systems shall be inventoried and sorted by using the following categorisation:

- machinery systems (e.g. engines, steering gear, integrated automation systems, incinerator)
- navigation systems (e.g. ECDIS, DGPS, AIS, NavTex, radar, sonar, VDR)
- communication systems (e.g. satellite communications, VHF, satellite phones, ship security alert systems)
- cargo management systems (e.g. cargo control, ballast water treatment, loading PC)
- operations systems (e.g. gateway, domain controller, safety management system, enterprise resource planing, crew workstations, emailing systems)
- users systems (e.g. crew WiFi, passengers WiFi).

2.3.2 Systems description

Each system shall be described (see Tab 4) with the following information:

- name of the system (with a brief description of the function when needed)
- when used, description of any link to ashore description (e.g. connected to ashore for remote monitoring)
- list of aboard locations where the equipment of the system are installed (e.g. engine room and bridge)
- list of connections with other aboard systems (e.g. integrated automation system is connected to the main engine)
- brand of the system (e.g. the equipment supplier)
- model of the system
- version of the system (e.g. software version number, model number, release, issue, mark).

Table 4 : Example of systems inventory

Aboard system	Linked to ashore equipment	Location	Links with other system(s)	Brand	Model	Version
Machinery systems						
Main engine	No	Engine room / Bridge	Integrated automation system	Weissnat PLC	GRIFFINDOR-VI	Mark II
Auxiliary engine	No	Engine room / Bridge	Integrated automation system	Weissnat PLC	DNA-2300	A
Integrated automation system	Yes	Engine room	Engines	Nader-Haag	TRACTION	V2
Engine monitoring	Yes	Engine room	Connected to IAS through serial cables	Skiles Group	CENTURY	1.23.98
Steering gear	No	Engine room / Bridge	None	Kobayashi	MIDCAP	model K
Sewage treatment	No	Engine room	None	Grenier Poirier S.A.	ZUES-1200	2.12
Incinerator	No	Engine room	None	Grenier Poirier S.A.	TELLUS	B.C
Oily bilge generator	No	Engine room	None	Nader-Haag	BELUGA	Model Air
Auxiliary boiler	No	Engine room	None	Martinelli e figli	CRP-NX	GF65241
Navigation systems						
Automatic identification system	No	Bridge	GPS, ECDIS, Radar, Sonar	Fierro-Navarrete	PEERLESS-T	AI236
Doppler sonar	No	Bridge	ECDIS, AIS	Fierro-Navarrete	AVIATOR-DEF	DS876
ECDIS	Yes (Charts update)	Bridge	IT Gateway	Fierro-Navarrete	BENZ	E2.23
Echo sounder	No	Bridge	ECDIS	Fierro-Navarrete	TAURO	4.3
DGPS	Yes (Charts update)	Bridge	ECDIS, AIS	Fierro-Navarrete	MORY	9.12
NavTex	No	Bridge	None	Fierro-Navarrete	SPRINTER	Model V
Radar	No	Bridge	ECDIS	Fierro-Navarrete	TAXI-34D	RD82
VDR	No	Bridge	Multiple	Martinelli e figli	HORIZONT	V8712
Communication systems						
SatCom 1	Yes (Internet)	Network room	Gateway	Schutte Ltd	JACKAL	12.76
SatCom 2	Yes (Internet)	Network room	Gateway	Jansen Brisee BV	ALPHA-TF	43.34
VHF	No	Bridge	None	Bernard et Fils	MIRREN	Mark IV
Satellite phone	No	Confidential	None	Funk, Ryan and Erdman	STIM	Ir2
Ship security alert system	No	Bridge	None	Funk, Ryan and Erdman	KEYSTONE	v 15
Cargo management systems						
Cargo control	Yes	Cargo control room	Integrated automation system	Papakiriskou	MELCHESTER	release 9
Ballast water treatment	No	Engine room	None	Hendriks Akin NV	ZENIT	v 3.2
Loading PC	No	Cargo control room	None	Willms-Schmitt	IMOLEVE	4.2

Aboard system	Linked to ashore equipment	Location	Links with other system(s)	Brand	Model	Version
Operations systems						
Gateway	Yes (Multiple)	Network room	All other systems	Nikolopoulos	PORTIMAO	Sep. 19
Domain controller	Yes (Administration)	Network room	Workstations	Ouellet	RODOVIA	WS11
Safety management system	Yes (Management)	Network room (Server) Bridge Cabins	Workstations	Dion S.A.S	CRIOS	model K
Enterprise resource planning	Yes	Network room (Server) Cabins	Workstations	Blum Horn KG	PHAROAH	v 4
Emailing system	Yes	Multiple	Workstations	Blum Horn KG	LYSKAMM	multiple
Users systems						
Crew WiFi	Yes	Multiple	Multiple	Blum Horn KG	AMPLE	multiple
Passenger WiFi	Yes	Multiple	Multiple	Sheng Zhu	PEPINIERES	multiple

2.4 Systems interconnections

2.4.1 Objective

Systems interconnections are to be inventoried using both a dedicated table (see [2.4.2]) and a drawing visualizing data paths (see [2.4.3]).

2.4.2 Interconnections inventory

The following requirements define the list of situations where interconnection of a system to another is to be detailed in the table (see Tab 5):

- connections from a system involving another system either to send data or to receive data
- connections from any aboard system to any ashore system, when involved
- interconnection using either cabled or wireless links
- any system interconnection based on Ethernet cables
- any system interconnection based on Internet protocol suite
- any system interconnection using any communication protocol.

For each identified interconnection, the following are to be explained:

- the name of the source system (the source means the system in charge to establish a connection)
- the name of the destination system (the destination means the system in charge to listen to incoming connections)
- the type of the physical layer used for data transportation: Ethernet, optical, serial, wireless (e.g. Bluetooth, WiFi)
- the direction of the connection (single or dual). Single connections are connections which can be disrupted by using either a firewall (applicable to bi-directional protocols like TCP/IP) or a diode (applicable to uni-directional protocols like serial links dedicated to monitoring). Single connection are granted to TCP/IP connection with acknowledgment packets. Single connection refers to listening services hosted by a single host (also named as client-server connection).
- the purpose of the connection (general description of the objective of the interconnection).

Table 5 : Example of interconnections inventory

Source System	Destination System	Physical layer type	Direction	Purpose
Cargo Management System	Gateway / Internet (Shipowner)	Ethernet	Single	Send monitoring information to on, shore system
ECDIS	Gateway / Internet (equipment supplier)	Ethernet	Single	Connects to the Internet to collect charts updates
DGPS	Gateway / Internet (equipment supplier)	Ethernet	Single	Connects to the Internet to update GPS maps
Crew WiFi	Gateway / Domain Controller / Internet	WiFi	Dual	Deliver Internet access to Crew members
Passengers WiFi	Gateway / Domain Controller / Internet	WiFi	Dual	Deliver Internet access to passengers as a service

Source System	Destination System	Physical layer type	Direction	Purpose
Safety Management System	Gateway / Domain Controller / Internet (Shipowner)	Ethernet	Dual	Get procedures updates / Managed from on shore
Enterprise Resource Planning	Gateway / Domain Controller / Internet (Shipowner)	Ethernet	Dual	Connect to central ERP / Managed from on shore
Workstations	Gateway / Domain Controller / Internet (Shipowner)	Ethernet	Dual	Connect to aboard servers / Managed from on shore
SatCom1 and SatCom2	Gateway	Ethernet	Dual	Transport ingoing and outgoing traffic / Managed from on shore
Engine Monitoring	Gateway / Internet (Shipowner)	Ethernet	Dual	Send engine monitoring data to on shore equipment
Integrated Automation System	Engine Monitoring System	Serial	Dual	Send engine monitoring data to aboard engine monitoring equipment
Main Engine	Integrated Automation System	Optical	Single	Send engine monitoring data to IAS

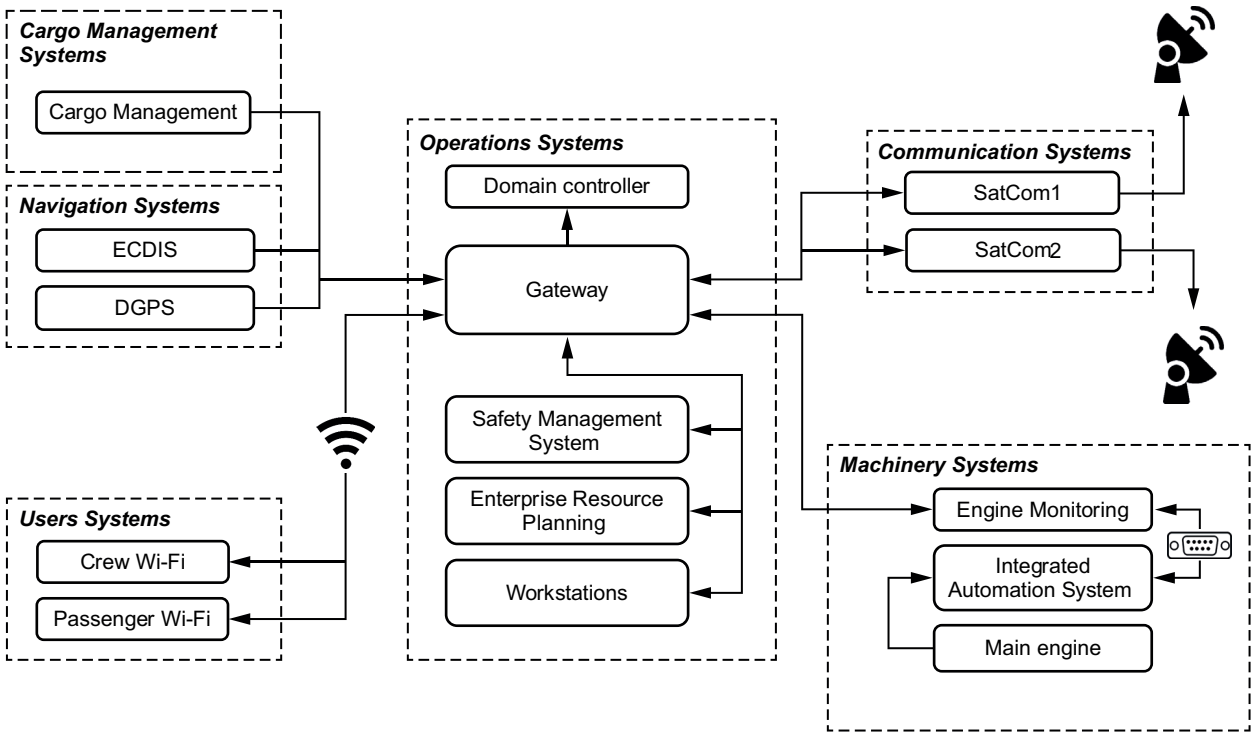
2.4.3 Plan requirements

The following requirements define the list of situations where interconnection of a system to another is to be represented on the plan (see Fig 2):

- connections from a system involving another system either to send data or to receive data
- connections from any aboard system to any ashore system, when involved
- interconnection using either cabled or wireless links
- any system interconnection based on Ethernet cables
- any system interconnection based on Internet protocol suite
- any system interconnection using any communication protocol.

The way of connection establishment from a system to another shall also be represented by the use of single or dual arrow.

Figure 2 : Example of interconnection plan



2.5 Systems architecture

2.5.1 Applicability

The information as detailed in [2.5] and presented in Tab 6 is to be delivered in the following situations:

- to any system connected to on shore, for ships to be assigned the additional class notation **CYBER MANAGED**
- to any system for ships to be assigned the additional class notation **CYBER SECURE**
- to the whole system, for systems or equipment to be type approved.

Table 6 : Example of system's equipment inventory

Name	Brand	Model	Version	Cat.	Q.	Ashore	Purpose
ECDIS							
Console	Fierro-Navarrete	BENZ	E2.23	Cat. A	2	No	ECDIS consoles used for navigation
Update box	Fierro-Navarrete	BENZ ONLINE	1.01	Cat. B	1	No	Box used to update ECDIS consoles from Internet
Server	unknown					Yes	Server containing ECDIS charts updates

2.5.2 Equipment inventory

When a system installed is composed of multiple equipment, a detailed table (see Tab 6) is to inventory those equipment. The system architecture table shall detail the following:

- the name of the equipment
- the brand of the equipment
- the model including any revision version number
- the version number (e.g. operating version number for workstations, firmware version number for network appliances)
- the category (Cat. A, Cat. B or Cat. C), to be specified in accordance with the Categories definition from Sec 1, [2.3.2]
- the quantity of similar equipment to consider (e.g. workstations)
- if the equipment is located on shore
- the role of the equipment in the system.

Note 1: Equipment refer to any asset included in the operation delivered by the system (e.g. workstations, mobile endpoints, network equipment or automation, etc).

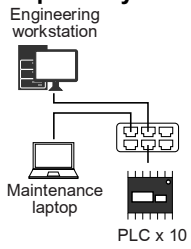
2.5.3 Ashore equipment

When involved in any system activity, operation or maintenance, on shore equipment are to be identified as part of the system described in [2.5.2].

2.5.4 System drawing

Drawing of equipment involved in a system may be delivered (see Fig 3) to support, or to replace, the inventory delivered in [2.5.2].

Figure 3 : Example of system architecture



2.6 On shore processing

2.6.1 Process chain

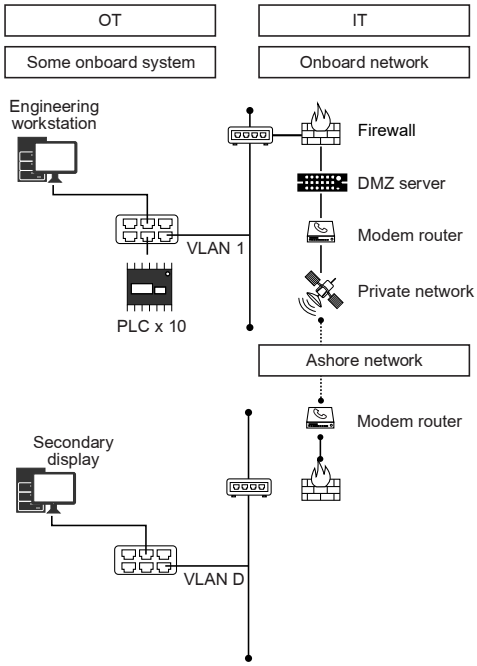
Systems connected to ashore systems or equipment are to be described through a process chain drawing.

Process chain drawings are to detail the delivered system architecture (see Tab 6) with an explanation of the workflow applied to each equipment (e.g. ground computer, satellite link, ship IT router, ship VLAN over the IP network, OT firewall, SCADA computer, automation) involved in information processing between aboard and ashore equipment (see Fig 4).

A brief description of the chain is to be delivered.

Note 1: Example presented in Fig 4 could be described like this: "On Some System, the Engineering Workstation retrieves information from the PLC every hour. The PLC sends information to PC via Modbus protocol. Then, the workstation sends information through HTTPS to the DMZ via VLAN 1 managed and operator by switch X. In the control center, the secondary display console connects to dedicated switch on VLAN D. It gets through firewall and send HTTPS request to DMZ on user demand".

Figure 4 : Process chain example



3 Intermediate Inventory

3.1 Applicability

3.1.1 Ships

For ships to be assigned the additional class notation **CYBER RESILIENT** or **CYBER SECURE**, inventory of assets as detailed in Article [3] is to be delivered by Shipyards:

The networks to consider are limited to those installed by the Shipyard or the system integrator.

Systems internal networks delivered, installed and maintained by equipment suppliers are not to be described.

3.1.2 Systems and equipment

The documentation requested in Article [3] is to be delivered by the supplier for type approval certification of system or equipment.

Each network delivered, installed or maintained with the system or equipment is to be included.

3.2 Networks

3.2.1 Networks list

Each network is to be described and detailed.

Networks refer to logical telecommunication nodes used to transport data and communicate between themselves.

Either physical or logical networks are to be considered.

- dedicated cabled computer networks (e.g. Ethernet, Optical loops)
- wireless networks (e.g. WiFi, Bluetooth)
- partitioned network (e.g. VLAN)
- virtualized networks (e.g. virtualized machines)
- serial links.

Specific protocols may also be referred as networks when dedicated to a group of equipment linked through:

- serial line protocols (e.g. MODBUS)
- tunnelling protocols (e.g. IPSec)
- any protocol relying on any layer, as defined by the ISO/OSI model communication stack, dedicated to a specific function and a specific group of equipment.

The network list (see Tab 7) shall contain the following information:

- network name (e.g. IT system, bridge, crew, engine management, maintenance…)
- network reference (e.g. VLAN number, internal code)
- purpose of the network through a brief description (e.g. IT/ICS, redundancy, operations, administration…)
- physical support (e.g. shared copper cables, dedicated optical fibre, wireless…)

- location hosting the network (e.g. bridge only, on shore and bridge…)
- connection points with other networks (e.g. diodes from IT to OT machinery, gateway to sitcom, DMZ…). Other networks to consider, and to specify, are:
  - networks delivered within the system
  - aboard networks supplied by another system or equipment, on which the system is connected to
  - any ashore networks.

Table 7 : Example of vessel network list

Name	Reference	Purpose	Physical support	Area	Connection points
Engine Remote Controller	ERC	Orders transportation from bridge to engine	Dedicated optical loop	Bridge / Engine room	IAS: Through Ethernet to IAS Network
IAS network	IAS	Engine and cargo automation management	Ethernet	Engine room / Cargo management room	Engine: Ethernet Cargo: Ethernet AIS: Communication box (serial) Monitoring: Monitoring network through serial communication
Monitoring network	IPSec-01	Collect monitoring information from AIS	Ethernet	Engine room	IAS: (serial) Ashore: (internet)
WiFi	VLAN03	Provide internet to crew members	WiFi	Cabins	Router: To the gateway
Business	VLAN01	Provide email, ERP and SMS access a to officers' workstations	Ethernet	Bridge / Cabins	Gateway

3.2.2 Network resilience

Equipment dedicated to cyber security (e.g. firewalls, intrusion detection or prevention systems, access management system, isolated means, IPSec, virtual private networks, multiprotocol label switching networks, diodes, Demilitarized Zones, physical disruption, security information and event management) or cyber safety (e.g. network redundancy, uninterruptible power supply, dedicated means, bandwidth management) are to be inventoried.

This inventory is to list measures which have been applied on the networks to contribute to the partitioning of networks, the safety of operations, the confidentiality of informations, the availability of equipment and the integrity of data.

Equipment dedicated to cyber resilience are to be detailed in a table (see Tab 8) containing the following information:

- the name of the network (as previously delivered in a table detailed in [3.2.1])
- the name of the solution ensuring cyber resilience function (as suggested in [3.2.2]) with its brand, model and version
- brand of the equipment
- model, version of the equipment
- a short description of the function and its implementation.

Table 8 : Example of table listing equipment enforcing network resilience

Network resilience equipment	Brand	Model	Description
Engine remote controller network			
Link Aggregation	not applicable		Safety: Two optical fibres link the bridge to the engine
UPS	POWA	VOLT Mk 2	Safety: Uninterruptible power supply delivery
IAS Network			
VLAN	CISKROM	Guardian 3000	Security / Safety: IAS operations are grouped in dedicated VLAN
AIS communication box	Fierro-Navarrete	CONNEX	Security: A dedicated device ensures a physical disruption between IAS network and data gathered from the AIS
Monitoring communication box	Fierro-Navarrete	My Fuel Supervisor	Security: A dedicated device ensures a physical disruption (Ethernet/Serial with diode) between IAS network and monitoring PC connected to the Internet
Monitoring network			
Firewall	CISKROM	Guardian 3000	Security: A firewall, installed in the vessels' gateway, filters traffic coming from the outside to the monitoring network (registered source ip, limited protocols, specific ports)

Network resilience equipment	Brand	Model	Description
Intrusion Prevention System	CISKROM	Guardian 3000	Security: An IPS, installed in the vessel's gateway, traps irrelevant traffic going from or to the monitoring network
WiFi network			
Intrusion Prevention System	CISKROM	Guardian 3000	Security: An IPS, installed in the vessel's gateway, traps irrelevant traffic going from or to the WiFi network
WPA3 routers	WAWAY	Air 40	Security: Crew network is limited to WPA3 encryption and strong access control

3.2.3 Network management

Equipment dedicated to the network management (e.g. gateway, routers, switches, etc.) are to be inventoried in a table (see Tab 9) with the following information:

- name of the relevant network (as previously delivered in a table detailed in [3.2.1])
- name of the equipment (brand and model, version)
- function of the equipment (e.g. VLAN management, DHCP server)
- technical specifications of the equipment (e.g. dedicated ports, port mirroring, network address translation, local connection, remote access).

Table 9 : Example of table listing equipment involved in network management

Network management equipment	Brand	Model	Function	Technical Specification
Engine remote controller network				
Switch	CISKROM	OPT 2100	The switch regroups optical fibres and provides fault-tolerance service	Multi-link trunking
IAS Network				
Router	CISKROM	Guardian 3000	The router manages connections (equipment) and VLAN	DHCP Static MAC Address filtering VLAN
Gateway	FLORON	Gatekeeper 100	Manages on board VLAN and traffic routing to Satcom units	

3.2.4 Network maintenance

Equipment dedicated to the network maintenance (e.g. maintenance laptops, remote maintenance...) are to be inventoried in a dedicated table (see Tab 10) with the following information:

- name of the relevant network (as previously delivered in a table detailed in [3.2.1])
- name of the equipment (brand and model, version)
- function of the equipment (e.g. VLAN management, DHCP server)
- technical specifications of the equipment (e.g. dedicated ports, port mirroring, network address translation, local connection, remote access).

Table 10 : Example of table listing equipment involved in network maintenance

Network management equipment	Brand	Model	Function	Technical Specification
Monitoring network				
On shore workstation	BELL	C64	The on shore PC is used to remotely manage the on board network equipment (CISKROM Guardian 3000)	SSH
IAS Network				
On shore workstation	BELL	C64	The on shore PC is used to remotely manage the on board gateway FLORON Gatekeeper 100	HTTPS
Engine remote controller				
Aboard maintenance laptop	BELL	Light 43	The maintenance laptop is used on board by crew member, with supplier supervision, in case of engine reprogramming	The maintenance PC is directly connected to local network with a network cable

4 Detailed Inventory

4.1 Enforceability

4.1.1 Ships

For ships to be assigned the additional class notation **CYBER RESILIENT** or **CYBER SECURE**, inventory of assets as detailed in Article [4] is to be delivered by Shipyards.

The networks to consider are limited to those installed by the Shipyard or the system integrator.

Systems internal networks delivered, installed and maintained by equipment suppliers are not to be described.

4.1.2 Systems and equipment

The documentation requested in Article [4] is to be delivered by the supplier for type approval certification of system or equipment.

4.2 Networks traffic

4.2.1 Network flows

For each equipment of the system (as previously delivered in a table detailed in Tab 6, the following information are to be provided (see Tab 11) for each network on which the equipment is connected to (as previously delivered in a table detailed in [3.2.1]):

- description of the network flow (e.g. remote shell, command and control, emails)
- name of any service (e.g. DNS, LDAP, SMTP, SFTP, MODBUS, DNP3, Profibus, LonWorks, DALI)
- connection type:
  - outgoing: the connection is established by this equipment
  - ingoing: this equipment is listening to connection coming from other equipment
  - broadcast: this equipment broadcast packets on the network.
- list of equipment connected to this service (either as a service or as a server)
- interface dedicated to the network (e.g. Ethernet, serial).

Table 11 : Example of table detailing network flows of an equipment

Equipment name: Remote I/O control				
Description	Service name	Connection type	Connected to	Interface
Network: Operational network				
Data processing transfer	Modbus TCP/IP	outgoing	Processing PLC	Eth0
Network: Management VLAN3				
Management	SNMP	ingoing	Management workstation	Eth1
Data transfer	SFTP	outgoing	Management workstation	Eth1
Automatic assignment of the IP address	DHCP	broadcast	Domain Server	Eth1

Section 3 Criticality Assessment

1 General

1.1 Framework

1.1.1 Objective

The objective of the Criticality Assessment is to sort out equipment in three groups, named Levels of Criticality, with specific rules dedicated to each of them.

Throughout this process, any organization involved manages both the initial investment support during construction phase and the management effort support during the service life of the ship.

1.2 Applicability

1.2.1 Ships

The requirements of this Section are to be complied with by:

- Shipyards for new ships to be assigned one of the additional class notations **CYBER RESILIENT** or **CYBER SECURE**
- Shipowners for existing ships to be assigned one of the additional class notations **CYBER MANAGED**, **CYBER RESILIENT** or **CYBER SECURE**.

1.2.2 Systems or equipment (For Type Approval Certification)

The requirements of this Section are to be complied with by equipment suppliers for systems or equipment to be type approved.

1.3 Methodology

1.3.1 Definition

The Level of Criticality of a system or equipment is referred to as “Level” in this Rule Note.

When assessed, the assignment of a Level is definitive.

The Level does not take into account the benefits of security measures applied by the classification notation. On the contrary, the amount and the quality of security measures and applicable requirements to be implemented on the equipment, the system and, or, the management processes depend on the assigned Level.

Levels (Level 1, Level 2 or Level 3) apply to each system and describe the critical level of the systems. Level 3 is the highest Level of Criticality. An upper Level means more mandatory rules with required documentation deliveries from suppliers, Shipyards or Shipowners.

Level is referred with the following wording: Level 1, Level 2 or Level 3.

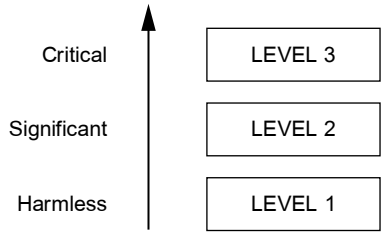
IT and OT system are grouped in three Levels referring to the following definitions (see Fig 1):

- Level 1: Harmless
- Level 2: Significant
- Level 3: Critical.

Each Level introduces rules on usage, connectivity and management detailed in relevant chapters of this Rule Note.

Note 1: When applied to a system or an equipment, mitigation measures, procedures or technical protection do not contribute to change the Level: it shall remain unchanged, independently of any protection measures.

Figure 1 : Scale of criticality



1.3.2 Scope of application

The assessment of the Levels of Criticality is applicable to equipment defined in Basic, Intermediate or Detailed Inventory.

1.3.3 Level assignment

Systems in scope are to be associated to a Level by using the methodology described in [1.3.4].

Each equipment inside a system inherits the Level of its parent system. This rule may be subject to exceptions when demonstrated to the satisfaction of the Society.

Level 1 rules are generally considered as recommendation or options.

1.3.4 Methodology

A methodology to deliver Criticality Assessment is proposed with a standard template detailed in App 1. This template and associated methodology may be used by Shipyards, Shipowners or suppliers. This Criticality Assessment can also be performed by a third party contributor applying a recognized methodology.

1.4 Deliverables

1.4.1 Deliverable

The responsible of the delivery shall assess the Levels of Criticality and apply the relevant rules as detailed in this Section.

Levels of Criticality assessment applies for both IT and OT systems.

The whole ship is in the scope of Levels of Criticality as each system shall be checked.

The Criticality Assessment is to be submitted for approval.

The Criticality Assessment document shall contain a table containing Levels of Criticality (with rationale) for each system and equipment.

1.4.2 Maintenance

The Criticality Assessment document is to be updated should any change occur regarding the infrastructure, the architecture, the networks, the physical implementation of any system and equipment.

The update procedure of the Criticality Assessment document is to be integrated to the Change Management Plan (as required in Ch 2, Sec 2, [6.1.1]).

The maintenance policy of the Criticality Assessment document is to be specified in the Cyber Security Policy document as requested in Ch 2, Sec 2, [3.2.1].

Section 4 Design Assessment

1 General

1.1 Framework

1.1.1 Objective

The objective of the Design Assessment is to evaluate the attack surface of the ship.

The Design Assessment applies to new ships. It delivers a way to take into account the benefits of the rules and to identify residual risks as negligible, significant or unacceptable.

1.2 Applicability

1.2.1 New ships

The requirements of this Section are to be complied with by Shipyards for new ships to be assigned the additional class notation **CYBER RESILIENT** or **CYBER SECURE**.

1.2.2 Existing ships

This Section does not apply to existing ships to be assigned the additional class notation **CYBER MANAGED**.

1.2.3 System or equipment

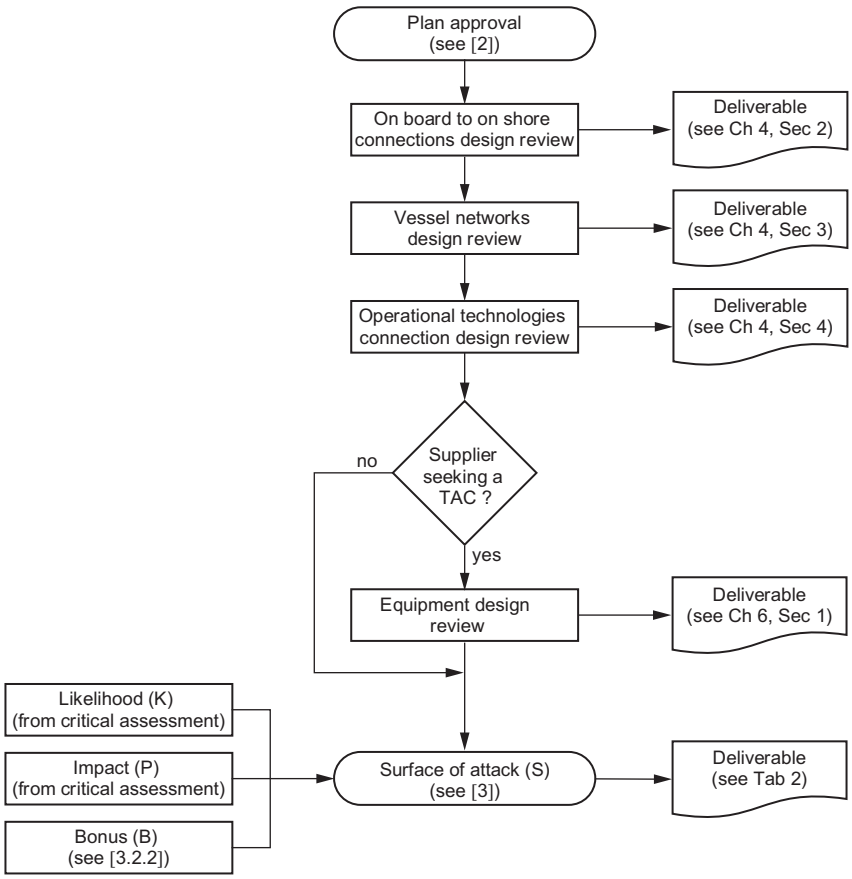
The requirements of this Section are to be complied with by equipment suppliers for systems or equipment to be type approved.

1.3 Methodology

1.3.1 Overview

The Design Assessment is divided as shown in Fig 1:

Figure 1 : Design Assessment delivery workflow



1.3.2 Plan approval

The Plan approval is applicable to:

- Assignment of the additional class notation **CYBER RESILIENT** or **CYBER SECURE**
- Type Approval of systems or equipment.

For ships granting a classification notation, rules applicable by the Shipyard to the design of the ship are to be in line with those detailed in the relevant chapter (see references in [2]). The proof of implementation is to be delivered by the Shipyard, including extended tests, which are to be performed during initial and annual survey.

For systems or equipment seeking a Type Approval Certificate, requirements applied on equipment hardening, as detailed in Ch 5, Sec 3, Ch 5, Sec 4 and Ch 5, Sec 5, are to submitted. The proof of implementation is to be delivered by the supplier, including extended tests, which are to be performed during design phase tests to verify both functional requirements and security mechanisms implementation.

1.4 Deliverables

1.4.1 Deliverable

The responsible of the delivery shall assess the design of the ship and apply the relevant rules as detailed in this Section.

The Design Assessment documentation is to be submitted for approval.

The deliverable shall include the plan approval, as described in [2]

1.4.2 Maintenance

The Design Assessment documentation is to be updated should any change occur regarding the infrastructure, the architecture, the networks, the physical implementation of any system and equipment.

The update procedure of the Design Assessment documentation is to be integrated to the Change Management Plan (as required in Ch 2, Sec 2, [6.1.1]).

The maintenance policy of the Design Assessment documentation is to be specified in the Cyber Security Policy document as requested in Ch 2, Sec 2, [3.2.1].

2 Plan approval

2.1 Definitions

2.1.1 Ships

Ships to be assigned the additional class notation **CYBER RESILIENT** or **CYBER SECURE** are to be secure by design in accordance with the rules on Ship Design of Chapter 4.

The above rules on Ship Design are applicable to on board systems and equipment according to their level of criticality.

The Shipyard is to deliver documents dedicated to the review of the design by the Society.

In this Plan Approval document, rules applicable to the architecture of the systems integrated on board are to be identified. Any rationale on application of the rules is to be explained and justified.

2.1.2 Systems or equipment

Systems or equipment to be type approved are to be secure by design in accordance with Chapter 5.

The above rules are applicable to the equipment according to their level of criticality.

The Supplier is to deliver documentation dedicated to the review of the design by the Society.

In this plan approval documentation, the Supplier is to identify rules applicable to the architecture and the systems on board. Any rationale on application of the rules is to be explained and justified.

2.2 Deliverable

2.2.1 Ships

The deliverable for ships assigned the additional class notation **CYBER RESILIENT** or **CYBER SECURE** are described in Sec 1, [5.2.1].

2.2.2 Systems or equipment

The deliverables for systems or equipment to be type approved are described in Sec 1, [5.2.2]

Section 5 Cyber Risk Assessment

1 General

1.1 Framework

1.1.1 Objective

The requirements of this Section apply only to existing ships.

The objective of the Cyber Risk Assessment is to reduce the volume and the impact of cyber incidents during the whole life cycle of the ship.

Based on Levels of Criticality that are going to be used as fundamental entry points, the Cyber Risk Assessment will allow the Shipowner to consider the equipment in its future maritime environment and take into account all of his operational and organisational priorities, the specific features of some of his ships, and the particular threats the Shipowner might already face or anticipate.

There are different ways to consider the risk management as it may be used to address different kind of objectives. The Cyber Risk Assessment measures the residual risks regarding feared hazards and, in conclusion, helps the Shipowner make a decision about mitigation measures to install.

The entry point is thus the ship's missions which need vital functions to operate free from cyber attacks. Vital must be understood here as regarding both operational objectives of the ship and its safety.

Vital functions are achieved through process chains which are exposed to threats. Threats are ways to exploit the feared hazards. Threats will be considered to assess the index of the vital function which will determine the level of importance of the systems involved in the processing chain.

The risks will be then reduced by introducing crew cyber awareness, training, organizational mitigation measures with procedures and physical control, technical mitigation measures to detect or harden systems involved in vital functions.

The Cyber Risk Assessment contributes to:

- enhance technical and human processes to reduce risks
- optimize to the risk management of the Shipowner
- comply with IMO Resolution MSC.428(98).

Note 1: The Cyber Risk Assessment is a dynamic process, an study written under the responsibility of the author, the Shipowner. The risk calculation is neither a mathematical formula nor an automatic system: each situation is to be studied case by case.

1.2 Applicability

1.2.1 Existing ships

The requirements of this Section are to be complied by Shipowners for existing ships to be granted one of the additional class notations **CYBER MANAGED**, **CYBER RESILIENT** or **CYBER SECURE**.

1.2.2 Systems or equipment

This Section does not apply to systems or equipment to be type approved

1.3 Methodology

1.3.1 Overview

The Cyber Risk Assessment assumes that Criticality Assessment has been performed, in accordance with Sec 3.

1.3.2 Scope of application

The Cyber Risk Assessment is based on systems and equipment defined during the Criticality Assessment as explained in Sec 3.

1.3.3 Suggested methodology

The Cyber Risk Assessment may be divided in 3 following steps (see Fig 1):

a) A first step dedicated to the definition of the Vital Functions assessment (see [2]). It is a customization by the Shipowner of the risks by design according to his own strategy, vision, concerns or constraints.

The Vital function grade (VF) which describes the impact index on a short list of functions which are vital for the ship's mission, is freely decided by the Shipowner from superficial (VF1), major (VF2) or absolute (VF3).

b) A second step is to decide on risk treatment opportunity (see [3]). The risk by design (systems levels of criticality) is to be challenged by introducing risk as identified by the Shipowner.

The Risk Level grade (RL) defines the degree of risk on a vital function before application of mitigation measures. The highest the Risk Level, the more critical it is.

c) The third and last step concludes the Cyber Risk Assessment with decisions on the Risk as identified by the Shipowner, by delivering a plan for Risk Mitigation (M) and a Residual Risk (RR) (see [4]).

The Mitigation grade (M) assesses the effort of mitigation on risk affecting vital functions.

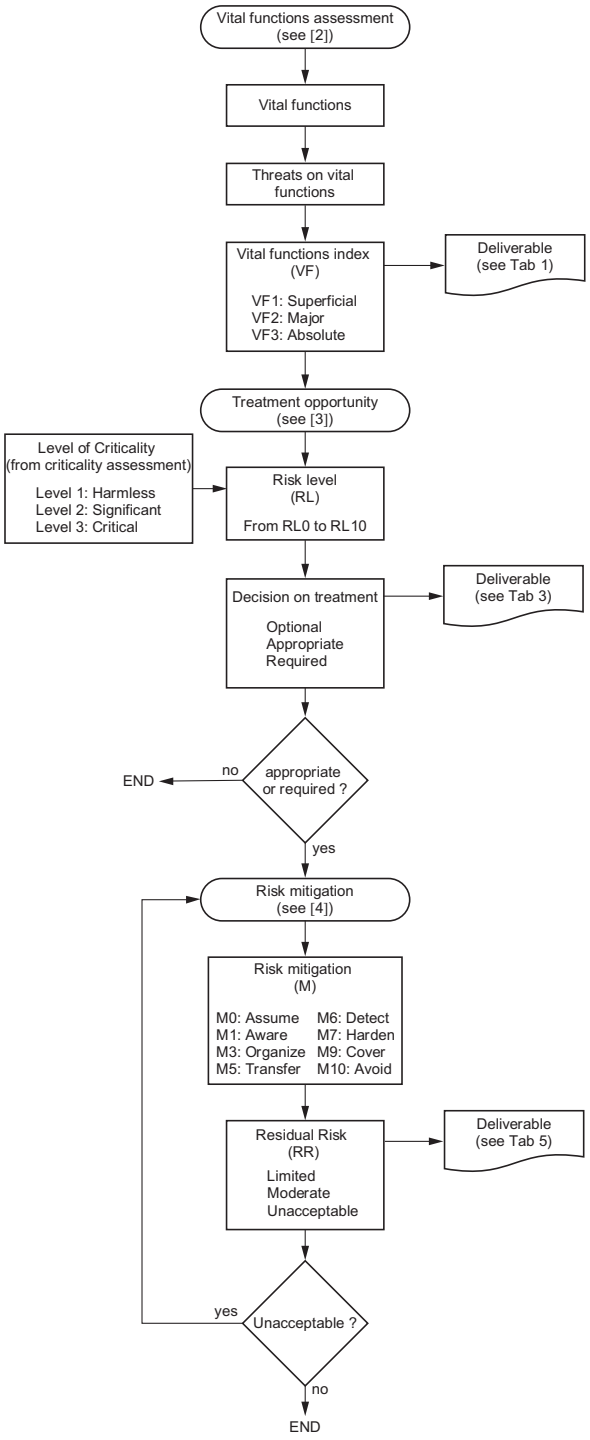
The Residual Risk value (RR) identifies the risk after mitigation as limited, moderate or unacceptable.

1.3.4 Other recognized methodologies

The following other methods may be used:

- ANSSI EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité)
- ENISA BS 7799-3 (Information security management systems)
- IACS Rec. 171: Recommendation on incorporating cyber risk management into Safety Management Systems
- NIST SP 800-39 (Managing Information Security Risk).

Figure 1 : Cyber Risk Assessment delivery workflow



1.4 Documentation

1.4.1 Documents

The Cyber Risk Assessment document is to be submitted by the Shipowner to the Society, for approval.

The Shipowner is responsible of the Cyber Risk Assessment results, application and mitigation measures.

The Cyber Risk Assessment applies both for IT and OT systems.

The Cyber Risk Assessment can be written:

- by the system integrator or a qualified engineer on board
- by a third-party partner.

If the methodology applied by the Shipowner is the one which is suggested in the Section, the three following tables are to be delivered:

- A table of Risk on vital functions as shown in Tab 1
- A table of Treatment opportunity as shown in Tab 3
- A table of Risk Mitigation as shown in Tab 4.

Note 1: As this methodology is in line with this Rule Note and, notably, with the Criticality Assessment, it is encouraged to apply it.

1.4.2 Maintenance

The update procedure of the Risk Assessment document is to be integrated to the Cyber Security Policy document as requested in Ch 2, Sec 2, [3.2.3].

2 Vital Functions assessment

2.1 General

2.1.1 Objective

Risks identified the during ship's construction are focused on safety, cyber risks identified by the Shipowner should be also considered.

The comprehension of the Risk by Design is a way, for the Shipowner and crew members, to understand the cyber risk on systems and equipment, to manage it in a Cyber Risk Committee and take every days decisions.

2.2 Workflow

2.2.1 Vital functions

Vital functions must be identified, selected and justified by this Committee. Those vital functions may, for example, concern:

- information which is confidential for the Shipowner (e.g. performances, fuel consumption)
- business systems which are vital for operations (e.g. emails, procedures, schedules, productivity)
- personal and sensitive information (e.g. medical, passengers, cameras)
- IT/OT systems which are essential for the service delivered by the ship (e.g. passengers Wi-Fi, kitchen management).

The vital function list must faithfully reflect the Shipowner's convictions and concerns, and must therefore be consistent with his strategy. For example, passenger Wi-Fi on a cruise ship can be considered as vital as propulsion if this network allows passengers to get access to their cabins. The objective is not to deliver an exhaustive list of vital functions but to deliver a short relevant list of indisputable vital functions whom criticality has been established as a priority. This list, along with its justification, is to be included in the Cyber Risk Assessment.

Vital functions should not consider systems already secure by design (e.g. navigation systems or propulsion systems).

2.2.2 Threats on vital functions

By considering the internal and external context in which the ships operate, the Cyber Risk Committee is to identify the challenges to face for each vital function.

Threats on vital functions may be considered from:

- An external context: remote maintenance, difficult IT management, contractual external actors, political context, competitiveness
- The internal context: company strategic objectives, identified internal risks such as cyber training awareness of crew or extreme staff turnover making cyber training very difficult to manage, poor IT resource
- Any other threat as detailed in App 1, [2.3.3].

2.2.3 Vital functions impact index

Threats on vital functions are to be assessed with an index.

This grade is to characterize the level of impact relevant to the Shipowner needs as detailed in [2.2.1] and the threats on vital functions delivered in [2.2.2]. on vital functions:

- Superficial (VF1) is the index applicable to vital functions that are covered by the security measures. Of course, the risk still exists but the impact is considered as negligible.
- Major (VF2) is the index for vital functions covered by the security measures but which still need to be regularly tracked and presented at board level to satisfy the needs of cyber security as detailed by the Shipowner. In case of cyber attack, the impact would be considered as moderate and risk treatment may be applied to reduce the risk.
- Absolute (VF3) are vital functions whose risk is to be mitigated and followed-up during the service-life of the ship. Even if they are fully or partially covered by security measures, they request special care.

2.3 Documentation

2.3.1 A table is to sum up the following (see Tab 1):

- the vital functions
- the systems involved in the vital function
- the threats identified on the vital function
- the vital functions index (VF).

Table 1 : Risk on vital functions (RV)

Vital Function	System	Threats	Vital function Index (VF)
Supply Chain (Because the competition is known to be fierce between companies targeting the same clients, the Shipowner is aware that he can't afford a cyber incident that would tarnish his reputation.)	Cargo Management	Malicious or unexpected action during system maintenance	Major VF2
	Loading PC	Covered by Design	
	Emailing	Phishing	
	ERP	Ransomware	

3 Treatment opportunity

3.1 General

3.1.1 Objective

The Risk by Design may be reconsidered and re-evaluated with a justification. Shipowner may consider a risk as underestimated or overestimated.

In order to conduct this challenge, it is recommended that the Shipowner convene a risk committee, composed of IT/OT staff and competent representatives of all disciplines on board.

3.2 Workflow

3.2.1 Risk Level

The level of risk (RL) is to be calculated from:

- the Level of Criticality of the system (Level)
- the Vital Functions index (VF).

The Risk Level (RL) can be determined by using Tab 2 or from the following formula:

$RL = 2\ (VF + L - 1)$

Note 1: Levels of Criticality as calculated in the Criticality Assessment document are to be used as an entry point. For each system involved in the vital function analysis, the Level of Criticality is directly reported.

Note 2: For new construction, every system is protected by design and the risk has been mitigated by the Shipyard. But as far as it is, the Shipowner is responsible, during the service life of the ship, for ensuring protection measures and taking care of the system cyber security. From this, Level 3 systems endorse a criticality, meaning a risk, that, even if mitigated, shall not be forgotten. The risk already exists and current cyber security measures are to be applied and monitored.

Table 2 : Risk Level

	Level 1 Harmless	Level 2 Significant	Level 3 Critical
VF1 Superficial	RL2	RL4	RL6
VF2 Major	RL4	RL6	RL8
VF3 Absolute	RL6	RL8	RL10

3.2.2 Decision on treatment

The opportunity of treatment for risks identified on vital functions is to be applied with the following principle:

- treatment is optional for RL2
- treatment is appropriate for RL4 as systems are considered as being at risk with new threats identified by the Shipowner.
- treatment is required from RL6 as systems are critical or risk on vital functions is unacceptable.

In the second and third situations, a treatment on the risk shall be decided by the Cyber Risk Committee.

3.3 Documentation

3.3.1 Table

A table is to sum up the following (see Tab 3):

- system name (from Tab 1)
- level of Criticality (from the Criticality Assessment document defined in Sec 3)
- risk on Vital function (assessed in Article [2])
- risk Level (calculated in)
- treatment opportunity (decided from [3.2.2]).

Table 3 : Treatment opportunity table

System	Level of criticality	Risk on Vital function	Risk Level	Treatment opportunity
Cargo Management	Level 3	VF2	RL8	required
Loading PC	Level 2	VF2	RL6	required
Emailing	Level 1	VF2	RL4	appropriate
ERP	Level 1	VF2	RL4	appropriate

4 Risk Treatment

4.1 General

4.1.1 Overview

The Shipowner (Risk Committee) is to decide on the strategy to be adopted in order to treat risks, when necessary.

4.2 Workflow

4.2.1 Decision on Risk

The principle of risk mitigation is to reduce the risk by applying an effort. This effort can be summed up in 3 categories:

- null (take the risk without any security measure)
- treatment (actions are taken to reduce the risk)
- avoid (change the context in order to be disengaged from the risk).

4.2.2 Risk Mitigation

The decision on the risk is to be categorized from the herein below list:

- Assume (M0): there is no mitigation measures: the risk is assumed, effort is considered as null
- Aware (M1): human mitigation measures: raising crew cyber awareness, training crew
- Organize (M3): organizational mitigation measures: installing new procedures, introducing locks or room access controls
- Transfer (M5): use a third-party operator to cover the operation and, thus, the risk
- Detect (M6): technical mitigation measures: installing dedicated monitoring solutions with aboard equipment (e.g. IPS)
- Harden (M7): technical mitigation measures: adding a cyber security component (e.g. DMZ), using certified equipment
- Cover (M9): Using multiple mitigation measures (from M1 to M7)
- Avoid (M10): change the context in order to be disengaged from the risk.

4.2.3 Residual Risk

The residual risk (RR) is obtained from the subtraction of the mitigation (M) to the risk level (RL):

RR = RL – M

The mitigation is the effort to reduce the risk as demonstrated in Fig 2.

The following rules apply (as detailed in Tab 4):

- score greater than 8 refers to an unacceptable risk
- score between 3 and 8 refers to a moderate risk
- score lower than 3 refers to a limited risk.

Moderate and limited risks are considered residual risks.

Unacceptable Risks are not accepted and mitigation measures shall be reconsidered in order to evaluate the risk once more in an iterative process.

Limited risks still exist: limited does not mean removed. The limited risk means that the effort is in accordance with the risk level.

Note 1: The residual risk calculation is not to be considered when M10 Mitigation is applied (as avoiding the risk by changing the context, will disengage from the risk).

Risks already, always and still exist. The Risk Analysis goal is not to eliminate those risks, but to identify them in order to properly prevent them (Level of Equipment), monitor them and track them at board-level (see Fig 3).

Table 4 : Residual risk table of values

M	RL10	RL8	RL6	RL4	RL2
Assume (M0)	Unacceptable (10)	Moderate (8)	Moderate (6)	Moderate (4)	Limited (2)
Aware (M1)	Unacceptable (10)	Moderate (7)	Moderate (5)	Moderate (3)	Limited (1)
Organize (M3)	Moderate (7)	Moderate (5)	Moderate (3)	Limited (1)	Limited (1)
Transfer (M5)	Moderate (5)	Moderate (3)	Limited (1)	Limited (1)	Limited (1)
Detect (M6)	Moderate (4)	Limited (2)	Limited (1)	Limited (1)	Limited (1)
Harden (M7)	Moderate (3)	Limited (1)	Limited (1)	Limited (1)	Limited (1)
Cover (M9)	Limited (1)	Limited (1)	Limited (1)	Limited (1)	Limited (1)

Figure 2 : Residual risk evolution

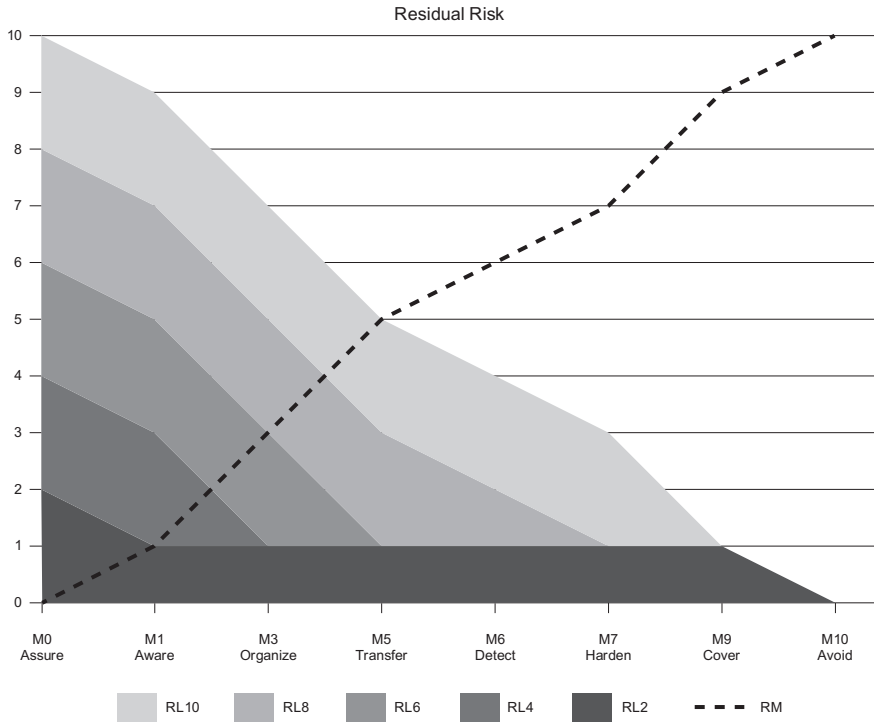
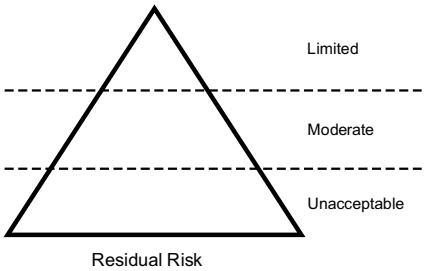


Figure 3 : Residual risk terminology



4.3 Deliverable

4.3.1 A table is to summarize the following (see Tab 5):

- system
- risk level (RL)
- risk mitigation (M)
- description of the mitigation
- residual risk (RR).

Table 5 : Risk treatment table

System	Risk Level (RL)	Risk Mitigation (M)	Description	Residual Risk (RR)
Cargo management	RL8	Organize (M3)	• Firewall configuration is checked every day • Password management policy is reinforced • Recovery plan is in place	Moderate
Loading PC	RL6	Aware (M1)	Crew members are aware about the loading PC security procedures	Moderate
Emailing	RL4	Cover (M9)	• Harden: Endpoint protection software is installed on every computer • Aware: Crew members are trained to thwart phishing • Detect: Multiple antivirus solutions are in place on endpoints, server and network	Limited
ERP	RL4	Harden (M7)	• Patch management policy requests an every day update • Server operating system is hardened • Recovery plan is in place	Limited

Section 6 Cyber Handbook

1 General

1.1 Framework

1.1.1 Objective

The Cyber Handbook is dedicated to the cyber security procedures applicable to on board equipment defined in [1.3.1].

Those procedures are under responsibility of the Shipowner and can also derive from procedures delivered by Shipyard and equipment suppliers.

1.2 Applicability

1.2.1 Ships

This Section is applicable to all ships to be assigned the additional class notation **CYBER MANAGED**, **CYBER RESILIENT** or **CYBER SECURE**.

1.2.2 Systems or equipment

The requirements of this Section are to be complied with by equipment suppliers for systems or equipment to be type approved.

1.3 Methodology

1.3.1 Ships methodology overview

This methodology (see Fig 1) applies to Shipyards or Shipowners for ships assigned the additional class notation **CYBER MANAGED**, **CYBER RESILIENT** or **CYBER SECURE**. Additionally, this methodology applies to equipment to be type approved.

The first step is to identify systems whose procedures will apply to:

- on board systems already type approved by the Society, if any, are to be listed as explained in [2.1]
- other ships systems which are eligible to procedures delivery are to identified as explained in [2.2]

The second step (explained in [1.4.2]) is to build the cyber handbook document by:

- gathering existing procedures from type approved equipment, if any
- writing procedures relevant to other eligible systems identified in the first step.

Systems included in the Cyber Handbook are the systems which are graded as i.e. Critical (LV3) in the conclusion of the Criticality Assessment.

- ONE: Outgoing Network Equipment
- INE: Interconnection Network Equipment
- SNE: Security Network Equipment
- L3E: Level 3 Equipment
- OVS: Outgoing Vessel System.

1.3.2 Type Approval methodology overview

This methodology (see Fig 2, explained in [1.4.3]) applies to suppliers for equipment to be type approved as detailed in [1.2.2]. It does not apply for assigning a classification notation to the ship.

The first step is to identify equipment for which the procedure is applicable.

The second step is to build the Cyber Handbook document by writing procedures relevant to identified equipment.

Figure 1 : Vessels methodology

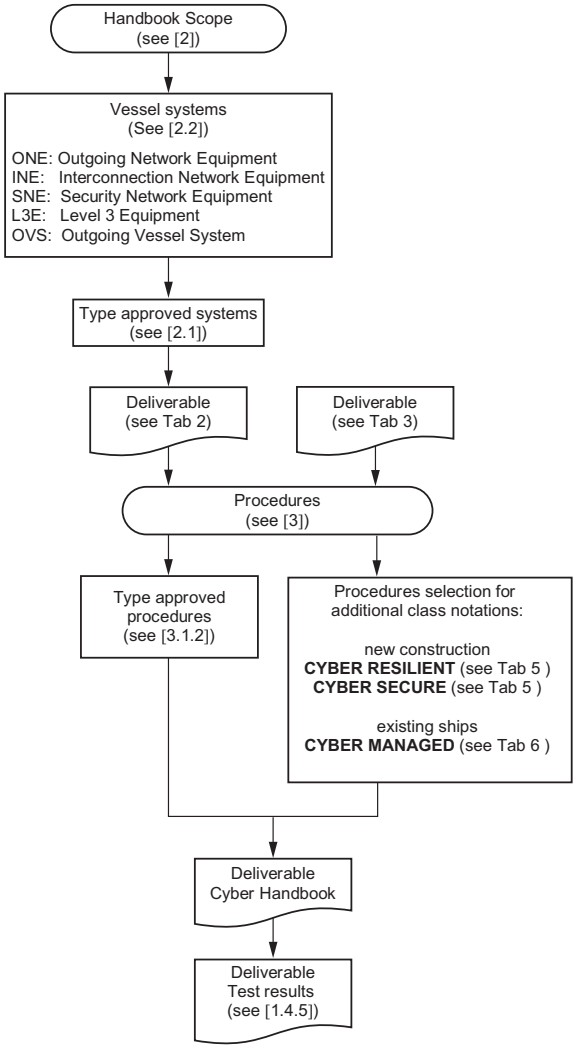
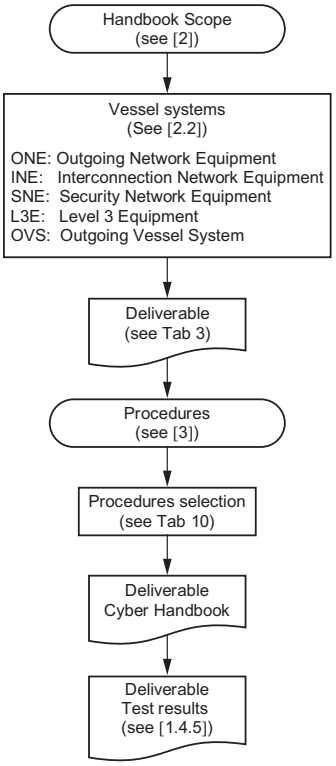


Figure 2 : Type Approval methodology



1.4 Documentation

1.4.1 General

The Cyber Handbook documents are to be submitted to the Society for approval in accordance with [1.2].

The entity responsible to deliver the documentation shall collect information by applying the methodology detailed in [1.3].

Documentation to be delivered by Shipowners for ships assigned the additional class notation **CYBER MANAGED**, **CYBER RESILIENT** or **CYBER SECURE** is detailed in [1.4.2].

Documentation to be delivered by suppliers for equipment type approved is detailed in [1.4.3].

1.4.2 Ship documentation

For an existing ship to be assigned the additional class notation **CYBER MANAGED**, **CYBER RESILIENT** or **CYBER SECURE**, the Shipowner is to deliver the Cyber Handbook document with the following entries:

a) The Handbook scope with:

- a table (see Tab 2) containing a list of systems selected in accordance with [2.2], referred to as “Ship Systems”
- a table (see Tab 1) containing a list of type approved systems, in any, in accordance with [2.1] referred to as “Type Approved Systems”.

b) A set of procedures, built from the two following sources:

- procedures gathered from equipment suppliers, as explained in [3.1.2], selected in “Type Approved Systems”
- procedures, to be delivered for each system listed in “Ship Systems”, and selected in accordance with Tab 5.

1.4.3 Type Approval documentation

For equipment to be type approved, the Supplier is to deliver the Cyber Handbook document with the following entries:

- the Handbook scope with a table (see Tab 2) containing a list of aboard systems selected in accordance with [2.2], referred to as “Ship Systems”
- a set of procedures, to be delivered by the Supplier for each system listed in “Vessel Systems”, and selected in accordance with Tab 6.

1.4.4 Approval

If, for operational, safety or any other justified reason, a rule cannot be fully or partially applied, substitute measures are to be proposed such as physical access control or organisational procedures.

When a rule cannot be applied (e.g. technical incapacity), the rationale is to be used to justify it.

Any exemption is to be justified and submitted for approval to the Society.

1.4.5 Maintenance

The Cyber Handbook document is to be updated should any change occur regarding the infrastructure, the architecture, the networks, the physical implementation of any system and equipment.

The update procedure of the Cyber Handbook document is to be integrated to the Change Management Plan (as required in Ch 2, Sec 2, [6.1.1]).

The maintenance policy of the Cyber Handbook is to be specified in the Cyber Security Policy document as requested in Ch 2, Sec 2, [3.2.1].

2 Handbook scope

2.1 Type approved systems

2.1.1 Systems installed on board and Type Approved on cyber security are to be summed up in a table (see Tab 1).

Table 1 : Type Approved systems

Type approved systems
Equipment X
Equipment Y

2.2 Ship systems

2.2.1 From the Cyber Inventory and the Criticality Assessment, the following equipment is to be listed in a table dedicated to the scope of compliance:

a) Network equipment (e.g. routers, switches) used:
   - from the ship to on shore – referred to as "Outgoing Network Equipment" (ONE)
   - from any aboard system to any other aboard system:
     - network equipment used to interconnect system is to be considered – referred to as "Interconnection Network Equipment" (INE)
     - network equipment dedicated to a system is not to be considered.

b) Any security equipment (e.g. firewalls, authentication servers) – referred to as "Security Network Equipment" (SNE)

c) Any equipment from criticality level 3 systems – referred to as "Level 3 System (L3S)"

d) Any equipment included in a system connected to on shore – referred to as "Outgoing Vessel System" (OVS). The following are excluded from this label:
   - network equipment
   - security equipment
   - level 3 systems.

3 Procedures

3.1 Introduction

3.1.1 Compliance

The compliance refers to the expected state of systems and equipment. The expected state is a set of elements which define how systems and equipment shall be installed and configured in order to operate in a normal and safe state. This set of elements is the compliance baseline.

The systems and equipment on which the compliance is to be defined, are to be listed in the "Handbook Scope" as explained in [2.2.1].

The expected state of those systems and equipment, here after named "Compliance Baseline", is to defined through different procedures:

- The monitoring of the Compliance Baseline applicable to the Handbook Scope is to be enforced using suitable Monitoring procedures as explained in [3.2].
- The maintenance of systems and equipment defined in the Handbook Scope is to be enforced using suitable Maintenance procedures as explained in [3.3].
- The incident response to apply in case of cyber incident on systems and equipment defined in the Handbook Scope is to be enforced using suitable Incident Response procedures as explained in [3.4].

3.1.2 Type approved procedures

Shipyard is to refer to the supplier in order to obtain the type approved equipment Cyber Handbook.

Procedures in the type approved equipment Cyber Handbook are to be used as is. This document is not to be re-written.

Type approved equipment Cyber Handbooks are to be gathered and delivered within the Cyber Handbook delivered by the Shipyard.

3.1.3 Procedures Selection

The selection of procedures to be delivered depends on two factors:

- the nature of ship systems as defined in [2.2]
- the classification notation to be assigned.

By using sorted Ship Systems table (see Tab 2), the procedures are to be defined for each system in accordance with the classification notation to be assigned (as explained in [1.4]).

For example, for a ship to be assigned the additional class notation **CYBER MANAGED**, whose systems would be listed in Tab 2, the procedures to be delivered should be selected from Tab 4.

With this example, the table of contents of the Cyber Handbook would contain the entries of Tab 3.

Table 2 : Ship systems

Outgoing Network Equipment
Equipment A
Equipment B
Interconnection Network Equipment
Equipment C
Equipment D
Security Network Equipment
Equipment E
Equipment F
Level 3 System
Equipment G
Equipment H
Outgoing Vessel System
Equipment I
Equipment J

Table 3 : Example of table of contents

Monitoring procedures
Physical interfaces
Procedures to be detailed for equipment A B E F G H I J
Networks
Procedures to be detailed for equipment A B
Security equipment
Procedures to be detailed for equipment E F
Remote access
Procedures to be detailed for equipment A B I J
Log events
Procedures to be detailed for equipment E F I J
Accounts
Procedures to be detailed for equipment A B I J
Maintenance procedures
Updates
Procedures to be detailed for equipment A B E F I J
Antivirus
Procedures to be detailed for equipment I J
Accounts
Procedures to be detailed for equipment A B I J
Incident Response procedures
Backup
Procedures to be detailed for equipment E F G H
Restore
Procedures to be detailed for equipment E F G H

Table 4 : Shipyard procedures for ships to be assigned the notations CYBER RESILIENT or CYBER SECURE

Procedure	Rule	Applicability				
		Network			System	
		ONE	INE	SNE	L3S	OVS
Monitoring procedures						
Physical interfaces	[3.2.2]	X		X	X	X
Networks	[3.2.3]	X				
Security equipment	[3.2.4]			X		
Remote access	[3.2.5]	X				X
Log events	[3.2.6]			X		
Accounts	[3.2.7]	X				X
Maintenance procedures						
Updating	[3.3.1]	X		X		X
Antivirus	[3.3.4]					X
Accounts	[3.3.6]	X				X
Incident Response procedures						
Backup	[3.4.2]			X	X	
Restore	[3.4.3]			X	X	

Table 5 : Shipowner procedures for existing ships to be assigned the notations CYBER MANAGED, CYBER RESILIENT or CYBER SECURE

Procedure	Rule	Applicability				
		Network			System	
		ONE	INE	SNE	L3S	OVS
Monitoring procedures						
Management	[3.2.1]	X	X	X	X	X
Physical interfaces	[3.2.2]	X		X	X	X
Networks	[3.2.3]	X				
Security equipment	[3.2.4]			X		
Remote access	[3.2.5]	X				X
Log events	[3.2.6]			X		X
Accounts	[3.2.7]	X				X
Maintenance procedures						
Updating	[3.3.1]	X		X		X
Patch management	[3.3.2]	X		X		X
Maintenance management	[3.3.3]	X			X	X
Antivirus	[3.3.4]					X
Antivirus management	[3.3.5]					X
Accounts	[3.3.6]	X				X
Accounts management	[3.3.7]	X				X
Incident Response procedures						
Loss of compliance	[3.4.1]	X		X	X	X
Backup	[3.4.2]			X	X	
Restore	[3.4.3]			X	X	
Availability management	[3.4.4]			X	X	

Table 6 : Supplier procedures for equipment type approval certificate

Procedure	Rule	Applicability				
		Network			System	
		ONE	INE	SNE	L3S	OVS
Monitoring procedures						
Physical interfaces	[3.2.2]	X	X	X	X	X
Networks	[3.2.3]	X	X	X		
Security equipment	[3.2.4]			X		
Remote access	[3.2.5]	X				X
Log events	[3.2.6]	X	X	X	X	X
Accounts	[3.2.7]	X	X	X	X	X
Compliance testing	[3.2.8]	X	X	X	X	X
Accounts monitoring	[3.2.9]	X	X	X	X	X
Maintenance procedures						
Updating	[3.3.1]	X	X	X	X	X
Antivirus	[3.3.4]				X	X
Accounts	[3.3.6]	X	X	X	X	X
Vulnerabilities management	[3.3.8]	X	X	X	X	X
Incident Response procedures						
Backup	[3.4.2]	X	X	X	X	X
Restore	[3.4.3]	X	X	X	X	X
Forensics	[3.4.5]				X	X

3.1.4 Procedures responsibilities

Procedures are to be the under responsibility of identified personnel either on board or on shore.

Each delivered procedure is to clearly identify supervisors of its proper, consistent and effective application.

Supervisors in charge of procedures are suggested in Tab 7 and divided in two categories:

- crew members when the procedure is to be executed at sea
- skilled personnel, generally from IT department, when the procedure is intended to be executed by cyber security skilled personnel.

Table 7 : Procedures responsibilities

Procedure	Supervisor
Monitoring procedures	
Management	crew members
Physical interfaces	crew members
Networks	skilled personnel
Security equipment	skilled personnel
Remote access	skilled personnel
Log events	skilled personnel
Accounts	crew members / skilled personnel
Compliance testing	crew members / skilled personnel
Accounts monitoring	skilled personnel
Maintenance procedures	
Updating	skilled personnel
Patch Management	skilled personnel
Maintenance management	crew members
Antivirus	skilled personnel
Antivirus management	skilled personnel
Accounts	skilled personnel
Accounts management	skilled personnel
Vulnerabilities management	skilled personnel

Procedure	Supervisor
Incident Response procedures	
Loss of compliance	crew members
Backup	crew members
Restore	crew members
Availability management	crew members
Forensics	skilled personnel

3.2 Monitoring Procedures

3.2.1 Management

A procedure is to describe the general management of cyber security.

This procedure is to detail

- the periodicity of monitoring operations
- situations when to alert the Cyber Security Officer
- emergency measures in case of suspicion of compromise system or equipment
- responsibilities when procedure is to be executed at sea by crew members
- responsibilities when procedure is intended to be executed by skilled personnel, generally from IT department.

3.2.2 Physical interfaces

A procedure is to describe how to visually check the compliance of physical interfaces (e.g. Ethernet).

This procedure is to detail how to visually check the compliance of:

- physical interfaces (e.g. cabled or not cabled; turned on or off)
- physical interface lockers, when used
- linked equipment connected to the interface (e.g. from the gateway to the satellite router).

Physical interfaces to consider are listed here below:

- USB ports
- Ethernet ports
- Port/USB Lockers
- Serial ports
- Buttons and switches (e.g. Programmable logic controller)
- DIP switches.

3.2.3 Networks

A procedure is to describe how to check network integrity.

This procedure is to detail how to check compliance of:

- routes (e.g. VLAN)
- network services (e.g. DHCP)
- traffic encryption mechanisms (e.g. IPSec)
- network equipment security mechanisms (e.g. roles and accounts, auditing)
- network equipment administration (e.g. SSH certificates)
- network clients (e.g. scan discovery on network).

3.2.4 Security equipment

A procedure is to describe how to check security equipment integrity and efficiency.

This procedure is to detail how to check compliance of:

- configuration (e.g. firewall rules)
- security mechanisms (e.g. roles and accounts, auditing)
- administration (e.g. SSH certificates)
- filtering (e.g. unauthorized packets shall not pass trough a firewall).

3.2.5 Remote access

A procedure is to describe how to check remote access activity. A real-time check is highly recommended.

This procedure is to detail how to:

- check events generated by security equipment (e.g. NGFW, IDS, IPS).
- perform specific actions to establish remote connection
- check authenticity of connections (e.g. white list of MAC/IP address or users).

3.2.6 Log events

A procedure is to describe how to check events generated by equipment.

This procedure is to detail how to:

- check events (e.g. log reader)
- check network events audit strategy (e.g. successful and failed authentication recording)
- manage alerts threshold (e.g. maximum number of failed attempts before logging)
- manage events storage (e.g. location, duration)
- detect unusual events (e.g. remove false positives).

3.2.7 Accounts

A procedure is to describe how to check that accounts and passwords are in line with cyber security principles.

This procedure is to detail how to check that:

- equipment is only operable through an access control mechanism based on identification (e.g. login) and single or multi factor authentication (e.g. password)
- generic and default accounts are deactivated
- individual users are linked to users groups (e.g. operators) without individual users credentials
- groups credentials are in compliance with the baseline
- credentials granted to groups have limited privileges
- passwords are robust (e.g. comparison with history, complexity).

3.2.8 Compliance testing

A procedure is to propose an automation of the compliance testing. This procedure may rely on checksum techniques and scripting tools to compare files on equipment with expected signatures.

This procedure is to detail how to:

- test the compliance of the equipment (e.g. self-test)
- interpret the results of this test
- operate in case of test failure.

3.2.9 Accounts monitoring

A procedure is to detail how to review users accounts.

This procedure is to detail how to:

- build an inventory of accounts
- check the date of creation
- check the date and time of last connection.

3.3 Maintenance procedures

3.3.1 Updating

A procedure is to describe how to keep equipment up-to-date.

This procedure is to detail how to:

- collect last updates (e.g. newsletter subscription)
- collect information about equipment latest vulnerabilities (e.g. supplier website survey, third party)
- verify safety of the equipment after equipment update (e.g. remote and local tests).

Note 1: As equipment vulnerabilities dramatically increase the risk of cyber attack, patch management and software updates are to be considered as a priority. Equipment shall be kept up-to-date with a strong process keeping in mind both cyber security and safety of the equipment.

3.3.2 Patch management

A procedure is to describe the patch management workflow.

This procedure is to detail who is in charge of:

- keeping equipment up-to-date (e.g. IT department)
- implementing updates (e.g. maintenance supplier)
- verifying safety of the equipment after equipment update (e.g. remote and local tests).

3.3.3 Maintenance management

A procedure is to describe rules about maintenance operations.

This procedure, under responsibility of the Master, is to explain how on board maintenance operation are to be previously agreed on:

- date and time of the start of maintenance operation
- scope of equipment impacted
- identity, skill and role of personnel involved in the operation
- tools and software used for maintenance (e.g. engineering software used to program PLC)
- hardware used for maintenance (e.g. third party laptop)
- estimated date and time of the end of maintenance operation
- sanitization procedure applied by the maintenance team to clean equipment used during maintenance operation (e.g. antivirus station for USB keys, antivirus report for laptops)
- verification procedure applied to start back the equipment after the operation
- any ingoing or outgoing equipment from or to the ship.

3.3.4 Antivirus

A procedure is to describe how the antivirus solution is to be kept updated.

This procedure is to detail how to:

- collect last updates (e.g. USB key)
- check integrity of the update (e.g. checksum)
- apply the update
- check antivirus status after installation (e.g. self-test)
- verify safety of the equipment after equipment update (e.g. remote and local tests).

3.3.5 Antivirus management

A procedure is to describe the antivirus management.

This procedure is to detail who is in charge of:

- implementing antivirus updates on board (e.g. crew member)
- checking antivirus status after update
- verifying safety of the equipment after antivirus update.

3.3.6 Accounts

A procedure is to describe human or technical interfaces dedicated to equipment accounts.

This procedure is to detail how to:

- create, modify, lock or delete users account
- manage roles and accesses.

3.3.7 Accounts management

A procedure is to describe equipment accounts management.

This procedure is to detail who is in charge of:

- monitoring legitimacy of accounts
- modifying credentials
- locking or deleting accounts.

3.3.8 Vulnerabilities management

A procedure is to propose Shipyards and Shipowners to be informed on the latest vulnerabilities and updates of the equipment (including operating system and third party software).

This procedure is to explain:

- where updates will be made available (e.g. website)
- how to enrol to be informed on update issue (e.g. email).

3.4 Incident Response Procedures

3.4.1 Loss of compliance

A procedure is to describe technical and organisational measures to apply to maintain the equipment in safety conditions in case of compliance failure.

This procedure is to detail:

- who is to be informed (e.g. cyber security officer)
- who is to take decision (e.g. master)
- physical actions to apply locally (e.g. equipment isolation).

Procedures are to be simple and designed to be implemented by any crew member and to respond both to emergency and to safety situations.

3.4.2 Backup

A procedure is to explain how to backup equipment.

This procedure is to detail how to:

- backup sensitive files, configuration, systems and assets
- store the backup (when on board).

3.4.3 Restore

A procedure is to explain how to restore equipment.

This procedure is to detail how to:

- locate the backup when it is stored on a logical device
- restore a previous backup in a safe and practicable way
- make the equipment ready to operate after restore operation.

3.4.4 Availability management

A procedure is to explain backup and restore management.

This procedure is to explain who is in charge of:

- equipment backup
- storing the backup
- deciding to restore the equipment
- restoring the equipment
- checking and deciding if the equipment is ready to operate after restore operation.

3.4.5 Forensics

A procedure is to explain how to investigate the equipment in case of cyber attack.

This procedure is to detail:

- how to investigate digital evidence with computer forensics tools (e.g. mount and read the file system)
- how to locate and read recorded activity.

Appendix 1 Methodology for Criticality Assessment

1 Methodology

1.1 General

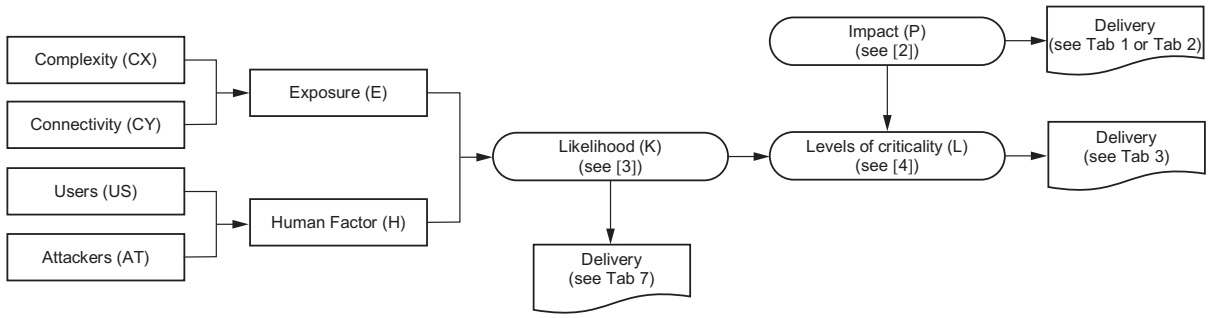
1.1.1 The Criticality Level (Level 1, Level 2 or Level 3) of a system or equipment is determined by assessing the Impact and the Likelihood (see Fig 1):

- The Impact relies on the assessment, in case of cyber attack, of the consequences on the vital functions leading to data leaks, loss of function or corruption of information. Impact is detailed in [2.1]
- The Likelihood is the result of the assessment of odds to be impacted by a cyber attack. This assessment relies on both technical and human factors as defined below:
  - the technical factor considers the connectivity and the complexity of the system or equipment
  - the human factor considers the risks coming from normal or malicious users.

Note 1: The probability of cyber attack is intrinsically linked to the Exposure. Connectivity assesses the probability to penetrate the system. Complexity assesses the probability of vulnerabilities exploitation.

Note 2: The frequency is determined by the Human Factor. Organized crime, by targeting a system or an equipment, will increase the frequency of attack. Unaware end users will increase the opportunities of attack.

Figure 1 : Criticality Assessment delivery workflow



1.1.2 Cyber assessment terms and définition

The definitions listed in Tab 1 are used in this Appendix in relation to the Criticality Assessment (see Sec 3), Design Assessment (see Sec 4) and Cyber Risk Assessment (see Sec 5).

Table 1 : Cyber assessment terms and définition

Term	Definition	Grade / Score	Reference
AT Attacker grade	AT defines the requested competencies to successfully achieve a feared hazard. Attacker grade is part of the human factor score H	AT1 to AT5	[2] [3.7]
CX Complexity grade	CX qualifies depth of parameters, amount of technologies and granted privileges of a system. Complexity grade is part of the exposure score E	CX1 to CX3	see [3.4]
CY Connectivity grade	CY qualifies aperture of a system regarding accesses, exchanges and communications. Connectivity grade is part of the exposure score E	CY1 to CY5	see [3.3]
E Exposure score	E measure the attack surface of a system. E is estimated from complexity grade CX and connectivity grade CY. Exposure score is part of the likelihood score K.	E1 to E5	see [3.2]
H Human factor score	H qualifies non-technical elements susceptible to affect a cyber-event. Human factor is part of the likelihood score K.	H0 to H4	see [3.5]
P Impact score	P qualifies effects in case of cyber attack. Impact may be negligible (P1), acceptable (P2), unacceptable (P3), high (P4) or catastrophic (P5). Impact is part of the level of criticality score L	P1 to P5	see [2]

Term	Definition	Grade / Score	Reference
L Level of criticality	L indicate the level of criticality of a system or equipment. It characterizes the vulnerability of a system or equipment to cyber threats. Level 1 (L1) indicates harmless systems. Level 2 (L2)indicates significant systems. Level 3 (L3) refers to critical systems.	L1 to L3	see [4]
K Likelihood score	K defines odds of having appearance of a feared hazard. K is based on Human factor score H and Exposure score E. Likelihood is part of the level of criticality L.	K1 to K9	see [3]
US Users grade	U defines the awaited competencies to successfully counter a feared hazard. Users grade is part of the human factor score H	US1 to US4	see [3.6]

2 Impact

2.1 General

2.1.1 Objective

The Impact on vital functions is assessed either by directly selecting a grade from the definition list or by developing threats and relevant effects.

The first method is the quickest one as it relies on the evaluation of consequences whatever the attack is. This method is recommended for the additional class notation **CYBER MANAGED** and detailed in [2.2].

The second method, detailed in [2.3], is more exhaustive and is to be preferred at design level (for the additional class notation **CYBER SECURE** or Type Approval of Equipment) to focus on high-risk system or equipment. This method will highlight applicable scenarios and will lead the Shipyard or the equipment supplier to technical or organizational counter measures.

For the additional class notation **CYBER RESILIENT** any of the aforementioned methods can be used.

2.2 First method

2.2.1 Objective

The objective of this first method is to assess the impact of a cyber attack on each system or an equipment of the ship by assigning a grade from a pre-determined list of impacts detailed in [2.2.4].

2.2.2 Deliverable

A table presenting the following elements is to be submitted for approval (see Tab 2):

- Equipment:

  Short description of the system or equipment.
- Confidentiality:

  Description of the effect, if any, in case of data leaks or disclosure as detailed in [2.2.3]. Attribution of an Impact grade in accordance with [2.2.4].
- Integrity:

  Description of the effect, if any, in case of corruption of the information as detailed in [2.2.3]. Attribution of an Impact grade in accordance with [2.2.4].
- Availability:

  Description of the effect, if any, in case of unavailability of the system or equipment as detailed in [2.2.3]. Attribution of an Impact grade in accordance with [2.2.4].
- Non-repudiation:

  Description of the effect, if any, in case of repudiation of action as detailed in [2.2.3]. Attribution of an Impact grade in accordance with [2.2.4].
- Impact:

  Assessed Impact grade for the system or equipment (generally selected from the highest grade attributed to confidentiality, integrity, availability or non-repudiation).

Table 2 : First method delivery example

Equipment	Confidentiality	Integrity	Availability	Non-repudiation	Impact (P)
Engine control	No confidential data (no impact)	Orders need to be secured. Invalid order may to lead to ship loss (Impact 5)	Engine control is backup by a local control in application of the SOLAS	In case of accident, lack of traceability of orders may lead to legal sue (Impact 3)	5 (highest score from this line)

2.2.3 Effects assessment

The assessment of the effects relies on the four pillars of the cyber security which are confidentiality, integrity, availability and non-repudiation. The principle of this assessment is to answer to the following questions to evaluate the relevant impact on safety, operations, human, environment or business as detailed in [2.2.4]:

- Confidentiality:

  It refers to any information which shall not be disclosed (authentication, personal information, cargo contents, location, competitive know-how or any other sensitive data). If such information is to be considered from unauthorized viewers, the impact in case of disclosure is to be assessed.

- Integrity:

  It refers to any information which, when modified, may lead to wrong, falsified or unexpected display or behaviour of a system or equipment. If such information is to be considered, the impact in case of alteration is to be assessed.

- Availability:

  It refers to any system of equipment which may be unavailable because of a cyber attack (e.g. denial of service, ransomware) and whose unavailability is to be considered. In such case, the level of impact of the unavailability of those systems and equipment shall be assessed.

- Non-repudiation:

  The non-repudiation is a way to deliver the proof of the origin of an action of the systems. When applied, the non-repudiation may be used to investigate incidents but also may be used as a legal proof. If actions linked to a system or an equipment are to be traced in this way, the loss of traceability, and thus the loss of non-repudiation, shall be considered. The level on impact of uncontrolled origin of the action shall be assessed.

2.2.4 Impact assessment

The impact grade is determined according to the following definitions:

- Impact 1:

  Negligible. System could be shutdown without any significant effect. No human nor environmental impacts are involved.

- Impact 2:

  It refers to an acceptable impact which may be one or more of the following:

  - shutdown of the system means a pointed disrupt of the service
  - environmental impact is in the standard margin and has no consequence but to be declared to authorities
  - event could lead to labour disruption because of injuries and medical treatment.

- Impact 3:

  It refers to an unacceptable impact which may be one or more of the following:

  - loss of system activity is significant (e.g. email system is off and IT department needs time to recover)
  - Shipowner request investigations from a third-party committee (e.g. unexplained disruption of business activity, loss of non-repudiation traceability)
  - loss of confidential information (e.g. data leaks, competitive know-how disclosure)
  - financial loss are considered unacceptable by the Shipowner
  - fraud and money steal
  - cargo and goods stealing
  - tarnished reputation
  - environmental impact is limited
  - limited loss of competitiveness and financial impact
  - human impact leads to permanent disability.

- Impact 4:

  It refers to a high impact which may be one or more of the following:

  - physical systems damages (e.g. material breakage)
  - permanent loss of the system without standard restoration process (e.g. ransomware) to restart it in its operational state
  - ship is off (e.g. cargo management is off)
  - the regulatory asks for investigation
  - illegal trafficking
  - significant pollution conducts to people evacuation
  - long-term loss of competitiveness
  - human impact leads to death.

- Impact 5:

It refers to a catastrophic impact which may be one of the following:

- physical systems destruction (e.g. fire, explosion)
- loss of the ship (e.g. collision or grounding)
- fleet is off (e.g. systems blackout, legal investigations)
- environmental disaster (e.g. major pollution) with long-term environmental consequences.
- financial loss conducts to Shipowner bankruptcy.
- human impact leads to multiple deaths or crew, passengers kidnapping.

2.3 Second Method

2.3.1 Objective

The objective of the second method is to assess the impact of a cyber attack on a system or an equipment by confronting it to a list of cyber threats. For each relevant scenario, effects are estimated and an grade of Impact is figured out. For each system or equipment, the highest Impact grade from the evaluated threats will determine its Impact grade.

2.3.2 Deliverable

A table representing the following elements is to be submitted for approval (see Tab 3):

- System:

  Short description of the system or equipment.
- Threat:

  For each system or equipment, a selection of threats, when applicable, is to be detailed. Those threats may be selected from [2.3.3]. Multiple threats may be applicable.
- Effect:

  For each threat, a description of effects, if any, is to be delivered in accordance with [2.2.3].
- Impact:

  For each effect, an Impact grade is to be assigned in accordance with [2.2.4].

Table 3 : Second method delivery example

System	Threat	Effect	Impact
Cargo Control	Loss of important data due to infection of removable media	• OPERATION SHUTDOWN: ship is stuck in harbour during forensics operations • CARGO: Cargo can't be delivered or may not been delivered correctly • FINANCIAL LOSS: Possible legal actions, possible huge commercial penalties	4
		TARNISHED REPUTATION: Media cover is not favourable to the company	2
	Important information leakage using web applications	TARNISHED REPUTATION: Loss of customer	2
		LOSS OF COMPETITIVENESS: Sensitive commercial data are used by rival companies to their profit	2
	Malicious code or software execution	CARGO: Cargo shipping inventory is not reliable, operations are delayed	3
		LOSS OF COMPETITIVENESS: A key customer denounces contracts	3

2.3.3 Threats

The following general threats are suggested. This list is non-exhaustive and the Shipowner or equipment supplier may introduce new threats if needed.

- Nefarious activities
  - Brute force (Non-repudiation):

    Aboard or remotely, an attacker or a physical device, may try to gain unauthorized access to a system or equipment through a infinite loop of attempts to guess authentication information. E.g.: Rainbow tables are well-known techniques used by brute force attackers to guess credentials. IT and OT systems using generic authentication systems may be vulnerable to generic tools embedded in hacking suites.
  - Denial of Service (Availability):

    Aboard or remotely, a multiple number of computers or a single physical device, send massive data or requests to a system, a network or an equipment. Such attack floods the equipment by generating memory overflows or excessive CPU occupancy. E.g.: Range of infected computer (called zombies) may be employed by an attacker to deny access to on shore systems used by aboard equipment.
  - Malware (Confidentiality, Availability, Integrity, Non-repudiation):

    A malware installed aboard may exploit equipment's operating systems, services or software vulnerabilities to gain privileges. Such escalation elevates the rights of the unauthorized process which can try any action.

- Social Engineering (Confidentiality):

  The attacker can use human interactions to obtain or compromise information about ship organization and processes by asking questions, by pretending to be another person and gathering information he needs. The attacker can ask several sources by relying on information he can get from the fist source to add to his credibility or send malicious links. E.g.: Generic passwords used by maintenance third party may be collected by social engineering. Such information would be used to forge malware and gain access to secure sensitive equipment.

- Manipulation of data (Integrity):

  Aboard system or equipment or on shore system used by aboard equipment, is modified in order to manipulate data. Corrupted information would be used by aboard equipment, misleading systems and crew members. E.g.: charts corruption on Internet website).

- Phishing (Confidentiality):

  Crew members receive falsified emails or connect to trustworthy corrupted web sites. From this, hackers will infiltrate aboard computers to introduce malware. E.g.: Crew members receive an email with a link to a recognized and trusted website but the web address contains minor difference which cannot be detected by the human: a common character may be replaced by a similar one, leading the user to a web site which will collect its credentials or will introduce a malware aboard.

- Geo-localization spoofing (Integrity):

  The attacker spoofs GPS or AIS signal by sending short distance corrupted signal. When undetected by crew members, this leads to navigation error.

- Targeted attacks (Confidentiality, Availability):

  An organization invests in a sophisticated attack to get control of a system or equipment. This may lead to fleet or fleet blackout. E.g.: Rare OT attacks in oil industry led to system disruption or explosion.

- Abuse and theft of data (Confidentiality, Integrity):

  The hacker, through different means, steals sensitive data (personal data, freight tracking data, operational data…) and/or abuses the certificates used in the ship operations. E.g.: Cargo may be targeted and manipulated in order to be unloaded at the wrong port or loaded with illicit contents.

- Network manipulation and Information gathering (Confidentiality, Non-repudiation):

  Aboard or remotely, attackers may sniff networks to gather intelligence. Such information is typically used to target vulnerable systems and equipment. E.g.: Passenger ships may host an attacker getting sensitive information from the public Wi-Fi network. Such information may be used to get access to the gateway or get through the firewall. At this point, aboard operational network may be compromised and considered unsafe.

- Man-in-the-middle (Confidentiality, Integrity, Non-repudiation):

  Aboard and remote networks may be listened, recorded and reverse engineered to gather information, modify packets or replay commands. E.g.: A rogue Wi-Fi hotspot may be introduced aboard or while at port, to collect network traffic.

• Physical attacks

  - Unauthorized physical access:

    A crew member or an unauthorized user, intentionally uses access to a physical port (USB or Ethernet) to connect a spy device or a hacking tool. This may lead to any nefarious activity as detailed hereinbefore.

  - Authorized physical access:

    A crew member or a maintenance third party employee, connects an infected device to a network (e.g. infected laptop) or a removable media (e.g. infected USB key). This action spreads a virus through the network which gains access to the system or equipment.

• Unintentional actions

  - Erroneous use or administration of devices and systems:

    Erroneous administration can jeopardize the proper functioning of ship systems. E.g.: Crew members may try to optimize an OT system by using infected tools downloaded from the Internet. Those tools may contain remote access toolkit which, when used by a remote attacker, may lead to loss of control of the equipment.

  - Erroneous penetration testing (Availability):

    In order to test the ship IT or OT security level, the Shipowner may order penetration testing which, if not carried out properly, can damage the systems. E.g.: Some penetration tools check operating systems vulnerabilities which, when discovered, may freeze the equipment or leave unexpected files. Such actions may trespass supplier's conditions of usage and cancel contractual guarantees.

  - Use of unreliable source (Integrity, Availability):

    The IT department of staff members in charge of maintenance may apply defective updates or irrelevant patches.

  - Deletion/change of data (Integrity):

    OT and IT system use sensitive commands and parameters. They may be unintentionally executed or modified by crew members, leading to unexpected situations. Such situation, when identified, shall be covered by technical or human double-check.

- Third party security failure:

  If aboard equipment or remote services are not correctly managed by the suppliers, vulnerabilities may appear. Such security breaches would directly affect the ship.

- Information leakage (Confidentiality):

  Crew members, on shore employees or third parties may share, by mistake or ignorance, sensitive data if there is insufficient awareness or data protection solutions.

3 Likelihood

3.1 General

3.1.1 Likelihood calculation

Likelihood describes the odds of being under attack.

Likelihood (K) is the result of the addition of Exposure (E) and Human Factor (H).

Likelihood = Exposure + Human Factor

K = E + H

Scoring Exposure (E), Connectivity (CY) and Complexity (CX) of the equipment is achieved by using [3.2].

Scoring the Human Factor (H), Users (US) and Attacker (AT) is achieved by using [3.5].

3.1.2 Deliverable

A table containing details of likelihood assessment is to be submitted for approval (see Tab 4).

Table 4 : Likelihood delivery example

Equipment	Effects assessment						Likelihood (K)
	Exposure			Human Factor			
	Connectivity	Complexity	Exposure score	Users	Attackers	Human factor score	
Engine Control	Bridge is interconnected to engine. The engine control is not connected to anything else. This is a closed system (CY2) grade is CY2	Engine control contains programming workstation for automation updates. Because of the programming stations, it is living system (CX2) grade is CX2	score is E2	Aware users grade is US1	Standard attacker grade is AT3	score is H1	E2 + H1 = K3

3.2 Exposure (E)

3.2.1 Definition

The calculation of exposure requires to deliver a score for connectivity and complexity. The system integrator is to evaluate connectivity of each system. To limit rules impact regarding the final Level (1, 2 or 3), system integrator may consider to adapt design of the ship by limiting connectivity to meet the needs without excess.

3.2.2 Exposure score

The exposure score is the combination of Complexity (CX) and Connectivity (CY) as defined in Fig 2.

- for Complexity 1, the Exposure Score equals the Connectivity Level
- for Complexity 2, the Exposure Score equals the Connectivity Level, no less than 2
- for Complexity 3, the Exposure Score is:
  - 3 when Connectivity is 1 or 2
  - 4 when Connectivity 3 or 4
  - 5 when Connectivity is 5.

Figure 2 : Exposure score (E)

COMPLEXITY \ CONNECTIVITY	CY1	CY2	CY3	CY4	CY5
CX1	E1	E2	E3	E4	E5
CX2	E2	E2	E3	E4	E5
CX3	E3	E3	E4	E4	E5

3.3 Connectivity (CY)

3.3.1 Definition

The Connectivity grade (CY) is dedicated to the assessment of the interfaces, interconnections and networks of the system or equipment. A high grade indicates a high likelihood of cyber attack. A low grade refers to a low likelihood.

This grade is ranging from CY1 to CY5. It is to be selected by assessing different components of the system's interfaces as summarized in Tab 5.

3.3.2 Isolated systems (CY1)

Isolated systems are systems without any connection to any other system.

The grade CY1 (connectivity one) is granted to:

- isolated equipment
- isolated cabled systems (see Fig 3).

For isolated cabled system, when using network components, the following rules are to be complied with:

- the system relies on a dedicated, isolated, local network
- operations are dedicated to the system itself
- any data exchange is dedicated to the system itself
- usage of network equipment is accepted when dedicated to the closed local area network.

The following usage are prohibited:

- any connection to any other system
- access to the internet
- usage of Wi-Fi equipment.

Figure 3 : Isolated cabled system

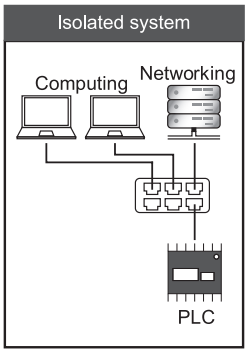


Table 5 : Elements of connectivity assessment

Elements of connectivity	Isolated Systems CY 1	Closed Systems CY 2	Authenticated Systems CY 3	Demilitarized Zones CY 4	Filtered Systems CY 5
Wi-Fi	No	No	Yes	Yes	Yes
Connection to another system	No	Yes	Yes	Yes	Yes
One-way communication	n.a.	• Yes (diode) • No (isolated networks) • No (IPsec tunnel)	No	No	No
Note 1: n.a. means not applicable					

Elements of connectivity	Isolated Systems CY 1	Closed Systems CY 2	Authenticated Systems CY 3	Demilitarized Zones CY 4	Filtered Systems CY 5
Connection to ashore system	n.a.	• Yes (diode) • No (isolated networks) • No (IPsec tunnel)	Yes	Yes	Yes
Transport encryption	n.a.	Yes	Yes	• No • Yes (for privileged accounts)	No
Data encryption	n.a.	Yes	Yes	Yes	No
Privileged accounts	n.a.	• Yes (diode) • No (isolated networks) • No (IPsec tunnel)	Yes (on board)	Yes (ashore)	No
DMZ	n.a.	• Yes (diode) • No (isolated networks) • No (IPsec tunnel)	No	Yes	No
Note 1: n.a. means not applicable					

3.3.3 Closed systems (CY2)

Closed systems are isolated systems which are connected to one or more other isolated systems by using robust security mechanisms to exchange data.

The grade CY2 (connectivity two) is granted to:

- systems using unidirectional gateway (see Fig 4)
- isolated network connected to any isolated network
- IPsec tunnels (see Fig 5).

This grade is not granted to systems using Wi-Fi equipment.

For systems using unidirectional gateway, the following rules are to be complied with:

- both systems are to be aboard
- the unidirectional gateway relies on one proxy installed in the local system and another proxy installed in the second system
- the proxies create a disruption in the communication protocol between the two systems
- one of the proxy send data to the other one in a one-way direction
- the direction of the data flow goes either from the local system or to the local system
- a physical device (diode) is installed between the two proxies to ensure the partition of the networks
- the physical nature of the diode ensures a unidirectional network connection
- each proxy is configured in order to run only with the predetermined connection points
- error correction is to be used during data transmission
- data encryption is to be used during data transmission.

For isolated network connected to any isolated network, the following rule is to be complied with:

- both systems are to be aboard
- both systems are part of a global solution (e.g. the second system is the management system of the local system)
- transport encryption is to be used.

For systems using IPsec tunnels, the following rules are to be complied with:

- there is no restriction regarding the ways of connection
- there is no restriction regarding the location of the systems
- communications between the local system and any other system are ensured by the usage of virtual private networks (VPN)
- IPsec is implemented in tunnel mode
- the entire IP packet is encrypted and authenticated
- IPsec is to be implemented in accordance with Ch 4, Sec 3, [4.1.2].

Figure 4 : Unidirectional gateway (CY2 example)

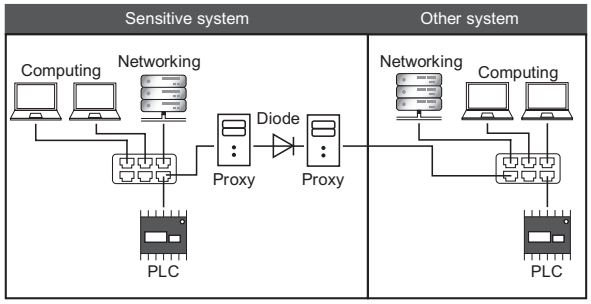
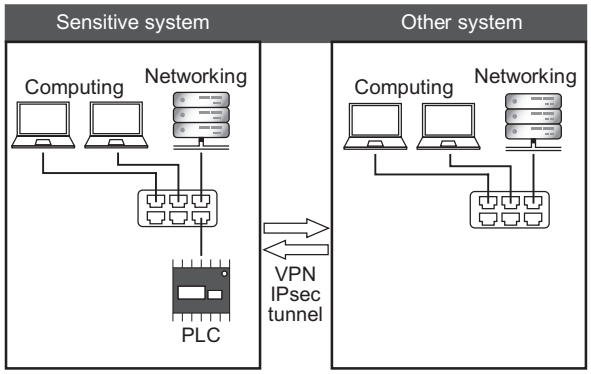


Figure 5 : IPsec tunnel (CY2 example)



3.3.4 Authenticated systems (CY3)

Authenticated systems are systems using, at transport layer, identification, authentication and encryption mechanisms relying on shared third party network equipment.

The grade CY3 (connectivity three) is granted to:

systems connected to systems with transport mode encryption (see Fig 6).

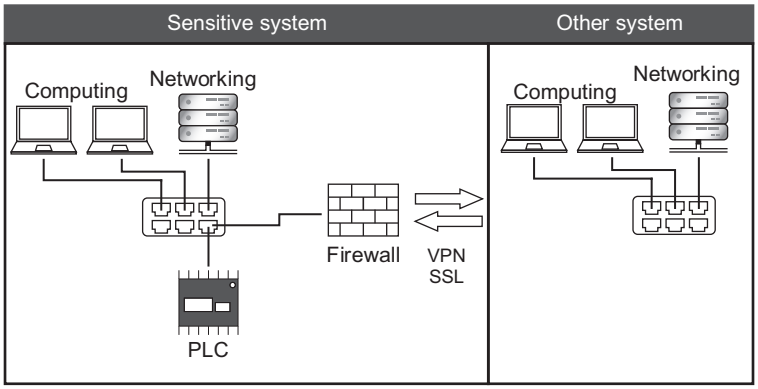
For systems connected to systems with transport mode encryption, the following rules are to be complied with:

- there is no restriction regarding the ways of connection
- both cabled and wireless networks are accepted
- there is no restriction regarding the location of the systems
- the transport layer and the payload packets are to be encrypted
- IPsec in transport mode is a recognized solution when the authentication header is implemented
- SSL VPN is a recognized solution when a dedicated VPN gateway is used in the local system
- a firewall is to be implemented in the local system.

The following usage is prohibited:

usage of high privilege accounts from ashore systems (e.g. system administration, software update).

Figure 6 : Encrypted transport (CY3 example)



3.3.5 Demilitarized Zones (CY4)

Demilitarized zone are areas which prevent direct connection from one system to another one.

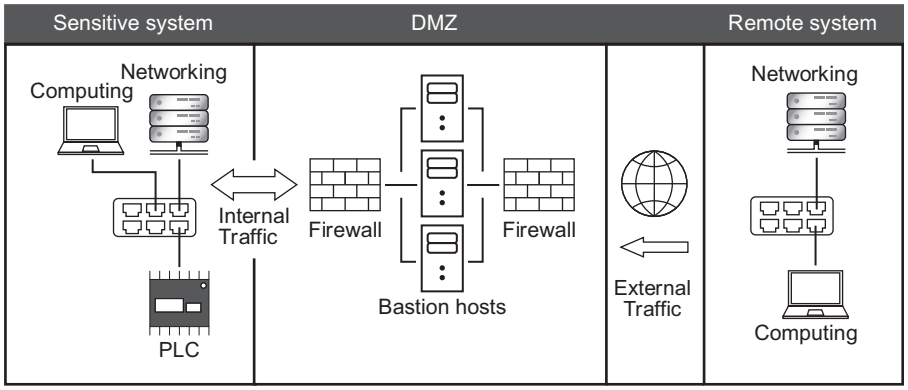
The grade CY4 (connectivity four) is granted to:

Demilitarized Zones (DMZ) (see Fig 7).

For Demilitarized Zones, the following rules are to be complied with:

- there is no restriction regarding the ways of connection
- there is no restriction regarding the location of the systems
- local system is connected to a system by relying on a traffic disruption endorsed by a bastion host
- the bastion host is installed in a demilitarized zone
- each side of the demilitarized zone is protected by a firewall
- high privilege accounts used from ashore systems (e.g. system administration, software update) are accepted with strong authentication system and SSLVPN.

Figure 7 : Demilitarized Zone



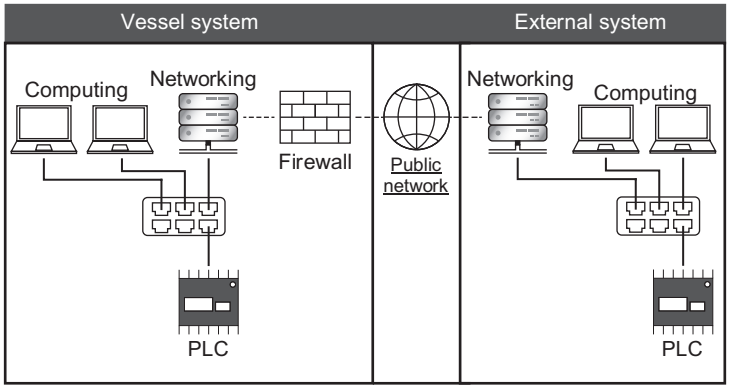
3.3.6 Filtered systems (CY5)

Filtered systems are systems whose security depends on one or more firewalls. Firewalls filtering rules are considered to be designed and properly configured to limit the traffic to authorized packets only.

The grade CY5 (connectivity five) is granted to:

- systems connected to another system with a dedicated firewall appliance (see Fig 8)
- group of systems connected to another system with a shared firewall appliance.

Figure 8 : Filtered systems



3.4 Complexity (CX)

3.4.1 Definition

The Complexity grade (CX) is dedicated to the typology of the equipment involved in a system and to the assessment of its operability, management and administration. A low grade refers to systems having a relative stability in term of configuration. A high grade refers to complex systems whose profile may change frequently.

This grade is ranging from CX1 to CX3.

The operability refers to any on board operations under responsibility of crew members.

The management refers to any on board or on shore operations dedicated to the global management for aboard system (e.g. account creation, patch management, log management, etc.).

The administration refers to operations which request a high level of privileges (e.g. firewall rules modification).

3.4.2 Standalone systems (CX1)

Standalone systems refers to systems or equipment whose software, configuration files and operating systems are relatively stable while being executed (see Fig 9).

For standalone systems, the equipment list shall be restricted to one or more of the following:

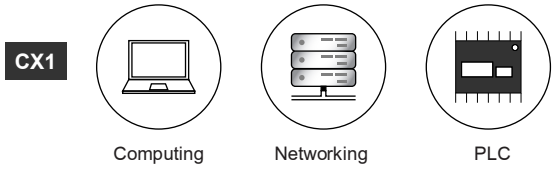
- any workstations
- any end-user endpoints operated thanks to a standard operating system like Windows, Linux, Android or macOS
- any light servers used to file storage, printing services or any other local service
- any sensor, controllers and control command connected to OT networks
- any industrial automation and control systems (IACS) operated thanks to a firmware
- any programmable devices (DCS, PLC, SCADA).

Moreover, the following rules shall be complied with for the operability, management and administration of standalone systems:

- restoration procedures are easy to apply
- operations linked to the usage of equipment by crew members are detailed in procedures
- management of the equipment is organized with clear documentation
- requests for administration of the equipment are rare.

Systems including a Compliance and Software Registry (CSR) Security Solution (as defined in Ch 5, Sec 5, [2]) or equivalent, are granted CX1.

Figure 9 : Standalone systems



3.4.3 Living systems (CX2)

Living systems refers to systems or equipment whose software, configuration files or operating systems are modified or updated daily (see Fig 10).

Living systems are systems which contain one or more of the following typology of equipment:

- any identification and authentication servers
- any maintenance equipment used to program any part of the system
- any database management systems
- any network equipment whose rules or configuration are modified more than once per week
- any virtual machine monitors
- calculators
- any smart equipment used to take decision having a direct effect on ships' operations.

Living systems include equipment whose operability, management and administration may be defined as one or more of the following:

- restoration procedures cannot be handled at sea or request more than 24 hours
- crew members need support from on shore for some operations
- management of the equipment is not clearly documented or shared and relies on third parties
- administration of the equipment is based on weekly or daily activity
- administration relies on experts.

Figure 10 : Living systems

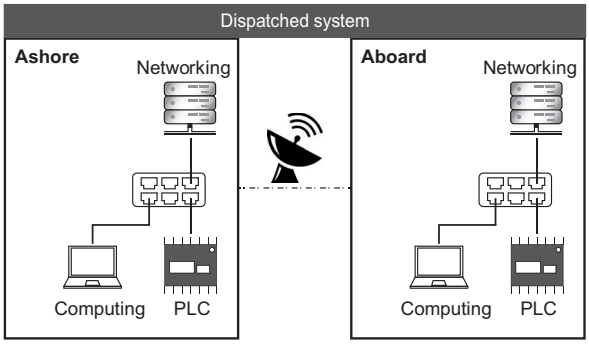
3.4.4 Dispatched systems (CX3)

Dispatched systems refers to systems whose operability and efficiency requires equipment dispatched through remote or distributed architecture (see Fig 11).

For dispatched systems, the equipment list shall be restricted to one or more of the following:

- unmanned vessels
- swarm robotics
- distributed system architectures.

Figure 11 : Dispatched systems



3.4.5 Adjustments on complexity grade

The following adjustments on complexity grade are to be done:

- for assignment of the additional class notation **CYBER SECURE**, or
- for seeking Type Approval Certificate for equipment / system,

during the assessment of a system or equipment, the score of complexity may be decreased or increased depending of the following parameters:

- opacity of responsibilities: Complexity of global on shore / aboard ecosystems and stakeholder (e.g. unclear roles, unclear third parties) may increase the grade
- imbalance between efficiency and cybersecurity: priorities to functional requirements may increase the grade when the cyber security management is not considered (e.g. equipment use generic account)
- any technical opacity in the systems or equipment's architecture (e.g. internal design of sub-networks is not delivered) may increase the grade of complexity while a mastered system may decrease it
- strong interdependencies (e.g. many unclear interactions, components, software…) may increase the grade while clear description of interconnections and security measures would decrease it
- new cyber risks from digital transformation (e.g. high connectivity to on shore 3rd party) are to be considered with an grade CX3 when the stakeholders involved provide insufficient information regarding cybersecurity.

For the additional class notations **CYBER SECURE** or **CYBER MANAGED**, during the assessment of a system or equipment, the score of complexity may be decreased or increased depending of the following parameters:

- lack of digital culture in the ecosystem (e.g. outdated equipment due to IT department inaction) will increase the grade while a strong culture will decrease it
- legacy systems and practices (e.g. outdated versions due to lack of equipment maintenance by the supplier) will definitely increase the grade
- difficulties to stay up to date with latest threats (e.g. updates are not installed) will automatically increase the grade while a efficient patch management policy may decrease the grade
- supply chain challenges (e.g. traceability of maintenance tasks) will increase the grade while a controlled supply chain (e.g. hardware and software traceability and factory acceptance tests) would definitely decrease the grade.

3.5 Human factor (H)

3.5.1 Definition

Human Factor (H) is the conjunction of users' level of maturity and attackers motivation. On one hand, users training and activity recording is taken into account. On the other hand, attackers hacking skills are evaluated.

3.5.2 Human factor score

The Human Factor score H is assessed using Users grade (US) and Attackers grade (AT) according to Tab 6.

Table 6 : Human Factor (H)

Attackers' grade	Aware users US1	Controlled users US2	Accredited users US3	Any users US4
Unintentional attacks (AT1)	H0	H1	H1	H2
Malicious attacks (AT2)	H1	H1	H2	H2
Standard attacks (AT3)	H1	H2	H2	H3
Criminal attacks (AT4)	H2	H2	H3	H3
Cyberwarfare (AT5)	H2	H3	H3	H4

3.6 Users (US)

3.6.1 Definition

The Users grade (US) is ranging from US1 to US4 taking into account the level of training of the users and conditions of accessibility to the equipment. The first level (US1) refers to systems and equipment having cybersecurity mechanisms dedicated to identification and authentication of trained users. The last level (US4) is to be applied for systems and equipment having a low level of security and, or, accessible to uncontrolled users. A low grade reduces the likelihood of cyber attack.

The assessment of this grade shall not only consider the credentials and the awareness of the end-users but shall also take into account any access control of the equipment and activity monitoring (summarized in Tab 7) as defined here below:

- The credentials of end-users refers to the access policy for the equipment. Credentials may be:
  - nominatives (users shall use dedicated users accounts with private password to operate the equipment
  - generic (users use generic accounts to get access to the equipment)
  - global (users getting physical access to the equipment are considered authorized).
- The awareness of the end-users means that those users are aware of cybersecurity risks. This awareness may be the result of a dedicated training or the application of on board procedures applied to the access management of the equipment.
- The access control of the equipment refers to access requirements. They may be physical and, or, logical:
  - physical protection may use a locker or any physical barrier. The access control (e.g. a key) shall to be under responsibility of the security officer.
  - logical protection shall be based on identification (e.g. login with user name) and authentication (e.g. password, fingerprint).
- The activity monitoring refers to the recording of any access of the equipment. Monitoring may record both successful and unsuccessful login events. Monitoring may also record both login and logout activities.

Table 7 : Users profiles (US)

Users' grade	Credentials	Awareness	Access Control	Activity Monitoring
Aware users (US1)	Nominative	Yes	Yes	Always
Controlled users (US2)	Generic	No	Yes	Partial
Accredited users (US3)	Global	No	No	No
Any users (US4)	No	No	No	No

3.6.2 Aware users (US1)

In application of [3.6.1], aware users (US1) are users and equipment observing the following rules:

- nominatives credentials are mandatory
- users are aware of cybersecurity risks
- access control is mandatory. Logical access is mandatory but physical access is recognized when logical access is not applicable.
- activity monitoring records:
  - both successful and unsuccessful accesses
  - both login and logout activities
  - In case of physical access control, any access to the equipment is to be manually recorded in the logbook with date of the access, name of the user and name of the granting officer.

Systems which are covered by an Intrusion and Detection Gate (IDG) Security Solution (as defined in Ch 5, Sec 5, [3]) or equivalent, are granted US1.

3.6.3 Controlled users (US2)

In application of [3.6.1], controlled users (US2) are users and equipment observing the following rules:

- nominatives or generic credentials are mandatory
- logical or physical access control is mandatory
- activity monitoring records:
  - unsuccessful accesses, at a minimum
  - login activities, at a minimum.

3.6.4 Accredited members (US3)

In application of [3.6.1], accredited users (US3) are any global users authorized by the system to get access to its operational mode.

3.6.5 Any users (US4)

The grade US4 is to be applied to any equipment not based on the usage of credentials.

3.6.6 Adjustments on users grade

For the additional class notation **CYBER SECURE**, **CYBER RESILIENT** or **CYBER MANAGED**, during the assessment of a system or equipment, the user level may be decreased or increased depending of the following parameters:

- lack of time and budget allocated (e.g. low reactivity, no team in place) will increase the grade while a budget dedicated to cyber security teams will decrease the grade.
- lack of awareness and training (e.g. technical cabinet managed by the equipment supplier only) will increase the grade while a strong effort on crew training will decrease the grade.
- lack of HR and qualified people (e.g. IT department using a firewall without the competencies on how to configure it) will increase the grade while dedicated IT and OT support will decrease the grade.
- usage of a cleaning station, (see Intrusion and Detection Gate (IDG) Security Solution defined in Ch 5, Sec 5, [3]) or equivalent, will deliver US1 grade.

3.7 Attackers (AT)

3.7.1 Definition

The Attack grade (AT) is ranging from AT1 to AT5, depending on the level of competence of the attacker. The first grade (AT1) corresponds to the lowest level and the last grade (AT5) to the most advanced strategy of attack. The grade shall be selected in accordance with the following definitions.

3.7.2 Unintentional attacks (AT1)

Unintentional attacks (AT1) grade is granted when attackers are considered crew members having unintentionally and accidentally introduced on board a common, not targeted virus or malware.

This grade, when applied, is to be justified.

3.7.3 Bypass attacks (AT2)

Bypass attacks (AT2) grade is granted when attackers are limited to crew members trying to bypass system security without malicious intent (e.g. equipment tuning, tinkers, ethical hackers).

This grade, when applied, is to be justified.

3.7.4 Standard attacks (AT3)

Standard attacks (AT3) grade is applied to prevent from malicious attackers using hacking tools and techniques.

The following are to be considered as malicious attackers: crew members, passengers, on shore operators, former employees, equipment maintenance staff and competitors.

This is the minimum grade, attributable by default, for attackers assessment.

3.7.5 Criminal attacks (AT4)

Criminal attackers (AT4) are considered as willing to invest time and money to gather intelligence about the shipping company, its fleet and the ship. They will probably build a dedicated scenario to penetrate the system in order to install a Advanced Persistent Threat (APT).

Criminal attacks grade is to be assigned:

- when considering the risk of dedicated means used by the attacker
- to prevent the target from scenarios of attacks built by criminal organizations.

3.7.6 Cyberwarfare (AT5)

Cyberwarfare (AT5) grade is assigned when attackers are using governmental attacks.

This grade is to be applied for naval ships.

3.7.7 Adjustments on attackers grade

During the assessment of a system or equipment, the grade of attackers may be decreased or increased depending of the following parameters:

- For well known equipment suppliers on the international maritime market, it is reasonable to think that a criminal organization may target their structure or equipment. In this case, and if the equipment is connected to on shore systems through Internet, the grade is to be 4.
- When an equipment is disconnected, isolated and installed in a room with limited and controlled access, the grade may be 1 or 2.
- For navy ships, grade 5 shall be considered a priority. Any other grade shall be justified.

4 Levels of criticality

4.1 Level of criticality

4.1.1 Objective

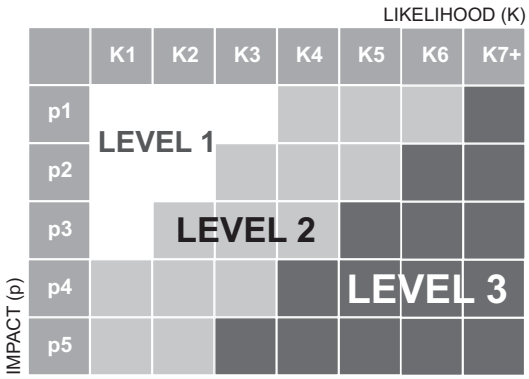
Level contributes to determine rules.

4.1.2 Level of equipment (L)

Level (1, 2 or 3) is the result of the intersection between Impact (P) and Likelihood (K), and is obtained in accordance with Fig 12

- Level 1: Harmless
- Level 2: Significant
- Level 3: Critical.

Figure 12 : Level (of equipment) score table



4.1.3 Deliverable

The Level is to be determined for each equipment in accordance with Likelihood (K) and Impact (P) and summed up in a table (as detailed in Tab 8).

Table 8 : Levels of criticality table

System	Likelihood							Criticality	
Name	Exposure			Human Factor			Likelihood (K=E+H)	Impact (P)	Level (L)
	Complexity (CX)	Connectivity (CY)	Exposure (E)	Attacker (AT)	Users (US)	Human Factor (H)			
Engine Control	CX2	CY2	E2	AT3	US1	H1	K3	P4	Significant Level 2

CHAPTER 2
ADDITIONAL CLASS NOTATION CYBER MANAGED

Section 1 CYBER MANAGED Notation

1 General

1.1 Application

1.1.1 CYBER MANAGED notation

The additional class notation **CYBER MANAGED** is a set of requirements dealing with the following elements:

- Equipment identification: As defined in Ship Rules, NR467, Pt C, Ch 3 Sec 3.
- Equipment Criticality Assessment: Systems criticality is assessed in order to focus the cyber security effort in the right place.
- Cyber Risk Assessment: Cyber security is to be assessed for the ship by taking into account Shipowner risks and constraints.
- Monitoring procedures: Compliance procedures are used to anticipate and detect cyber incident by verifying the integrity of the critical equipment. The principle is to have a picture of standard equipment from its nominal state, or last known as properly configured.
- Maintenance procedures: System nominal configuration addressing cyber risks that are to be mitigated by both updating the systems and preventing unexpected effects during maintenance operations.
- Incident response procedures: In case of system failure, the Shipowner and crew members have to ensure safety and, whenever possible, to restore critical systems to a safe state.
- Cyber Security Policy: A policy (or management plan) is to define cyber security governance and organization for a Shipowner's fleet (roles, responsibilities, rules).

Assignment of the additional class notation **CYBER MANAGED** is subject to compliance with the requirements of this Chapter.

1.1.2 Approval

The additional class notation **CYBER MANAGED** is assigned to a ship in order to reflect the fact that an effective and robust cyber security risk management is constantly implemented on board.

The assignment of the additional class notation implies that the following requirements have been fulfilled:

- equipment are identified, inventoried, categorized in accordance with Ch 1, Sec 2
- criticality, incident impact and cyber attack likelihood of equipment are assessed in accordance with Ch 1, Sec 3
- vital functions, treatment opportunity and risk mitigation are assessed in accordance with Ch 1, Sec 5
- monitoring, maintenance and incident response procedures are delivered in accordance with Ch 1, Sec 6
- Cyber Security Policy (or management plan) is delivered in accordance with Sec 2.

1.1.3 Initial survey

Assignment of the additional class notation **CYBER MANAGED** is subject to an initial survey by the Society as detailed in Ch 6, Sec 1, [1.1.2].

1.1.4 Maintenance of the notation

In compliance with the requirement of NR467, Pt A, Ch 2, Sec 2 and NR467, Pt A, Ch 5, Sec 17, the maintenance of the additional class notation **CYBER MANAGED** is subject to periodical surveys as detailed in Ch 6, Sec 1, [2] to Ch 6, Sec 1, [4], as applicable.

2 Documentation to be submitted

2.1 Methodology

2.1.1 Workflow

The delivery workflow is to follow the here below order:

a) “Basic” Cyber Inventory is to be built by following Ch 1, Sec 2

b) Criticality Assessment is to be built by following Ch 1, Sec 3

c) Cyber Risk Assessment is to be built by following Ch 1, Sec 5

d) Cyber Handbook is to be built by following Ch 1, Sec 6

e) Cyber Security Policy is to be built by following Sec 2.

2.2 Documentation

2.2.1 The documentation listed in Tab 1 is to be submitted for approval.

Table 1 : Documentation to be submitted for the additional class notation CYBER MANAGED

Document	Reference
Cyber Inventory:	
• Basic Inventory	• Ch 1, Sec 2, Tab 1
Criticality Assessment	• Ch 1, Sec 3
Cyber Risk Assessment	• Ch 1, Sec 5
Cyber Handbook:	
• Handbook Scope	• Ch 1, Sec 6, Tab 1 and Ch 1, Sec 6, Tab 2
• Procedures	• Ch 1, Sec 6, Tab 5
Cyber Security Policy:	
• Policies	• Sec 2, Tab 1

Section 2 Cyber Security Policy

1 General

1.1 Introduction

1.1.1 The Cyber Security Policy (CSP) is the main document for cyber security and cyber operation of the ship in operation. This document is under the responsibility of the Shipowner.

It details cyber security management rules and roles.

It is used as a reference for any action on system and equipment by the crew members. In operation, application of the CSP is under the responsibility of the Master.

The cyber security responsible is in charge to check and verify that the CSP is in place and applied by crew members and external partners. This document is to be printed and available on board at any time.

1.2 Goal

1.2.1 The cyber security policy objectives are to:

- support logical cyber security: Obsolete information systems, software or operating systems or antivirus solutions that are not properly updated, lack of networks partitioning are common observations on ships.
- reinforce physical security: Numerous actors get access to the ship during port calls or maintenance periods. Physical access to information systems is usually not controlled. On passenger ships, access to information equipment or network sockets can lead to vulnerabilities.
- consider ship complexity: Each ship is different from another, even in a fleet. Even if cyber rules and procedures are shared, security solutions are to be implemented differently depending on the ship environment, mission and crew.
- understand ship connectivity: Even at sea, ships are not isolated anymore. Remote services (such as cloud data hosting, remote diagnosis, remote maintenance) are now part of the eco-system. This extremely rapid digitalization does rarely come with an adapted Cyber risk management.
- define Shipowner's cyber security vision, and how the requirements of the IMO International Safety Managment Code (ISM Code) (i.e. responsibilities, procedures, training) are implemented in terms of cyber security
- aware crew members: At sea, crew may have the feel isolated, and therefore protected from attacks. Young crew members turn out to be overconfident in their numeric tools and will not monitor them enough to detect cyber incidents. For crews and Shipowners, the increasingly fast digitalization is often considered as a necessary evil. When time is money, trying to measure or even understand cyber risks is obviously not the first priority.

2 Documentation

2.1

2.1.1 Overview

The Cyber Security Policy is to detail the implementation of every topic described in this Section.

In operation, application of the document is under responsibility of the Master.

2.1.2 Documents to be submitted

The Cyber Security Policy (or management plan), as detailed in Tab 1, is to be submitted by the Shipowner to the Society for approval.

As long as all topics (when applicable) described from [3] to [6] are addressed, any Cyber Security Policy (or management plan) template may be used by Shipowners.

Table 1 : Cyber Security Policy document

Topics	Rules
Governance	
Information protection	[3.1]
Documentation maintenance	[3.2]
Roles and responsibilities	[3.3]
Cyber Management	
Monitoring policy	[4.1]
Maintenance policy	[4.2]

Topics	Rules
Incident response policy	[4.3]
Physical security	
Ship security	[5.1]
Removable media	[5.2]
Change management	
Organization	[6.1]
Change request	[6.2]
Change approval	[6.3]
Change validation	[6.4]

3 Governance

3.1 Information protection

3.1.1 Encryption policy

The Cyber Security Policy proposes an encryption policy which defines the scope of encryption (desktop, servers, networks, removable media, communications, on shore systems, email, documents).

Different kind of security levels may be proposed (sensitive, commercial, technical) in minimum respect of [3.1.2].

Algorithms (TLS, AES, DES) and implementation methods (type approved equipment) are defined.

3.1.2 Regulatory requirements

Legal (e.g. GDPR) and regulatory requirements applicable to the ship and regarding cybersecurity, including privacy and civil liberties obligations, are applied and described in the Cyber Security Policy.

3.2 Documentation maintenance

3.2.1 Cyber Inventory

The Cyber Inventory document update policy is to be specified in the Cyber Security Policy.

The policy shall request to update the Cyber Inventory document in the following situations:

- change on the architecture
- modification or deletion of any system or equipment inventoried, as defined in Ch 1, Sec 2, [2.1.2]
- addition of any system or equipment
- physical modification, deletion or relocation of any Level 2 and Level 3 equipment
- modification, deletion or addition of any system or equipment using or involved in ashore connection
- modification, deletion or addition of networks, sub-networks or networks flows.

In case of modification of any Level of Criticality the following are to be updated:

- Design Assessment document
- Cyber Risk Assessment document.

3.2.2 Criticality Assessment

The Criticality Assessment document update policy is to be specified in the Cyber Security Policy.

The policy shall request to update the Criticality Assessment document in the following situations:

- updates of the Cyber Inventory
  - when modifying connectivity, complexity of the system or equipment
  - when adding any system or equipment.
- changes on users accreditation, awareness
- new considerations regarding the attackers levels
- new threats to be taken into account.

3.2.3 Cyber Risk Assessment

The policy shall request to update the Cyber Risk Assessment document in the following situations:

- updates of the Criticality Assessment
  - when introducing new Level 3 equipment
  - when modifying the Level of any equipment.

The Cyber Risk Assessment update procedure is to be submitted in the Cyber Security Policy to constantly reflect the current systems integrated.

3.2.4 Cyber Handbook

The Cyber Handbook document update policy is to be specified in the Cyber Security Policy.

The policy shall request to update the Cyber Handbook document in the following situations:

- updates of the Cyber Risk Assessment
- updates of the Cyber Security Policy.

3.3 Roles and responsibilities

3.3.1 Board level

Board-level involvement is measurable with training and regular information about cyber threats, incidents and level of vulnerability.

Cyber Security Policy identifies elements to be checked at board-level regarding cyber security of the ship (weaknesses, vulnerabilities, security events, mitigation measures, etc.).

The cyber security officer is in charge to deliver elements requested at board-level.

3.3.2 Cyber security responsible

The cyber security responsible role is defined in accordance with Ch 1, Sec 1, [2.2.1].

Cyber security responsible ensures:

- application of Cyber Security Policy
- execution of procedures defined in the Cyber Handbook.

Cyber security responsible delivers logical access, roles and responsibilities in application of the principle of least privilege for both crew members and third parties/external partners.

The principle of least privilege is commonly used in computers to limit users' access to resources that are legitimate for their role. A basic security mechanisms is for example the user management and its relevant access control list.

Cyber Security Policy identifies the crew member in charge of assuming this role.

3.3.3 Cyber security officer

The cyber security officer role is to be defined in accordance with Ch 1, Sec 1, [2.2.1].

Cyber security officer ensures:

- respect of the classification notation rules application
- update of Cyber Risk Assessment document
- update of Cyber Security Policy
- update of Cyber Inventory
- maintenance and security of Cyber Security documentation.

The cyber security officer is in charge of informing board-level regarding cyber events, cyber risks, threats, issues, cyber situation and equipment vulnerabilities.

3.3.4 Third party

Security roles and responsibilities for third parties/external partners are to be detailed in the Cyber Security Policy.

The Shipowner is in charge to inform third parties regarding their responsibilities and cyber security procedures to apply while in factory, locally or remotely, delivering, updating, maintaining, managing, operating or acceding any system or equipment.

Regarding cyber security risk and procedures, the third party is in charge to train technicians involved in maintenance.

The third party is in charge to inform the Shipowner regarding any cyber security issue or any default regarding the Cyber Security Policy.

For Level 2 and Level 3 equipment, a tracking of third parties/external partners' dates of access, roles, nature of operations is to be organized.

3.3.5 Declared crew

For Level 2 and Level 3 equipment, crew members, locally or remotely accessing hardware and software, are to be declared to the cyber security responsible.

3.3.6 Authorized crew

For Level 2 and Level 3 equipment, crew members, locally accessing hardware and software, are to be controlled and authorized by the cyber security responsible.

For Level 2 and Level 3 equipment, crew members, remotely accessing hardware and software, are to be controlled and authorized by the cyber security officer.

The cyber security officer may transfer the control and authorization action to a third-party (e.g. a privileged administrator) in order to manage accounts during ship's operations.

3.3.7 Crew-members

For Level 2 and Level 3 equipment, crew members accessing are to be trained to Cyber Security awareness, risks, administration or operation at sea and on shore.

Cyber Security Policy and Cyber Handbook implementation are part of the training and should be subject of periodic cyber security drills.

For Level 3 equipment, crew members are to be trained before their first access to those systems.

For Level 2 and Level 3 equipment, crew members, locally or remotely accessing hardware and software, should sign an engagement of responsibility.

3.3.8 Privileged users

Any privileged access deliverance is to be made under authority of cyber security officer only.

For Level 2 and Level 3 equipment, privileged users have signed a specific assumption of responsibility.

3.3.9 Remote users

Remote users are users using remote access facilities to access ship's systems and equipment. Comprehensive procedures are to be in place in order to authorize any remote access to the ship.

Procedures include the following topics:

- Authentication mechanisms are implemented for connection: a very robust password policy is to be defined with a regular process for password change.
- Remote service supplier is to deliver logical access, roles and responsibilities in application of the principle of least privilege.
- For performing all maintenance work, remote users are to use an account that is separated from their regular, non-privileged account.
- A technical mechanism is to be installed to ensure recording of connections (success and failure). Logs are to be regularly verified by the Cyber Security Responsible.
- Time out for connection inactivity is to be defined and a procedure explains its management. If the connection to the remote maintenance location is disrupted for some reason, access to the system is to be terminated by an automatic logout function.
- Ashore systems and equipment used by the remote user are declared to the Shipowner. The remote user provides: flow, protocols and a detailed network cartography, matrix and addresses plan.
- Remote users are considered as part of the ship's network.
- When connected to the ship, remote users cannot use computers connected to a second network: computers used for remote connections are dedicated to the ship.
- When connected to the ship through private link, remote users cannot use computers connected to a second network like, in example, public network or internet.
- Remote users delivers their risk analysis and their security policy regarding their own infrastructure.
- Remote users are to be controlled and authorized by the Shipowner.
- Any remote access deliverance is under authority of the Shipowner only.
- Remote users are responsible of the proper application of security procedures in place to protect the ship against any malicious action, malicious content, and malicious code injection coming from their system.
- Remote users are to be trained and are to sign a nominative engagement of responsibility.
- Remote accesses are to be submitted by the Shipowner for a limited amount of months and regularly updated on demand.

3.3.10 Personnel departures

For Level 2 and Level 3 equipment, procedures define how to add, lock, change role, manage level of privileges or remove user's account in case of arrival and departures.

3.3.11 Traceability

Each role, nomination, training session, authorization and engagement is to be logged.

4 Cyber management

4.1 Monitoring policy

4.1.1 Definition

Monitoring is about periodical actions and metrics checking regarding cyber security.

The Cyber Security Policy delivers monitoring policy procedures for the following contents. The objective is to have a periodical way to check:

- compliance of the ship regarding equipment listed in the compliance scope Ch 1, Sec 6, [2.2.1])
- network activity over ship's infrastructure.

The Cyber security officer is in charge of checking security events and look for alerts or suspicious behaviour in systems networks and equipment.

Enforced monitoring procedures apply to Level 3 equipment.

4.1.2 Ship compliance

Ship compliance monitoring is to be done by applying Ch 1, Sec 6, [3.2] procedures issued in the Cyber Handbook.

Periodicity of monitoring is to be defined in the Cyber Security Policy for the following situations:

- before going to sea: to verify proper state of the systems
- after on shore maintenance operations: to check inadvertent/wilful modification of sensitive components or introduction of malicious part of software
- in case of system malfunction: to clear up doubts
- in case of unexpected changes in equipment: to guarantee the compliance of the ship
- in case of suspicious network communication behaviour (e.g. networks lack of speed), the ship and the ground
- in-service: once a week, to log and trace integrity of the systems and equipment.

Compliance monitoring frequency is to be increased for:

- remote access equipment
- Level 3 equipment.

The Compliance monitoring is to be recorded in an accurate, complete, timely and auditable way.

4.1.3 Infrastructure integrity

Compliance of any system used for remote connection to a ship is to be verifiable from the board and from third party authority. This rule applies at any time. Ship's infrastructure events are checked.

Remote Access infrastructures monitoring policy is to be defined based on Cyber Handbook procedures from Ch 1, Sec 6, [3.2.5] application.

4.1.4 Compliance availability

For Level 3 equipment, the Cyber Security Policy is to propose procedures to periodically verify the effective functioning of the compliance monitoring.

Procedures rely on procedures defined in Cyber Handbook from Ch 1, Sec 6, [3.2] application.

4.1.5 Accounts integrity

For Level 3 equipment, the Cyber Security Policy is to propose procedures to periodically test and verify validity of users and roles. Special attention to privileged accounts is to be brought.

The Procedures rely on Cyber Handbook Ch 1, Sec 6, [3.3.6]).

4.2 Maintenance policy

4.2.1 Definition

Maintenance is about everyday operations regarding:

- general security procedures
- updates and patch management
- log and system audits management.

Cyber Security Policy delivers organisation, roles and responsibilities about ship's maintenance.

4.2.2 Equipment protection

The Cyber Security Policy lists equipment requering mandatory maintenance protection. This list can be done by checking equipment procedures issued in the Cyber Handbook from Ch 1, Sec 6, [3.3.3] application.

Organisation, roles and responsibilities are defined to open, apply, verify and close equipment isolation during maintenance operations.

4.2.3 Updates

Cyber Security Policy defines periodicity, organisation, roles and responsibilities for people in charge to update:

- compliance monitoring procedures (Cyber Handbook from Ch 1, Sec 6, [3.2.1])
- compliance baseline (Cyber Handbook from Ch 1, Sec 6, [3.2]).

The Cyber Security Policy also defines roles, tools, procedures and rules for patch management. References are made to Cyber Handbook update procedures for:

- antivirus software, Ch 1, Sec 6, [3.3]
- equipment software maintenance, Ch 1, Sec 6, [3.3]
- remote access equipment, Ch 4, Sec 2, [7.1.2]
- wireless networks, Ch 4, Sec 2, [3.1.1].

4.2.4 Event logging management

The Cyber Security Policy defines roles, tools, procedures and rules for event logging management. The objective is to ensure good functioning of events recording by using Cyber Handbook procedures for:

- remote access equipment, Ch 4, Sec 2, [7.1.3]
- wireless networks, Ch 4, Sec 2, [3.1.1].

4.3 Incident response policy

4.3.1 Definition

Response is about special situations, alerts detection and emergency management.

Cyber Security Policy is to deliver organization, roles and responsibilities about ship's incident response.

Cyber Security responsible is to be trained to implement incident response policy through periodic cyber incident drills.

4.3.2 Non-compliance response

In case of loss of compliance or any other situation as described in the compliance monitoring, the cyber security responsible is to be in charge of:

- implementing non-compliance response procedures defined in Ch 1, Sec 6, [3.4.1]
- adding event description in the compliance registry. Such events are to be completed with details about the past and present situations: context of usage, external events, internal events, actions and involved people
- opening a dedicated timeline of events in the compliance registry
- having a step by step trace of those elements
- starting any relevant action up to emergency procedures
- alerting cyber security officer
- increasing the frequency of full compliance monitoring of the ship
- closing the event as soon as the situation has been explained.

Any detection of unexpected change of compliance of any Level 3 equipment or network security component is to be handled with the highest level of priority and information. Master shall be informed of such event.

Note 1: Non-compliance management procedures are to be submitted in the Cyber Handbook.

4.3.3 Cyber security event detection

Cyber security events may be caused by malicious contents like antivirus alert, malware detection, loss of compliance on security equipment, unauthorized access to equipment.

Discoveries of cyber security events are always to be reported to the cyber security responsible.

Regarding cyber security events detection, the roles and responsibilities are to be established and well-known from crew members.

Cyber security events are to be disclosed to the Master and the cyber security officer as soon as possible.

4.3.4 Post processing monitoring procedures

Monitoring results may point new risks, vulnerabilities or threats. A procedure is to explain how to:

- control shutdown, reset and restart of the affected system
- conduct an action plan with milestones, mitigation measures and responsibilities.
- update Cyber Risk Assessment.

4.3.5 Backup plan

For Level 2 and Level 3 equipment, a backup plan describes periodicity, roles, responsibilities, backup location and procedures.

Backup actions are to be recorded.

Procedures are to rely on Cyber Handbook Ch 1, Sec 6, [3.4.2].

4.3.6 Disaster recovery plan

For Level 2 and Level 3 equipment, a disaster recovery plan is to describe roles, responsibilities and procedures.

The disaster recovery plan is to detail procedures to recover systems during or after an event. Restoration of systems and assets affected by the event is to be explained in a step by step way.

Procedures are to rely on Cyber Handbook Ch 1, Sec 6, [3.4.2].

4.3.7 Crisis management

Crisis Management is to be documented:

- what to do in case of incident
- who to alert
- who is in charge of coordinating situation
- what are the first-aids techniques.

Emergency actions are to be made under authorization and control of cyber security officer or Master.

Legal actions are to be managed by the Shipowner.

For Level 3 systems, disaster recovery plan decision is to be under Master authority.

For Level 3 equipment, emergency procedures are to detail workflow to alert Board-Level.

4.3.8 Incident reporting

Cyber incidents are to be traced with the following information:

- equipment identification
- time of beginning and end of intervention
- people in charge of intervention
- technical and functional scope of the intervention
- action registry with timeline and actors
- description of actions
- visual identification of evidences and backup (for forensic usage) done during intervention
- list of modified, replaced or removed equipment.

5 Physical security

5.1 Vessel

5.1.1 Physical access regulation

The needs of physical access to rooms containing networking infrastructures, remote access equipment, Level 2 or Level 3 equipment are to be defined and justified. The implementation of those physical accesses is to be explained, strictly limited to the needs hereinbefore defined and consistent with the rules implementation of IMO International Ship and Port Facility Security Code (ISPS Code).

Cyber Security Policy refines roles defined in Article [3] to vessel, systems, infrastructures technical rooms and machine rooms physical accesses.

5.1.2 Outgoings

Outgoing management for the ship is to be defined in the Cyber Security Policy. Outgoing crew members shall give back rooms and cabinet keys or badges to the cyber security responsible.

Rooms and cabinets passwords, access codes and alarms systems are to be reset by the cyber security responsible.

5.2 Removable and mobile media

5.2.1 Responsibilities

Any digital asset introduced on board, removable or mobile support, is to be under the responsibility of Master and under control of the cyber security responsible.

Roles defined in Article [3] to removable and mobile digital assets usage are to be defined in the Cyber Security Policy.

5.2.2 Authorization

Use of removable or mobile digital asset is restricted according to the Cyber Security Policy.

All media are to be identified and authorized.

As far as possible, usage of board only, identified and verified removable or mobile digital assets is to be preferred.

Their identification is to be recorded with the following information:

- entering date
- user
- usage (e.g. in operation, one-time maintenance)
- restriction of usage (e.g. areas, roles and users, etc.)
- authorisation of usage (attribution)
- authorized system and/or equipment
- authorized/unauthorized usage on public networks (e.g. internet)
- authorized/unauthorized usage on external computers
- authorized/unauthorized usage outside of the ship
- other specific security rule.

Without specific motivation, Level 2 and Level 3 removable and mobile digital assets are to be:

- confined on board
- never used on computers connected to Internet network
- dedicated to the system and equipment on which removable or mobile operation is needed.

Authorization is to be submitted by the cyber security responsible.

5.2.3 Media scan

A policy about malicious software scanning on removable or mobile digital assets is to be defined in the Cyber Security Policy. The policy is to detail:

- scope of applicability (e.g. USB keys, laptops, etc.)
- context of scanning (e.g. first time onboard, before any type of action, before maintenance, etc.)
- periodicity (e.g. every day, week, month, etc.)
- responsibilities (e.g. under self-engagement, with cyber security responsible authorization, etc.)
- scanning procedure (e.g. dedicated scan station, multiple antivirus, single antivirus, sandbox, etc.)
- scanning tools update context (e.g. last update, 48h old signature database update, etc.)
- scanning certificate issuance (e.g. printed paper, barcode sticker, etc.).

The results of the scanning process are to be recorded with:

- reference of scanned asset
- scan certificate
- scanning date
- antivirus version and date number
- antivirus results and any results of incident
- scan user.

5.2.4 Usage

During maintenance operation, or during any operation out of operational context, accesses to equipment via any external connection are to be systematically recorded.

Usage procedure may include specific regulation (e.g. depot in a locker for unused removable or mobile digital asset, usage of visual colours for authorized media, etc.)

Access procedures to equipment are to be well-known by the crew:

- procedures detailing connection rules
- without authorization or clearance, accesses to external connection of each equipment are notoriously banned.

5.2.5 End of life

Any information support, removable or static support, is erased, deleted or destroyed according to Cyber Security Policy under Master authority.

End of life operations are to be recorded.

6 Change management

6.1 Organization

6.1.1 Definition

The Cyber Security Policy delivers a set of rules regarding management of changes for Level 2 and Level 3 equipment on the ship.

Change management is a formal and internal workflow for driving change of any part of ship using software or computer-based hardware Cat. A, B or C.

Modifications of systems, equipment, infrastructures, physical location, rooms access, cabinets and networks configuration, system or network architecture are inputs of this workflow.

The change management plan, is under responsibility of Shipowner and usually reviewed by an internal board, like IT management.

6.1.2 Traceability

History of requests is to be recorded:

- change request
- change approbation (functional and financial)
- change validation (post-implantation verification).

6.1.3 Everyday changes

Everyday changes are minor changes whom implementation is pre-validated without application of the change management plan.

Those exceptions are to be defined, decided and accepted by the Shipowner. The list of everyday changes is presented in the change management plan.

The application (failure or success) of everyday changes is systematically recorded.

6.1.4 International safety management

The planned maintenance of equipment should be included in the safety management system complying with International Safety Management (ISM) code requirements. Records of maintenance activities should be maintained.

6.2 Change request

6.2.1 Change request

Change of any ship software or hardware is to be requested through an internal (e.g. Change Advisory Board) and documented workflow. Requests scope cover both regular patch management and ship upgrade.

The following considerations are to be included in the change request:

- identification of the need of any changes to operating procedures or documentation
- description of how to avoid security risks including unauthorized access and spread of malware
- identification of the software, CBS, and network to be maintained
- identification of all CBS affected due to their interface connections to other computer system requiring the software maintenance
- identification of individual responsibility for the maintenance and possible supervision of technician from Supplier
- procedures for restoring previous stable software version in case of failure, error or any other issue during the maintenance
- preparation for remote access, when required during the maintenance
- authorization of appropriate crew member to conduct or assist with the maintenance
- authorization of technician from Supplier to conduct the maintenance
- procedures for validating the maintenance after completion
- coordination with the Master for safety of navigation.

6.2.2 Patch management

For Level 2 equipment, patch management and software updates may be considered as everyday changes.

For Level 3 equipment, patch management and software updates are to be considered through the change management plan.

6.2.3 Change differential

Current version number must be recorded.

For Level 3 equipment, history of changes on configuration files or physical switches is to be recorded.

Before any change, in order to keep trace, compliance state is to be backed up by using compliance monitoring procedures defined in Cyber Handbook in Ch 1, Sec 6, [3.2.1].

6.3 Change approval

6.3.1 Change approval

The change management plan defines a decision group and rules of processing. The cyber security officer is part of this decision group.

For pre-integrated Level 3 systems, version upgrades, patch management are to be approved by the supplier.

Residual risks, if any, are presented to the decision group.

When the supplier has determined the need for a critical maintenance and provided the necessary means, this maintenance is to be planned between the supplier and Shipowner as soon as feasible, with a minimized downtime of the equipment.

A status of changes is to be issued by the decision group: accepted or rejected.

The status of changes are to the recorded with the relevant date of decision.

6.3.2 Life-cycle integration

Software updating follows the ship life cycle process with eventual safety testing and procedures.

When impacted, equipment documentation is to be updated.

6.3.3 Connectivity update

For Level 2 and Level 3 equipment, changes of configuration of any network configuration are to be specifically authorized by the Cyber Security Officer.

6.4 Change validation

6.4.1 Scan for malware

Before installation, equipment software files (operating systems as application) are to be inspected by an antivirus mechanism in order to detect malicious parts of software.

A signature ensures the integrity and the authenticity of the update. This signature is to be generated by using, for example, a CRC (Cyclic Redundancy Code) mechanism. A post-update verification is to ensure that the system is performing appropriately.

Digital safety certificate is to be submitted to the cyber security Officer.

6.4.2 Preventive backup

For Level 2 and Level 3 equipment, a backup is to be done before any change, modification, update on any equipment.

For Level 3 equipment, a rollback strategy is to be determined prior to the updating process and previous versions of software are to be stored and available to be installed in emergency situations. The system is to have the ability to revert simply to earlier revisions in the case of corruption.

6.4.3 Onshore testing

For Level 3 equipment updated during remote maintenance operation, changes are to be verified on shore before being introduced on board. Verifications are to be done through copy of systems on shore or virtual machines. A registry of verification results is to be delivered to the Shipowner before application of the up-to-date on board.

6.4.4 Testing

For Level 2 and Level 3 equipment, after software update, a compliance baseline is to be updated by using compliance monitoring procedures defined in Cyber Handbook.

If the supplier has confirmed that new functionalities, changes or improvements have been implemented, the Shipowner is to ensure that crew familiarization with the CBS is carried out.

For Level 3 equipment, after software update, the following tests are to be carried out by the supplier for validation:

- regression tests (regression tests are aimed at verifying that no functionality expected to be still present after the maintenance has been impaired)
- new functionalities and/or improvements tests (testing new functionalities and/or improvements is to verify that the software maintenance has had the intended effect)
- load tests (load tests are aimed to verify the behaviour of the system under a specific expected load, under both normal and peak conditions).

Verifications are to be done by using test procedures related to equipment.

Verification results are to be recorded.

Cyber security officer validation is to be mandatory before using the system in operation.

CHAPTER 3
ADDITIONAL CLASS NOTATION CYBER RESILIENT

Section 1 CYBER RESILIENT Notation

1 General

1.1 Application

1.1.1 CYBER RESILIENT notation

The additional class notation **CYBER RESILIENT** implies the following set of requirements are fulfilled:

- The ship complies with the requirement of Sec 2.
- Systems and equipment under the scope of Sec 2, [3.1] comply with the requirements of Ch 5, Sec 2.

1.1.2 Approval

The additional class notation **CYBER RESILIENT** is assigned to ship in order to reflect that the ship complies with the requirements regarding the following key elements to reinforce ships resilience when dealing with cyber-attacks:

- identify the CBSs on board, their interdependencies and the relevant information flows and the key resources involved in their management, operation and governance, their roles and responsibilities
- protect the CBSs with appropriate safeguards supporting the ability to limit or contain the impact of a potential incident
- detect anomalous activity on CBSs and networks onboard and identify cyber incidents
- respond to attack with means supporting the ability to minimize the impact of cyber incidents, containing the extension of possible impairment of CBSs and networks onboard
- recover the systems and restore CBSs and networks onboard affected by cyber incidents.

1.1.3 Initial survey

Assignment of the additional class notation **CYBER RESILIENT** may be subject to an initial survey by the Society as detailed in Ch 6, Sec 1, [1.1.2].

1.1.4 Maintenance of the notation

Maintenance of the additional class notation **CYBER RESILIENT** is subject to compliance with the applicable requirements of Sec 2, [10] and Chapter 6.

2 Documents to be submitted

2.1 Methodology

2.1.1 Workflow

The documentation workflow is to follow the applicable requirements of Ch 1, Sec 2.

2.2 Documentation

2.2.1 With reference to Sec 2, [10] and Ch 5, Sec 1, [3], the following documentation is to be submitted for approval:

- Inventory of hardware and software of the computer-based systems (CBS)
- Documentation of the product, equipment or component supplied to construct network segregation, including a diagram of zones and conduits and the configuration of traffic filtering / shaping rules
- Documentation on network protection measures including a test plan to verify the implemented control Antivirus, antimalware and antispam software installed or other security measures applied
- Installation locations, physical access restrictions, credential management policy, removable media access points
- Wireless networks diagrams, security capabilities, connection with other networks
- Policies and procedures on use of mobile and portable devices, roles and responsibilities
- Description on how to monitor networks, test plan; plans for training and drills
- Alarms and other means used to signal cyber incidents and procedures to respond to such incidents; plans for training and drills
- Incidence response plan
- Minimal risk conditions to be reached in case of unexpected or unmanageable failures or cyber events
- Instructions and procedures for the recovery of a failed system
- Documentation on how to execute controlled shutdown, reset to an initial state, roll-back to a safe state and restart from scratch to allow fast and safe recovery
- Test plans
- if applicable: Risk assessment for supplied products, equipment or components aimed at identification of cyber risks and relevant mitigation measures, including a concise list of excluded applications of relevant requirements.

In addition, the following documentation if to be submitted for information:

- Remote connection policies and procedures, roles and responsibilities
- Monitoring, alarm and diagnostic functions of CBS and network devices
- Procedures and operations for backup and restoration of data and software; plans for training and drills.

Section 2 Cyber Resilience of Ships

1 General

1.1 Introduction

1.1.1 When it comes to cybersecurity, attackers may target any combination of people and technology to achieve their aim, wherever there is a network connection or any other interface between onboard systems and the external world. Safeguarding ships, and shipping in general, from current and emerging threats involves a range of measures that are continually evolving.

It is then necessary to establish a common set of minimum functional and performance criteria to deliver a ship that can indeed be described as cyber resilient.

It is considered that minimum requirements applied consistently to the full threat surface using a goal-based approach is necessary to make cyber resilient ships.

1.2 Purpose

1.2.1 This Section gives requirements for cyber resilience of ships, with the purpose of providing technical means to stakeholders which would lead to cyber resilient ships.

This Section targets the ship as a collective entity for cyber resilience and is intended as a base for the complementary application of other documents and industry standards addressing cyber resilience of onboard systems, equipment and components.

Minimum requirements for cyber resilience of on-board systems and equipment are given in Ch 5, Sec 2.

1.3 Scope of applicability

1.3.1 Systems in scope

This Section applies to:

a) Operational Technology (OT) systems onboard ships, i.e. those computer-based systems (CBS) using data 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.

In particular, the CBSs used for the operation of the following ship functions and systems, if present onboard, are to be considered:

- Propulsion
- Steering
- Anchoring and mooring
- Electrical power generation and distribution
- Fire detection and extinguishing systems
- Bilge and ballast systems, loading computer
- Watertight integrity and flooding detection
- Lighting (e.g. emergency lighting, low locations, navigation lights, etc.)
- Any required safety system whose disruption or functional impairing may pose risks to ship operations (e.g. emergency shutdown system, cargo safety system, pressure vessel safety system, gas detection system, etc.)).

In addition, the following systems is to be included in the scope of applicability of this Section:

- Navigational systems required by statutory regulations
- Internal and external communication systems required by the Society and statutory regulations

For navigation and radiocommunication systems, standard such as IEC 61162-460 or IEC 63154 can be used as alternatives to this Section, as long as the application of such standards provides equivalent or greater cyber resilience as obtained from the application of the requirements contained in this Section. In any case, requirements under Articles [4] to [9] are to be complied with.

For navigation and radiocommunication systems, the application of IEC 61162-460 or other equivalent standards in lieu of the required security capabilities in Ch 5, Sec 2, [4] may be accepted by the Society, on the condition that requirements in this Section are complied with.

b) Any Internet Protocol (IP)-based communication interface from CBSs in scope of this Section to other systems. Examples of such systems are, but not limited to, the following:

- passenger or visitor servicing and management systems
- passenger-facing networks
- administrative networks
- crew welfare systems
- any other systems connected to OT systems, either permanently or temporarily (e.g. during maintenance).

The cyber incidents considered in this Section are events resulting from any offensive manoeuvre that targets OT systems onboard ships as defined in Article [2].

1.3.2 System Category

System categories are defined in Ship Rules, Pt C, Ch 3, Sec 3 on the basis of the consequences of a system failure to human safety, safety of the vessel and/or threat to the environment.

1.3.3 Additional documents on CBSs and cyber resilience

Attention is made to additional documents on CBSs and Cyber Resilience as follows:

- NR467 Rules for the Classification of Steel Ships, Pt C, Ch 3, Sec 3
- Requirements given in Ch 5, Sec 2.
- IACS Recommendation 166 - Recommendation on Cyber Resilience.

Note 1: non-mandatory recommended technical requirements that stakeholders may reference and apply to assist with the delivery of cyber resilient ships, whose resilience can be maintained throughout their service life. IACS Recommendation 166 on Cyber Resilience is intended for ships contracted for construction after its publication and may be used as a reference for ships already in service prior to its publication. For ships to which the requirements of this Section applies as mandatory instrument, when both this Section and Recommendation 166 are used, should any difference in requirements addressing the same topic be found between the two instruments, the requirements in this Section shall prevail.

2 Definitions

2.1

2.1.1 Attack Surface

The set of all possible points where an unauthorized user can access a system, cause an effect on or extract data from. The attack surface comprises two categories: digital and physical. The digital attack surface encompasses all the hardware and software that connect to an organization's network. These include applications, code, ports, servers and websites. The physical attack surface comprises all endpoint devices that an attacker can gain physical access to, such as desktop computers, hard drives, laptops, mobile phones, removable drives and carelessly discarded hardware.

2.1.2 Authentication

Provision of assurance that a claimed characteristic of an entity is correct.

2.1.3 Compensating countermeasure

An alternate solution to a countermeasure employed in lieu of or in addition to inherent security capabilities to satisfy one or more security requirements.

2.1.4 Computer Based System (CBS)

A programmable electronic device, or interoperable set of programmable electronic devices, organized to achieve one or more specified purposes such as collection, processing, maintenance, use, sharing, dissemination, or disposition of information. CBSs onboard include IT and OT systems. A CBS may be a combination of subsystems connected via network. Onboard CBSs may be connected directly or via public means of communications (e.g. Internet) to ashore CBSs, other vessels' CBSs and/or other facilities.

2.1.5 Cyber incident

An event resulting from any offensive manoeuvre, either intentional or unintentional, that targets or affects one or more CBS onboard, which actually or potentially results in adverse consequences to an onboard system, network and computer or the information that they process, store or transmit, and which may require a response action to mitigate the consequences. Cyber incidents include unauthorized access, misuse, modification, destruction or improper disclosure of the information generated, archived or used in onboard CBS or transported in the networks connecting such systems. Cyber incidents do not include system failures.

2.1.6 Cyber resilience

The capability to reduce the occurrence and mitigating the effects of cyber incidents arising from the disruption or impairment of operational technology (OT) used for the safe operation of a ship, which potentially lead to dangerous situations for human safety, safety of the vessel and/or threat to the environment.

2.1.7 Essential System

Services for essential for propulsion and steering, and safety of the ship. Essential services comprise “Primary Essential Services” and “Secondary Essential Services”.

2.1.8 “Primary Essential Services” and “Secondary Essential Services”

Primary Essential Services are those services which need to be in continuous operation to maintain propulsion and steering.

Secondary Essential Services are those services which need not necessarily be in continuous operation to maintain propulsion and steering but which are necessary for maintaining the vessel's safety.

2.1.9 Information Technology (IT)

Devices, software and associated networking focusing on the use of data as information, as opposed to Operational Technology (OT).

2.1.10 Integrated system

A system combining a number of interacting sub-systems and/or equipment organized to achieve one or more specified purposes.

2.1.11 Logical network segment

The same as “Network segment”, but two or more logical network segments share the same physical components.

2.1.12 Network

A connection between two or more computers for the purpose of communicating data electronically by means of agreed communication protocols.

2.1.13 Network segment

In the context of this Section, a network segment is an OSI layer-2 Ethernet segment (a broadcast domain).

Note 1: Note on TCP/IP: Network address plan is prefixed by their IP addresses and the network mask. Communication between network segments is only possible by the use of routing service at network layer (OSI Layer 3).

2.1.14 Operational Technology (OT)

Devices, sensors, software and associated networking that monitor and control onboard systems. Operational technology systems may be thought of as focusing on the use of data to control or monitor physical processes.

2.1.15 Physical network segment

The same as “Network segment” but where physical components are not shared by other network segments.

2.1.16 Protocol

A common set of rules and signals that computers on the network use to communicate. Protocols allow to perform data communication, network management and security. Onboard networks usually implement protocols based on TCP/IP stacks or various fieldbuses.

2.1.17 Security zone

A collection of CBSs in the scope of applicability of this Section that meet the same security requirements. Each zone consists of a single interface or a group of interfaces, to which an access control policy is applied.

2.1.18 Shipowner / Company

The owner of the ship or any other organization or person, such as the manager, agent or bareboat charterer, who has assumed the responsibility for operation of the ship from the Shipowner and who on assuming such responsibilities has agreed to take over all the attendant duties and responsibilities. The Shipowner could be the Shipyard or system integrator during initial construction. After vessel delivery, the Shipowner may delegate some responsibilities to the vessel management company.

2.1.19 Supplier

A manufacturer or provider of hardware and/or software products, system components or equipment (hardware or software) comprising of the application, embedded devices, network devices, host devices etc. working together as system or a subsystem. The Supplier is responsible for providing programmable devices, sub-systems or systems to the System Integrator.

2.1.20 Systems Integrator

The specific person or organization responsible for the integration of systems and products provided by suppliers into the system invoked by the requirements in the ship specifications and for providing the integrated system. The systems integrator may also be responsible for integration of systems in the ship. Until vessel delivery, this role is to be taken by the Shipyard unless an alternative organization is specifically contracted/assigned this responsibility.

2.1.21 Untrusted network

Any network outside the scope of applicability of this Section.

3 Goals and organization of requirements

3.1 Primary goal

3.1.1 The primary goal is to support safe and secure shipping, which is operationally resilient to cyber risks.

Safe and secure shipping can be achieved through effective cyber risk management system. To support safe and secure shipping resilient to cyber risk, the following sub-goals for the management of cyber risk are defined in the five functional elements listed in [3.2].

3.2 Sub-goals per functional element

3.2.1

a) Identify:

Develop an organizational understanding to manage cybersecurity risk to onboard systems, people, assets, data, and capabilities.

b) Protect:

Develop and implement appropriate safeguards to protect the ship against cyber incidents and maximize continuity of shipping operations.

c) Detect:

Develop and implement appropriate measures to detect and identify the occurrence of a cyber incident onboard.

d) Respond:

Develop and implement appropriate measures and activities to take action regarding a detected cyber incident onboard.

e) Recover:

Develop and implement appropriate measures and activities to restore any capabilities or services necessary for shipping operations that were impaired due to a cyber incident.

These sub-goals and relevant functional elements should be concurrent and considered as parts of a single comprehensive risk management framework.

3.3 Organization of requirements

3.3.1 The requirements are organized according to a goal-based approach. Functional/technical requirements are given for the achievement of specific sub-goals of each functional element. The requirements are intended to allow a uniform implementation by stakeholders and to make them applicable to all types of vessels, in such a way as to enable an acceptable level of resilience and apply to all classed vessels/units regardless of operational risks and complexity of OT systems.

- For each requirement, a rationale is given.
- A summary of actions to be carried out and documentation to be made available is also given for each phase of the ship's life and relevant stakeholders participating to such phase.

4 Requirements

4.1 General

4.1.1 Articles [5] to [9] contain the requirements to be satisfied in order to achieve the primary goal defined in [3.1], organized according to the five functional elements identified in [3.2].

The requirements are to be fulfilled by the stakeholders involved in the design, building and operation of the ship. Among them, the following stakeholders can be identified (see also Article [2] for definitions):

- Shipowner / Company
- System Integrator
- Supplier
- The Society.

Whilst the above requirements may be fulfilled by these stakeholders, for the purposes of this Section, responsibility to fulfil them will lie with the stakeholder who has contracted with the Society.

5 Identify

5.1 General

5.1.1 The requirements for the ”Identify” functional element are aimed at identifying: on one side, the CBSs onboard, their interdependencies and the relevant information flows; on the other side, the key resources involved in their management, operation and governance, their roles and responsibilities.

5.2 Vessel asset inventory

5.2.1 Requirements

An inventory of hardware and software (including application programs, operating systems, if any, firmware and other software components) of the CBSs in the scope of applicability of this Section and of the networks connecting such systems to each other and to other CBSs onboard or ashore are to be provided and kept up to date during the entire life of the ship.

5.2.2 Rationale

The inventory of CBSs onboard and relevant software used in OT systems, is essential for an effective management of cyber resilience of the ship, the main reason being that every CBS becomes a potential point of vulnerability. Cybercriminals can

exploit unaccounted and out-of- date hardware and software to hack systems. Moreover, managing CBS assets enables Companies understand the criticality of each system to ship safety objectives.

5.2.3 Requirement details

The vessel asset inventory is to include at least the CBSs indicated in [1.3.1] if present onboard.

The inventory is to be kept updated during the entire life of the ship. Software and hardware modifications potentially introducing new vulnerabilities or modifying functional dependencies or connections among systems are to be recorded in the inventory.

If confidential information is included in the inventory (e.g. IP addresses, protocols, port numbers), special measures are to be adopted to limit the access to such information only to authorized people.

5.2.4 Hardware

For all hardware devices in the scope of applicability of this Section, the vessel asset inventory is to include at least the information in Ch 5, Sec 2, [3.1.2].

In addition, the vessel asset inventory may specify system category and security zone associated with the CBS.

5.2.5 Software

For all software in the scope of applicability of this Section (e.g., application program, operating system, firmware), the vessel asset inventory is to include at least the information in Ch 5, Sec 2, [3.1.2].

The software of the CBSs in the scope of applicability of this Section is to be maintained and updated in accordance with the Shipowner's process for management of software maintenance and update policy in the Ship cyber security and resilience program, see [10.4].

5.2.6 Demonstration of compliance

a) Design phase:

The systems integrator is to submit the vessel asset inventory to the Society (see [10.2.4]).

The vessel asset inventory is to incorporate the asset inventories of all individual CBSs falling under the scope of this Section. Any equipment in the scope of this Section delivered by the systems integrator are also to be included in the vessel asset inventory.

b) Construction phase:

The systems integrator is to keep the vessel asset inventory updated.

c) Commissioning phase:

- The systems integrator is to submit Ship cyber resilience test procedure (see [10.3.2]) and demonstrate to the Society that:
  - Vessel asset inventory is updated and completed at delivery
- CBSs in the scope of applicability of this Section are correctly represented by the vessel asset inventory
- Software of the CBSs in the scope of applicability of this Section has been kept updated, e.g. by vulnerability scanning or by checking the software versions of CBSs while switched on.

d) Operation phase

- For general requirements to surveys in the operation phase, see [10.4].
- The Shipowner is in the Ship cyber security and resilience program to describe the process of management of change (MoC) for the CBSs in the scope of applicability of this Section, addressing at least the following requirements in this Section:
  - Management of change (see [10.4])
  - Hardware and software modifications (see [5.2.3])
- The Shipowner is in the Ship cyber security and resilience program also to describe the management of software updates, addressing at least the following requirements in this Section:
  - Vulnerabilities and cyber risks (see [5.2.2] and [5.2.3])
  - Security patching (see [6.7.3], item b))
- Surveys
  - First annual survey:

    The Shipowner is to present to the Society records or other documented evidence demonstrating implementation of the Ship cyber security and resilience program, i.e., that:
    - The approved management of change process has been adhered to.
    - Known vulnerabilities and functional dependencies have been considered for the software in the CBSs.
    - The Vessel asset inventory has been kept updated.
  - Subsequent annual surveys:

    The Shipowner is upon request by the Society to demonstrate implementation of the Ship cyber security and resilience program by presenting records or other documented evidence as specified for the first annual survey.
  - Special Survey:

    The Shipowner is to demonstrate to the Society the activities in [5.2.6], item c) as per the Ship cyber resilience test procedure.

6 Protect

6.1 General

6.1.1 The requirements for the "Protect" functional element are aimed at the development and implementation of appropriate safeguards supporting the ability to limit or contain the impact of a potential incident.

6.2 Security zones and network segmentation

6.2.1 Requirement

All CBSs in the scope of applicability of this Section are to be grouped into security zones with well-defined security policy and security capabilities. Security zones are either to be isolated (i.e. air gapped) or connected to other security zones or networks by means providing control of data communicated between the zones (e.g. firewalls/routers, simplex serial links, TCP/IP diodes, dry contacts, etc.)

Only explicitly allowed traffic is to traverse a security zone boundary.

6.2.2 Rationale

While networks may be protected by firewall perimeter and include Intrusion Detection Systems (IDS) or Intrusion Prevention Systems (IPS) to monitor traffic coming in, breaching that perimeter is always possible. Network segmentation makes it more difficult for an attacker to perpetrate an attack throughout the entire network.

The main benefits of security zones and network segmentation are to reduce the extent of the attack surface, prevent attackers from achieving lateral movement through systems, and improve network performance. The concept of allocating the CBSs into security zones allows grouping the CBSs in accordance with their risk profile.

6.2.3 Requirements details

A security zone may contain multiple CBSs and networks, all of which are to comply with applicable security requirements given in this Section and Ch 5, Sec 2.

The network(s) of a security zone is to be logically or physically segmented from other zones or networks. See also [6.7.3]

CBSs providing required safety functions are to be grouped into separate security zones and are to be physically segmented from other security zones.

Navigational and communication systems are not to be in same security zone as machinery or cargo systems. If navigation and/or radiocommunication systems are approved in accordance with other equivalent standard(s) (see [1.3.1]), these systems should be in a dedicated security zone.

Wireless devices are to be in dedicated security zones. See also [6.6].

Systems, networks or CBSs outside the scope of applicability of this Section are considered untrusted network and are to be physically segmented from security zones required by this Section. Alternatively, it is accepted that such systems are part of a security zone if these OT-systems meet the same requirements as demanded by the zone.

It is to be possible to isolate a security zone without affecting the primary functionality of the CBSs in the zone, see also [8.4].

6.2.4 Demonstration of compliance

a) Design phase:

- The systems integrator is to submit Zones and conduit diagram and the Cyber security design description (see [10.2.2] and [10.2.3]).
- The Zones and conduit diagram is to illustrate the CBSs in the scope of applicability of this Section, how they are grouped into security zones, and include the following information:
  - Clear indication of the security zones
  - Simplified illustration of each CBS in scope of applicability of this Section, and indication of the security zone in which the CBS is allocated, and indication of physical location of the CBS/equipment.
  - Reference to the approved version of the CBS system topology diagrams provided by the suppliers (see Ch 5, Sec 2, [3.1.3])
  - Illustration of network communication between systems in a security zone
  - Illustration of any network communication between systems in different security zones (conduits).
  - Illustration of any communication between systems in a security zone and untrusted networks (conduits).

- The systems integrator is to include the following information in the Cyber security design description:
  - A short description of the CBSs allocated to the security zone. It is to be possible to identify each CBS in the Zones and conduit diagram.
  - Network communication between CBSs in the same security zone. The description is to include purpose and characteristics (i.e. protocols and data flows) of the communication.
  - Network communication between CBSs in different security zones. The description is to include purpose and characteristics (i.e. protocols and data flows) of the communication. The description is also to include zone boundary devices and specify the traffic that is permitted to traverse the zone boundary (e.g. firewall rules).
  - Any communication between CBSs in security zones and untrusted networks. The description is to include discrete signals, serial communication, and the purpose and characteristics (i.e. protocols and data flows) of IP-based network communication. The description is also to include zone boundary devices and specify the traffic that is permitted to traverse the zone boundary (e.g. firewall rules).

b) Construction phase

The systems integrator is to keep the Zones and conduit diagram updated.

c) Commissioning phase

The systems integrator is to submit Ship cyber resilience test procedure (see [10.3.2]) and demonstrate to the Society that:

- the security zones on board are implemented in accordance with the approved documents (i.e. zones and conduit diagram, cyber security design description, asset inventory, and relevant documents provided by the supplier). This may be done by e.g., inspection of the physical installation, network scanning and/or other methods providing the Surveyor assurance that the installed equipment is grouped in security zones according to the approved design.
- security zone boundaries allow only the traffic that has been documented in the approved Cyber security description. This may be done by e.g., evaluation of firewall rules or port scanning.

d) Operation phase

- For general requirements to surveys in the operation phase, see [10.4].
- The Shipowner is in the Ship cyber security and resilience program to describe the management of security zone boundary devices (e.g., firewalls), addressing at least the following requirements in this Section:
  - Principle of Least Functionality (see [6.3.1])
  - Explicitly allowed traffic (see [6.2.1])
  - Protection against denial of service (DoS) events (see [6.3.1])
  - Inspection of security audit records (see [7.2.1]).
- Surveys:
  - First annual survey

    The Shipowner is to demonstrate to the Society that the Zones and conduit diagram has been kept updated and present records or other documented evidence demonstrating implementation of the Ship cyber security and resilience program, i.e., that security zone boundaries are managed in accordance with the above requirements.
  - Subsequent annual surveys

    The Shipowner is upon request by the Society to demonstrate implementation of the Ship cyber security and resilience program by presenting records or other documented evidence as specified for the first annual survey.
  - Special survey

    The Shipowner is to demonstrate to the Society the activities in [6.2.4], item c) as per the Ship cyber resilience test procedure.

6.3 Network protection safeguards

6.3.1 Requirements

Security zones are to be protected by firewalls or equivalent means as specified in [6.2]. The networks are also to be protected against the occurrence of excessive data flow rate and other events which could impair the quality of service of network resources.

The CBSs in scope of this Section are to be implemented in accordance with the principle of Least Functionality, i.e. configured to provide only essential capabilities and to prohibit or restrict the use of non-essential functions, where unnecessary functions, ports, protocols and services are disabled or otherwise prohibited.

6.3.2 Rationale

Network protection covers a multitude of technologies, rules and configurations designed to protect the integrity, confidentiality and availability of networks. The threat environment is always changing, and attackers are always trying to find and exploit vulnerabilities.

There are many layers to consider when addressing network protection. Attacks can happen at any layer in the network layers model, so network hardware, software and policies must be designed to address each area.

While physical and technical security controls are designed to prevent unauthorized personnel from gaining physical access to network components and protect data stored on or in transit across the network, procedural security controls consist of security policies and processes that control user behaviour.

6.3.3 Requirement details

The design of network is to include means to meet the intended data flow through the network and minimize the risk of denial of service (DoS) and network storm/high rate of traffic. Estimation of data flow rate is at least to be consider the capacity of network, data speed requirement for intended application and data format.

6.3.4 Demonstration of compliance

a) Design phase:

No requirements.

b) Construction phase:

No requirements.

c) Commissioning phase:

The systems integrator is to submit Ship cyber resilience test procedure (see [10.3.2]) and demonstrate the following to the Society:

- Test denial of service (DoS) attacks targeting zone boundary protection devices, as applicable.
- Test denial of service (DoS) to ensure protection against excessive data flow rate, originating from inside each network segment. Such denial of service (DoS) tests are to cover flooding of network (i.e., attempt to consume the available capacity on the network segment), and application layer attack (i.e., attempt to consume the processing capacity of selected endpoints in the network)
- Test e.g. by analytic evaluation and port scanning that unnecessary functions, ports, protocols and services in the CBSs have been removed or prohibited in accordance with hardening guidelines provided by the suppliers. See Ch 5, Sec 2, [5.1.8] and Ch 5, Sec 2, [6.3.5], item g).

The second and third tests may be omitted if performed during the certification of CBSs as per [10.3.2].

d) Operation phase

- For general requirements to surveys in the operation phase, see [10.4].
- Special survey:

  Subject to modifications of the CBSs, the Shipowner is to demonstrate to the Society the activities in [6.3.4], item c) as per the Ship cyber resilience test procedure.

6.4 Antivirus, antimalware, antispam and other protections from malicious code

6.4.1 Requirement

CBSs in the scope of applicability of this Section are to be protected against malicious code such as viruses, worms, trojan horses, spyware, etc.

6.4.2 Rationale

A virus or any unwanted program that enters a user's system without his/her knowledge can self-replicate and spread, perform unwanted and malicious actions that end up affecting the system's performance, user's data/files, and/or circumvent data security measures.

Antivirus, antimalware, antispam software will act as a closed door with a security guard fending off the malicious intruding viruses performing a prophylactic function. It detects potential virus and then works to remove it, mostly before the virus gets to harm the system.

Common means for malicious code to enter CBSs are electronic mail, electronic mail attachments, websites, removable media (for example, universal serial bus (USB) devices, diskettes or compact disks), PDF documents, web services, network connections and infected laptops.

6.4.3 Requirement details

Malware protection is to be implemented on CBSs in the scope of applicability of this Section. On CBSs having an operating system for which industrial-standard anti-virus and/or anti-malware software is available and maintained up-to-date, anti-virus and anti-malware software are to be installed, maintained and regularly updated, unless the installation of such software impairs the ability of CBS to provide the functionality and level of service required (e.g. for Cat.II and Cat.III CBSs performing real-time tasks).

On CBSs where anti-virus and anti-malware software cannot be installed, malware protection is to be implemented in the form of operational procedures, physical safeguards, or according to manufacturer's recommendations.

6.4.4 Demonstration of compliance

a) Design phase:

The systems integrator is to include the following information in the Cyber security design description:

- For each CBS, summary of the approved mechanisms provided by the supplier for protection against malicious code or unauthorized software.
- For CBSs with anti-malware software, information about how to keep the software updated.
- Any operational conditions or necessary physical safeguards to be implemented in the Shipowner's management system.

b) Construction phase:

The systems integrator is to ensure that malware protection is kept updated during the construction phase.

c) Commissioning phase:

The systems integrator is to submit Ship cyber resilience test procedure (see [10.3.2]) and demonstrate the following to the Society:

- Approved anti-malware software or other compensating countermeasures is effective (test e.g., with a trustworthy anti-malware test file).

The above tests may be omitted if performed during the certification of CBSs as per [10.3.2].

d) Operation phase:

- For general requirements to surveys in the operation phase, see [10.4]
- The Shipowner is in the Ship cyber security and resilience program to describe the management of malware protection, addressing at least the following requirements in this Section:
  - Maintenance/update (see [6.4.3])
  - Operational procedures, physical safeguards (see [6.4.3])
  - Use of mobile, portable, removable media (see [6.5.2] item d) and [6.8.3]
  - Access control (see [6.5])
- Surveys:
  - First annual survey:

    The Shipowner is to present to the Society records or other documented evidence demonstrating implementation of the Ship cyber security and resilience program, i.e., that:
    - Any anti-malware software has been maintained and updated.
    - Procedures for use of portable, mobile or removable devices have been followed.
    - Policies and procedures for access control have been followed.
    - Physical safeguards are maintained.
  - Subsequent annual surveys:

    The Shipowner is upon request by the Society to demonstrate implementation of the Ship cyber security and resilience program by presenting records or other documented evidence as specified for the first annual survey.
  - Special survey:

    The Shipowner is to demonstrate to the Society the activities in [6.4.4], item c) as per the Ship cyber resilience test procedure.

6.5 Access control

6.5.1 Requirement

CBSs and networks in the scope of applicability of this Section are to provide physical and/or logical/digital measures to selectively limit the ability and means to communicate with or otherwise interact with the system itself, to use system resources to handle information, to gain knowledge of the information the system contains or to control system components and functions. Such measures are to be such as not to hamper the ability of authorized personnel to access CBS for their level of access according to the least privilege principle.

6.5.2 Rationale

Attackers may attempt to access the ship's systems and data from either onboard the ship, within the company, or remotely through connectivity with the internet. Physical and logical access controls to cyber assets, networks etc. should then be implemented to ensure safety of the ship and its cargo.

Physical threats and relevant countermeasures are also considered in the ISPS Code. Similarly, the ISM Code contains guidelines to ensure safe operation of ships and protection of the environment. Implementation of ISPS and ISM Codes may imply inclusion in the Ship Security Plan (SSP) and Safety Management System (SMS) of instructions and procedures for access control to safety critical assets.

6.5.3 Requirement details

Access to CBSs and networks in the scope of applicability of this Section and all information stored on such systems are only to be allowed to authorized personnel, based on their need to access the information as a part of their responsibilities or their intended functionality.

a) Physical access control

CBSs of Cat.II and Cat.III are generally to be located in rooms that can normally be locked or in controlled space to prevent unauthorized access, or are to be installed in lockable cabinets or consoles. Such locations or lockable cabinets/consoles are to be however easy to access to the crew and various stakeholders who need to access to CBSs for installation, integration, operation, maintenance, repair, replacement, disposal etc. so as not to hamper effective and efficient operation of the ship.

b) Physical access control for visitors

Visitors such as authorities, technicians, agents, port and terminal officials, and Shipowner representatives are to be restricted regarding access to CBSs onboard whilst on board, e.g. by allowing access under supervision.

c) Physical access control of network access points

Access points to onboard networks connecting Cat.II and/or Cat.III CBSs are to be physically and/or logically blocked except when connection occurs under supervision or according to documented procedures, e.g. for maintenance.

Independent computers isolated from all onboard networks, or other networks, such as dedicated guest access networks, or networks dedicated to passenger recreational activities, are to be used in case of occasional connection requested by a visitor (e.g. for printing documents).

d) Removable media controls

A policy for the use of removable media devices is to be established, with procedures to check removable media for malware and/or validate legitimate software by digital signatures and watermarks and scan prior to permitting the uploading of files onto a ship's system or downloading data from the ship's system. See also [6.8].

e) Management of credentials

CBSs and relevant information are to be protected with file system, network, application, or database specific Access Control Lists (ACL). Accounts for onboard and onshore personnel are to be left active only for a limited period according to the role and responsibility of the account holder and is to be be removed when no longer needed.

Note 1: CBSs are to identify and authenticate human users as per item No.1 in Ch 5, Sec 2, Tab 1. In other words, it is not necessary to “uniquely” identify and authenticate all human users

Onboard CBSs are to be provided with appropriate access control that fits to the policy of their Security Zone but does not adversely affect their primary purpose. CBSs which require strong access control must need to be secured using a strong encryption key or multi-factor authentication.

Administrator privileges are to be managed in accordance with the policy for access control, allowing only authorized and appropriately trained personnel full access to the CBS, who as part of their role in the company or onboard need to log on to systems using these privileges.

f) Least privilege principle

Any human user allowed to access CBS and networks in the scope of applicability of this Section are to have only the bare minimum privileges necessary to perform its function.

The default configuration for all new account privileges is to be set as low as possible. Wherever possible, raised privileges are to be restricted only to moments when they are needed, e.g. using only expiring privileges and one-time-use credentials. Accumulation of privileges over time is to be avoided, e.g. by regular auditing of user accounts.

6.5.4 Demonstration of compliance

a) Design phase:

The systems integrator is to include the following information in the Cyber security design description:

- Location and physical access controls for the CBSs. Devices providing Human Machine Interface (HMI) for operators needing immediate access need not enforce user identification and authentication provided they are located in an area with physical access control. Such devices is to be specified.

b) Construction phase:

The systems integrator is to prevent unauthorised access to the CBSs during the construction phase.

c) Commissioning phase

The systems integrator is to submit Ship cyber resilience test procedure (see [10.3.2]) and demonstrate the following to the Society:

- Components of the CBSs are located in areas or enclosures where physical access can be controlled to authorised personnel.
- User accounts are configured according to the principles of segregation of duties and least privilege and that temporary accounts have been removed (may be omitted based on certification of CBSs as per [10.3.2])

d) Operation phase

- For general requirements to surveys in the operation phase, see [10.4].

- The Shipowner is in the Ship cyber security and resilience program to describe the management of logical and physical access, addressing at least the following requirements in this Section:
  - Physical access control (see [6.5.3], item a))
  - Physical access control for visitors (see [6.5.3], item b))
  - Physical access control of network access points (see [6.5.3], item c))
  - Management of credentials (see [6.5.3], item d))
  - Least privilege policy (see [6.5.3], item e))
- The Shipowner is in the Ship cyber security and resilience program to describe the management of confidential information, addressing at least the following requirements in this Section:
  - Confidential information (see [5.2.3])
  - Information allowed to authorized personnel (see [6.5.3]
- Surveys:
  - First annual survey:

    The Shipowner is to present to the Society records or other documented evidence demonstrating implementation of the Ship cyber security and resilience program, i.e., that:
    - Personnel are authorized to access the CBSs in accordance with their responsibilities.
    - Only authorised devices are connected to the CBSs.
    - Visitors are given access to the CBSs according to relevant policies and procedures.
    - Physical access controls are maintained and applied.
    - Credentials, keys, secrets, certificates, relevant CBS documentation, and other sensitive information is managed and kept confidential according to relevant policies and procedures.
    - Information transmitted on the wireless network (see [6.6.3])
  - Subsequent annual surveys:

    The Shipowner is upon request by the Society to demonstrate implementation of the Ship cyber security and resilience program by presenting records or other documented evidence as specified for the first annual survey.

6.6 Wireless communication

6.6.1 Requirement

Wireless communication networks in the scope of this Section are to be designed, implemented and maintained to ensure that:

- Cyber incidents will not propagate to other control systems
- Only authorised human users will gain access to the wireless network
- Only authorised processes and devices will be allowed to communicate on the wireless network
- Information in transit on the wireless network cannot be manipulated or disclosed.

6.6.2 Rationale

Wireless networks give rise to additional or different cybersecurity risks than wired networks. This is mainly due to less physical protection of the devices and the use of the radio frequency communication.

Inadequate physical access control may lead to unauthorised personnel gaining access to the physical devices, which in turn could lead to circumventing logical access restrictions or deployment of rogue devices on the network.

Signal transmission by radio frequency introduces risks related to jamming as well as eavesdropping which in turn could cater for attacks such as Piggybacking or Evil twin attacks.

Note 1: See CISA (Cybersecurity and Infracstructure Security Agency) Tips ST05-003: Securing Wireless Networks (https://us-cert.cisa.gov/ncas/tips/ST05-003).

6.6.3 Requirements details

Cryptographic mechanisms such as encryption algorithms and key lengths in accordance with industry standards and best practices are to be applied to ensure integrity and confidentiality of the information transmitted on the wireless network.

Devices on the wireless network are only to communicate on the wireless network (i.e. they are not to be “dual-homed”)

Wireless networks are to be designed as separate segments in accordance with [6.2] and protected as per [6.3].

Wireless access points and other devices in the network are to be installed and configured such that access to the network can be controlled.

The network device or system utilizing wireless communication is to provide the capability to identify and authenticate all users (humans, software processes or devices) engaged in that communication.

6.6.4 Demonstration of compliance

a) Design phase:

The systems integrator is to include the following information in the Cyber security design description:

- Description of wireless networks in the scope of applicability of this Section and how these are implemented as separate security zones. The description is to include zone boundary devices and specify the traffic that is permitted to traverse the zone boundary (e.g. firewall rules)

b) Construction phase:

The systems integrator is to prevent unauthorised access to the wireless networks during the construction phase.

c) Commissioning phase:

The systems integrator is to submit Ship cyber resilience test procedure (see [10.3.2]) and demonstrate the following to the Society:

- Only authorised devices can access the wireless network.
- Secure wireless communication protocol is used as per approved documentation by the respective supplier (demonstrate e.g. by use of a network protocol analyser tool).

The above tests may be omitted if performed during the certification of CBSs as per [10.3.2]

d) Operation phase

- For general requirements to surveys in the operation phase, see [10.4]
- Special survey:

  Subject to modifications of the wireless networks in the scope of applicability of this Section the Shipowner is to demonstrate to the Society the activities in [6.6.4] as per the Ship cyber resilience test procedure.

6.7 Remote access control and communication with untrusted networks

6.7.1 Requirement

CBSs in scope of this Section are to be protected against unauthorized access and other cyber threats from untrusted networks.

6.7.2 Rationale

Onboard CBSs have become increasingly digitalized and connected to the internet to perform a wide variety of legitimate functions. The use of digital systems to monitor and control onboard CBSs makes them vulnerable to cyber incidents. Attackers may attempt to access onboard CBSs through connectivity with the internet and may be able to make changes that affect a CBS's operation or even achieve full control of the CBS, or attempt to download information from the ship's CBS. In addition, since use of legacy IT and OT systems that are no longer supported and/or rely on obsolete operating systems affects cyber resilience, special care should be put to relevant hardware and software installations on board to help maintain a sufficient level of cyber resilience when such systems can be remotely accessed, also keeping in mind that not all cyber incidents are a result of a deliberate attack.

6.7.3 Requirements details

User's manual is to be delivered for control of remote access to onboard IT and OT systems. Clear guidelines are to identify roles and permissions with functions.

For CBSs in the scope of applicability of this Section, no IP address is to be exposed to untrusted networks.

Communication with or via untrusted networks requires secure connections (e.g. tunnels) with endpoint authentication, protection of integrity and authentication and encryption at network or transport layer. Confidentiality is to be ensured for information that is subject to read authorization.

a) Design

CBSs in the scope of applicability of this Section are to:

- have the capability to terminate a connection from the onboard connection endpoint. Any remote access is not to be possible until explicitly accepted by a responsible role on board.
- be capable of managing interruptions during remote sessions so as not to compromise the safe functionality of OT systems or the integrity and availability of data used by OT systems.
- provide a logging function to record all remote access events and retain for a period of time sufficient for offline review of remote connections, e.g. after detection of a cyber incident.

b) Additional requirements for remote maintenance

When remote access is used for maintenance, the following requirements are to be complied with in addition to those in item a):

- Documentation is to be provided to show how they connect and integrate with the shore side.
- Security patches and softwares are to be tested and evaluated before they are installed to ensure they are effective and do not result in side effects or cyber events that cannot be tolerated. A confirmation report from the software supplier towards above is to be obtained, prior to undertaking remote update.
- Suppliers are to provide plans for- and make security updates available to the Shipowner, see Ch 5, Sec 2, [5.1.3], Ch 5, Sec 2, [5.1.4] and Ch 5, Sec 2, [5.1.5].
- At any time, during remote maintenance activities, authorized personnel is to have the possibility to interrupt and abort the activity and roll back to a previous safe configuration of the CBS and systems involved.
- Multi-factor authentication is required for any access by human users to CBS's in scope from an untrusted network.
- After a configurable number of failed remote access attempts, the next attempt is to be blocked for a predetermined length of time.
- If the connection to the remote maintenance location is disrupted for some reason, access to the system is to be terminated by an automatic logout function.

6.7.4 Demonstration of compliance

a) Design phase:

The systems integrator is to include the following information in the Cyber security design description:

- Identification of each CBS in the scope of applicability of this Section that can be remotely accessed or that otherwise communicates through the security zone boundary with untrusted networks.
- For each CBS, a description of compliance with requirements in [6.7.4], item c), as applicable

b) Construction phase:

The systems integrator is to ensure that any communication with untrusted networks is only temporarily enabled and used in accordance with the requirements of this section.

c) Commissioning phase:

The systems integrator is to submit Ship cyber resilience test procedure (see [10.3.2]) and demonstrate the following to the Society:

- Communication with untrusted networks is secured in accordance with Ch 5, Sec 2, [4.1.3] and that the communication protocols cannot be negotiated to a less secure version (demonstrate e.g., by use of a network protocol analyzer tool).
- Remote access requires multifactor authentication of the remote user.
- A limit of unsuccessful login attempts is implemented, and that a notification message is provided for the remote user before session is established.
- Remote connections must be explicitly accepted by responsible personnel on board.
- Remote sessions can be manually terminated by personnel on board or that the session will automatically terminate after a period of inactivity.
- Remote sessions are logged (see item No. 13 in Ch 5, Sec 2, Tab 1.
- Instructions or procedures are provided by the respective product suppliers (see Ch 5, Sec 2, [3.1.4]).

d) Operation phase

- For general requirements to surveys in the operation phase, see [10.4]
- The Shipowner is in the Ship cyber security and resilience program to describe the management of remote access and communication with/via untrusted networks, addressing at least the following requirements in this Section:
  - User's manual (see [6.7.3])
  - Roles and permissions (see [6.7.3])
  - Patches and updates (see [6.7.3], item b))
  - Confirmation prior to undertaking remote software update (see [6.7.3], item b))
  - Interrupt, abort, roll back (see [6.7.3], item b))
- Surveys:
  - First annual survey:

    The Shipowner is to present to the Society records or other documented evidence demonstrating implementation of the Ship cyber security and resilience program, i.e., that:
    - Remote access sessions have been recorded or logged and carried out as per relevant policies and user manuals.
    - Installation of security patches and other software updates have been carried out in accordance with Management of change procedures and in cooperation with the supplier.
  - Annual survey:

    The Shipowner is upon request by the Society to demonstrate implementation of the Ship cyber security and resilience program by presenting records or other documented evidence as specified for the first annual survey.

- Special survey:

  The Shipowner is to demonstrate to the Society the activities in [6.7.4], item c) as per the Ship cyber resilience test procedure.

6.8 Use of Mobile and Portable Devices

6.8.1 Requirement

The use of mobile and portable devices in CBSs in the scope of applicability of this Section is to be limited to only necessary activities and be controlled in accordance with item No. 10 in Ch 5, Sec 2, Tab 1. For any CBS that cannot fully meet these requirements, the interface ports is to be physically blocked.

6.8.2 Rationale

It is generally known that CBSs can be impaired due to malware infection via a mobile or a portable device. Therefore, connection of mobile and portable devices should be carefully considered. In addition, mobile equipment that is required to be used for the operation and maintenance of the shipshould be under the control of the Shipowner.

6.8.3 Requirements details

Mobile and portable devices are only to be used by authorised personnel. Only authorised devices may be connected to the CBSs. All use of such devices are to be in accordance with the Shipowner's policy for use of mobile and portable devices, taking into account the risk of introducing malware in the CBS.

6.8.4 Demonstration of compliance

a) Design phase:

The systems integrator is to include the following information in the Cyber security design description:

- Any CBSs in the scope of applicability that do not meet the requirements of item No. 10 in Ch 5, Sec 2, Tab 1 i.e., that is to have protection of interface ports by physical means such as port blockers.

b) Construction phase:

The systems integrator is to ensure that use of physical interface ports in the CBSs is controlled in accordance with item No. 10 in Ch 5, Sec 2, Tab 1, and that any use of such devices follows procedures to prevent malware from being introduced in the CBS.

c) Commissioning phase:

The systems integrator is to submit Ship cyber resilience test procedure (see [10.3.2])) and demonstrate to the Society that capabilities to control use of mobile and portable devices are implemented correctly, the following countermeasures is to be be demonstrated as relevant:

- Use of mobile and portable devices is restricted to authorised users
- Interface ports can only be used by specific device types
- Files cannot be transferred to the system from such devices
- Files on such devices will not be automatically executed (by disabling autorun)
- Network access is limited to specific MAC or IP addresses
- Unused interface ports are disabled
- Unused interface ports are physically blocked

d) Operation phase:

- For general requirements to surveys in the operation phase, see [10.4].
- The Shipowner is in the Ship cyber security and resilience program to describe the management of mobile and portable devices, addressing at least the following requirements in this Section:
  - Policy and procedures (see [8.4.4])
  - Physical block of interface ports (see [6.8.1])
  - Use by authorized personnel (see [6.8.3])
  - Connect only authorized devices (see [6.8.3])
  - Consider risk of introducing malware (see [6.8.3])
- Surveys:
  - First annual survey:

    The Shipowner isl present to the Society records or other documented evidence demonstrating implementation of the Ship cyber security and resilience program, i.e., that:

    - The use of mobile, portable or removable media is restricted to authorised personnel and follows relevant policies and procedures.
    - Only authorised devices are connected to the CBSs.
    - Means to restrict use of physical interface ports are implemented as per approved design documentation.

- Subsequent annual surveys:

  The Shipowner is upon request by the Society to demonstrate implementation of the Ship cyber security and resilience program by presenting records or other documented evidence as specified for the first annual survey.

- Special survey:

  The Shipowner is to demonstrate to the Society the activities in [6.8.4], item c) as per the Ship cyber resilience test procedure.

7 Detect

7.1 General

7.1.1 The requirements for the "Detect" functional element are aimed at the development and implementation of appropriate means supporting the ability to reveal and recognize anomalous activity on CBSs and networks onboard and identify cyber incidents.

7.2 Network operation monitoring

7.2.1 Requirement

Networks in scope of this Section are to be continuously monitored, and alarms are to be generated if malfunctions or reduced/ degraded capacity occurs.

7.2.2 Rationale

Cyber-attacks are becoming increasingly sophisticated, and attacks that target vulnerabilities that were unknown at the time of construction could result in incidents where the vessel is ill- prepared for the threat. To enable an early response to attacks targeting these types of unknown vulnerabilities, technology capable of detecting unusual events is required. A monitoring system that can detect anomalies in networks and that can use post-incident analysis provides the ability to appropriately respond and further recover from a cyber event.

7.2.3 Requirements details

Measures to monitor networks in the scope of applicability of this Section are to have the following capabilities:

- Monitoring and protection against excessive traffic
- Monitoring of network connections
- Monitoring and recording of device management activities
- Protection against connection of unauthorized devices
- Generate alarm if utilization of the network's bandwidth exceeds a threshold specified as abnormal by the supplier. See NR467, Pt C, Ch 3 Sec 3, [6.1].

Intrusion detection systems (IDS) can be implemented, subject to the following:

- The IDS are to be qualified by the supplier of the respective CBS
- The IDS are to be passive and not activate protection functions that may affect the performance of the CBS
- Relevant personnel is to be trained and qualified for using the IDS.

7.2.4 Demonstration of compliance

a) Design phase:

No requirements.

b) Construction phase:

No requirements.

c) Commissioning phase:

The systems integrator is to specify in the Ship cyber resilience test procedure and demonstrate to the Society the network monitoring and protection mechanisms in the CBSs.

- Test that disconnected network connections will activate alarm and that the event is recorded.
- Test that abnormally high network traffic is detected, and that alarm and audit record is generated. This test may be carried on together with the test in [8.5.4], item c).
- Demonstrate generation of audit records (logging of security-related events)
- If Intrusion detection systems are implemented, demonstrate that this is passive and will not activate protection functions that may affect intended operation of the CBSs.

The above tests may be omitted if performed during the certification of CBSs as per [10.3.2])

Any Intrusion detection systems in the CBSs in scope of applicability to be implemented is to be subject to verification by the Society. Relevant documentation is to be submitted for approval, and survey/tests is to be carried out on board.

d) Operation phase

- For general requirements to surveys in the operation phase, see [10.4].
- The Shipowner is in the Ship cyber security and resilience program to describe the management activities to detect anomalies in the CBSs and networks, addressing at least the following requirements in this Section:
  - Reveal and recognize anomalous activity (see [7])
  - Inspection of security audit records (see [7.2.3])
  - Instructions or procedures to detect incidents (see [8.2.1])

  The above activities may be addressed together with incident response in [8.2].
- Surveys:
  - First annual survey:

    The Shipowner is to present to the Society records or other documented evidence demonstrating implementation of the Ship cyber security and resilience program, i.e., that:
    - The CBSs are routinely monitored for anomalies by inspection of security audit records and investigation of alerts in the CBSs.
  - Subsequent annual surveys:

    The Shipowner is upon request by the Society to demonstrate implementation of the Ship cyber security and resilience program by presenting records or other documented evidence as specified for the first annual survey.
  - Special survey:

    Subject to modifications of the CBSs, the Shipowner is to demonstrate to the Society the activities in [7.2.4], item c) as per the Ship cyber resilience test procedure.

7.3 Verification and diagnostic functions of CBS and networks

7.3.1 Requirement

CBSs and networks in the scope of applicability of this Section are to be capable to check performance and functionality of security functions required by this Section. Diagnostic functions are to provide adequate information on CBSs integrity and status for the use of the intended user and means for maintaining their functionality for a safe operation of the ship.

7.3.2 Rationale

The ability to verify intended operation of the security functions is important to support management of cyber resilience in the lifetime of the ship. Tools for diagnostic functions may comprise automatic or manual functions such as self-diagnostics capabilities of each device, or tools for network monitoring (such as ping, traceroute, ipconfig, netstat, nslookup, Wireshark, nmap, etc.).

It should be noted however that execution of diagnostic functions may sometimes impact the operational performance of the CBS.

7.3.3 Requirements details

CBSs and networks' diagnostics functionality are to be available to verify the intended operation of all required security functions during test and maintenance phases of the ship.

7.3.4 Demonstration of compliance

a) Design phase:

No requirements.

b) Construction phase:

No requirements.

c) Commissioning phase:

The systems integrator is to submit Ship cyber resilience test procedure (see [10.3.2]) and demonstrate to the Society the effectiveness of the procedures for verification of security functions provided by the suppliers.

The above tests may be omitted if performed during the certification of CBSs as per [10.3.2].

d) Operation phase:

- For general requirements to surveys in the operation phase, see [10.4].
- The Shipowner is in the Ship cyber security and resilience program to describe the management activities to verify correct operation of the security functions in the CBSs and networks, addressing at least the following requirements in this Section:
  - Test and maintenance periods (see [7.3.3])
  - Periodic maintenance (see [10.4.4])
- Surveys:
  - First annual survey:

    The Shipowner is to present to the Society records or other documented evidence demonstrating implementation of the Ship cyber security and resilience program, i.e., that:
    - The security functions in the CBSs are periodically tested or verified.

- Subsequent annual surveys:

  The Shipowner is upon request by the Society to demonstrate implementation of the Ship cyber security and resilience program by presenting records or other documented evidence as specified for the first annual survey.

8 Respond

8.1 General

8.1.1 The requirements for the "Respond" functional element are aimed at the development and implementation of appropriate means supporting the ability to minimize the impact of cyber incidents, containing the extension of possible impairment of CBSs and networks onboard.

8.2 Incident response plan

8.2.1 Requirement

An incident response plan is to be developed by the Shipowner covering relevant contingencies and specifying how to react to cyber security incidents. The Incident response plan is to contain documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of incidents against CBSs in the scope of applicability of this Section.

8.2.2 Rationale

An incident response plan is an instrument aimed to help responsible persons respond to cyber incidents. As such, the Incident response plan is as effective as it is simple and carefully designed. When developing the Incident response plan, it is important to understand the significance of any cyber incident and prioritize response actions accordingly.

Means for maintaining as much as possible the functionality and a level of service for a safe operation of the ship, e.g. transfer active execution to a standby redundant unit, should also be indicated. Designated personnel ashore should be integrated with the ship in the event of a cyber incident.

8.2.3 Requirements details

The various stakeholders involved in the design and construction phases of the ship are to provide information to the Shipowner for the preparation of the Incident Response Plan to be placed onboard at the first annual Survey. The Incident Response Plan is to be kept up-to- date (e.g. upon maintenance) during the operational life of the ship.

The Incident response plan is to provide procedures to respond to detected cyber incidents on networks by notifying the proper authority, reporting needed evidence of the incidents and taking timely corrective actions, to limit the cyber incident impact to the network segment of origin.

The incident response plan is, as a minimum, to include the following information:

- Breakpoints for the isolation of compromised systems
- A description of alarms and indicators signalling detected ongoing cyber events or abnormal symptoms caused by cyber events
- A description of expected major consequences related to cyber incidents
- Response options, prioritizing those which do not rely on either shut down or transfer to independent or local control, if any
- Independent and local control information for operating independently from the system that failed due to the cyber incident, as applicablr

The Incident response plan is to be kept in hard copy in the event of complete loss of electronic devices enabling access to it.

8.2.4 Demonstration of compliance

a) Design phase:

   The systems integrator is to include the following information in the Cyber security design description:

   - References to information provided by the suppliers (see Ch 5, Sec 2, [3.1.9]) that may be applied by the Shipowner to establish plans for incident response.

b) Construction phase

   No requirements.

c) Commissioning phase

   No requirements.

d) Operation phase

   - For general requirements to surveys in the operation phase, see [10.4].

- The Shipowner is in the Ship cyber security and resilience to program describe incident response plans. The plans are to cover the CBSs in scope of applicability of this Section and are to address at least the following requirements in this Section:
  - Description of who, when and how to respond to cyber incidents in accordance with requirements of [8.2]
  - Procedures or instructions for local/manual control in accordance with requirements in [8.3]
  - Procedures or instructions for isolation of security zones in accordance with requirements in [8.4]
  - Description of expected behaviour of the CBSs in the event of cyber incidents in accordance with requirements in [8.5].
- Surveys:
  - First annual survey:

    The Shipowner is to present to the Society records or other documented evidence demonstrating implementation of the Ship cyber security and resilience program, i.e., that:
    - The incident response plans are available for the responsible personnel onboard.
    - Procedures or instructions for local/manual controls are available for responsible personnel onboard.
    - Procedures or instructions for disconnection/isolation of security zones are available for responsible personnel onboard.
    - Any cyber incidents have been responded to in accordance with the incident response plans.
  - Subsequent annual surveys:

    The Shipowner is upon request by the Society to demonstrate implementation of the Ship cyber security and resilience program by presenting records or other documented evidence as specified for the first annual survey.

8.3 Local, independent and/or manual operation

8.3.1 Requirement

Any CBS needed for local backup control as required by SOLAS II-1 Regulation 31 is to be independent of the primary control system. This includes also necessary Human Machine Interface (HMI) for effective local operation.

8.3.2 Rationale

Independent local controls of machinery and equipment needed to maintain safe operation is a fundamental principle for manned vessels. The objective of this requirement has traditionally been to ensure that personnel can cope with failures and other incidents by performing manual operations in close vicinity of the machinery. Since incidents caused by malicious cyber events are also to be considered, this principle of independent local control is no less important.

8.3.3 Requirements details

The CBS for local control and monitoring are to be self-contained and not depend on communication with other CBS for its intended operation.

If communication to the remote control system or other CBS's is arranged by networks, segmentation and protection safeguards as described in [6.2] and [6.3] are to be implemented. This implies that the local control and monitoring system are to be considered a separate security zone. Notwithstanding the above, special considerations can be given to CBSs with different concepts on case by case basis.

The CBS for local control and monitoring are otherwise to comply with requirements in this Section.

8.3.4 Demonstration of compliance

a) Design phase:

The systems integrator is to include the following information in the Cyber security design description:

- Description of how the local controls specified in SOLAS II-1 Reg.31 are protected from cyber incidents in any connected remote or automatic control systems.

b) Construction phase:

No requirements.

c) Commissioning phase:

The systems integrator is to submit Ship cyber resilience test procedure (see [10.3.2]) and demonstrate to the Society that the required local controls in the scope of applicability of this Section needed for safety of the ship can be operated independently of any remote or automatic control systems. The tests are to be carried out by disconnecting all networks from the local control system to other systems/devices.

The above tests may be omitted if performed during the certification of CBSs as per [10.3.2].

d) Operation phase:

- For general requirements to surveys in the operation phase, see [10.4].
- Special survey:

  Subject to modifications of the CBSs, the Shipowner is to demonstrate to the Society the activities in [8.3.4] as per the Ship cyber resilience test procedure.

8.4 Network isolation

8.4.1 Requirement

It is to be possible to terminate network-based communication to or from a security zone.

8.4.2 Rationale

In the event that a security breach has occurred and is detected, it is likely that the incident response plan includes actions to prevent further propagation and effects of the incident.

Such actions could be to isolate network segments and control systems supporting essential functions.

8.4.3 Requirements details

Where the Incident Response Plan indicates network isolation as an action to be done, it is to be possible to isolate security zones according to the indicated procedure, e.g. by operating a physical ON/OFF switch on the network device or similar actions such as disconnecting a cable to the router/firewall. There is to be available instructions and clear marking on the device that allows the personnel to isolate the network in an efficient manner.

Individual system's data dependencies that may affect function and correct operation, including safety, are to be identified, clearly showing where systems must have compensations for data or functional inputs if isolated during a contingency.

8.4.4 Demonstration of compliance

a) Design phase:

The systems integrator is to include the following information in the Cyber security design description:

- specification of how to isolate each security zone from other zones or networks. The effects of such isolation are also to be described, demonstrating that the CBSs in a security zone do not rely on data transmitted by IP-networks from other zones or networks.

b) Construction phase:

No requirements.

c) Commissioning phase:

The systems integrator is to submit Ship cyber resilience test procedure (see [10.3.2]) and demonstrate to the Society by disconnecting all networks traversing security zone boundaries, that the CBSs in the security zone will maintain adequate operational functionality without network communication with other security zones or networks.

The above tests may be omitted if performed during the certification of CBSs as per [10.3.2].

d) Operation phase:

- For general requirements to surveys in the operation phase, see [10.4].
- Special survey:

  Subject to modifications of the CBSs, the Shipowner is to demonstrate to the Society the activities in [8.4.4], item c) as per the Ship cyber resilience test procedure.

8.5 Fallback to a minimal risk condition

8.5.1 Requirement

In the event of a cyber incident impairing the ability of a CBS or network in the scope of applicability of this Section to provide its intended service, the affected system or network is to fall back to a minimal risk condition, i.e. bring itself in a stable, stopped condition to reduce the risk of possible safety issues.

8.5.2 Rationale

The ability of a CBS and integrated systems to fallback to one or more minimal risk conditions to be reached in case of unexpected or unmanageable failures or events is a safety measure aimed to keep the system in a consistent, known and safe state.

Fallback to a minimal risk condition usually implies the capability of a system to abort the current operation and signal the need for assistance, and may be different depending on the environmental conditions, the voyage phase of the ship (e.g. port depart/arrival vs. open sea passage) and the events occurred.

8.5.3 Requirements details

As soon as a cyber incident affecting the CBS or network is detected, compromising the system's ability to provide the intended service as required, the system is to fall back to a condition in which a reasonably safe state can be achieved. Fall-back actions are to include:

- bringing the system to a complete stop or other safe state
- disengaging the system
- transferring control to another system or human operator
- other compensating actions.

Fall-back to minimum risk conditions is to occur in a time frame adequate to keep the ship in a safe condition.

The ability of a system to fall back to a minimal risk condition is to be considered from the design phase by the Supplier and the System Integrator.

8.5.4 Demonstration of compliance

a) Design phase:

The systems integrator is to include the following information in the Cyber security design description:

- Specification of safe state for the control functions in the CBSs in the scope of applicability of this Section.

b) Construction phase:

No requirements.

c) Commissioning phase:

The systems integrator is to submit Ship cyber resilience test procedure (see [10.3.2]) and demonstrate to the Society that CBSs in the scope of applicability of this Section respond to cyber incidents in a safe manner (as per [8.5.4]), e.g. by maintaining its outputs to essential services and allowing operators to carry out control and monitoring functions by alternative means. The tests is at least to include denial of service (DoS) attacks and may be done together with related test in [7.2.4], item a).

The above tests may be omitted if performed during the certification of CBSs as per [10.3.2].

d) Operation phase:

- For general requirements to surveys in the operation phase, see [10.4].
- Special survey:

  Subject to modifications of the CBSs, the Shipowner is to demonstrate to the Society the activities in [8.5.4], item c) as per the Ship cyber resilience test procedure.

9 Recover

9.1 General

9.1.1 The requirements for the “Recover” functional element are aimed at the development and implementation of appropriate means supporting the ability to restore CBSs and networks onboard affected by cyber incidents.

9.2 Recovery plan

9.2.1 Requirement

A recovery plan is to be made by the Shipowner to support restoring CBSs under the scope of applicability of this Section to an operational state after a disruption or failure caused by a cyber incident. Details of where assistance is available and by whom are to be part of the recovery plan.

9.2.2 Rationale

Incident response procedures are an essential part of system recovery. Responsible personnel should consider carefully and be aware of the implications of recovery actions (such as wiping of drives) and execute them carefully.

It should be noted, however, that some recovery actions may result in the destruction of evidence that could provide valuable information on the causes of an incident.

Where appropriate, externalcyber incident response support is to be obtained to assist in preservation of evidence whilst restoring operational capability.

9.2.3 Requirements details

The various stakeholders involved in the design and construction phases of the ship are to provide information to the Shipowner for the preparation of the recovery plan to be placed onboard at the first annual Survey. The recovery plan is to be kept up-to-date (e.g. upon maintenance) during the operational life of the ship.

Recovery plans are to be easily understandable by the crew and external personnel and include essential instructions and procedures to ensure the recovery of a failed system and how to get external assistance if the support from ashore is necessary. In addition, software recovery medium or tools essential for recovery on board are to be available.

When developing recovery plans, the various systems and subsystems involved are to be specified. The following recovery objectives are also to be specified:

a) System recovery: methods and procedures to recover communication capabilities are to be specified in terms of Recovery Time Objective (RTO). This is defined as the time required to recover the required communication links and processing capabilities.

b) Data recovery: methods and procedures to recover data necessary to restore safe state of OT systems and safe ship operation are to be specified in terms of Recovery Point Objective (RPO). This is defined as the longest period of time for which an absence of data can be tolerated.

Once the recovery objectives are defined, a list of potential cyber incidents is to be created, and the recovery procedure developed and described. Recovery plans are to include, or refer to the following information:

a) Instructions and procedures for restoring the failed system without disrupting the operation from the redundant, independent or local operation.

b) Processes and procedures for the backup and secure storage of information.

c) Complete and up-to-date logical network diagram.

d) The list of personnel responsible for restoring the failed system.

e) Communication procedure and list of personnel to contact for external technical support including system support vendors, network administrators, etc.

f) Current configuration information for all components.

The operation and navigation of the ship are to be prioritized in the plan in order to help ensure the safety of onboard personnel.

Recovery plans in hard copy onboard and ashore are to be available to personnel responsible for cyber security and who are tasked with assisting in cyber incidents.

9.2.4 Demonstration of compliance

a) Design phase:

The systems integrator is to include the following information in the Cyber security design description:

- references to information provided by the suppliers (see Ch 5, Sec 2, [3.1.9] that may be applied by the Shipowner to establish plans to recover from cyber incidents.

b) Construction phase:

No requirements.

c) Commissioning phase:

The systems integrator is to submit Ship cyber resilience test procedure (see [10.3.2]) and demonstrate to the Society the effectiveness of the procedures and instructions provided by the suppliers to respond to cyber incidents as specified in [6.4] and [6.5].

The above tests may be omitted if performed during the certification of CBSs as per [10.3.2].

d) Operation phase:

- For general requirements to surveys in the operation phase, see [10.4].
- The Shipowner is in the Ship cyber security and resilience program to describe incident recovery plans. The plans is to cover the CBSs in scope of applicability of this Section and is to address at least the following requirements in this Section:
  - Description of who, when and how to restore and recover from cyber incidents in accordance with requirements in [9.2]
  - Policy for backup addressing frequency, maintenance and testing of the backups, considering acceptable downtime, availability of alternative means for control, vendor support arrangements and criticality of the CBSs in accordance with requirements in [9.3].
  - Reference to user manuals or procedures for backup, shutdown, reset, restore and restart of the CBSs in accordance with requirements in [9.3] and [9.4].
- Surveys:
  - First annual survey:

    The Shipowner is to present to the Society records or other documented evidence demonstrating implementation of the Ship cyber security and resilience program, i.e., that:
    - Instructions and/or procedures for incident recovery are available for the responsible personnel onboard.
    - Equipment, tools, documentation, and/or necessary software and data needed for recovery is available for the responsible personnel onboard.
    - Backup of the CBSs have been taken in accordance with the policies and procedures.
    - Manuals and procedures for shutdown, reset, restore and restart are available for the responsible personnel onboard.
  - Subsequent annual surveys:

    The Shipowner is upon request by the Society to demonstrate implementation of the Ship cyber security and resilience program by presenting records or other documented evidence as specified for the first annual survey.

9.3 Backup and restore capability

9.3.1 Requirement

CBSs and networks in the scope of applicability of this Section are to have the capability to support back-up and restore in a timely, complete and safe manner. Backups are to be regularly maintained and tested.

9.3.2 Rationale

In general, the purpose of a backup and restore strategy should protect against data loss and reconstruct the database after data loss. Typically, backup administration tasks include the following: Planning and testing responses to different kinds of failures. Configuring the database environment for backup and recovery; Setting up a backup schedule; Monitoring the backup and recovery environment; Creating a database copy for long-term storage; Moving data from one database or one host to another, etc.

9.3.3 Requirements details

a) Restore capability

CBSs in the scope of applicability of this Section are to have backup and restore capabilities to enable the ship to safely regain navigational and operational state after a cyber incident.

Data are to be restorable from a secure copy or image.

Information and backup facilities are to be sufficient to recover from a cyber incident.

b) Backup

CBSs and networks in the scope of applicability of this Section are to provide backup for data. The use of offline backups are also to be considered to improve tolerance against ransomware and worms affecting online backup appliances.

Backup plans are to be developed, including scope, mode and frequency, storage medium and retention period.

9.3.4 Demonstration of compliance

a) Design phase:

No requirements.

b) Construction phase:

No requirements.

c) Commissioning phase:

The systems integrator is to submit Ship cyber resilience test procedure (see [10.3.2]) and demonstrate to the Society the procedures and instructions for backup and restore provided by the suppliers for CBSs in the scope of applicability of this Section.

The above tests may be omitted if performed during the certification of CBSs as per [10.3.2].

d) Operation phase:

- For general requirements to surveys in the operation phase, see [10.4].
- Special survey:

  Subject to modifications of the CBSs, the Shipowner is to demonstrate to the Society the activities in [9.3.4], item c) as per the Ship cyber resilience test procedure.

9.4 Controlled shutdown, reset, roll-back and restart

9.4.1 Requirement

CBS and networks in the scope of applicability of this Section are to be capable of controlled shutdown, reset to an initial state, roll-back to a safe state and restart from a power-off condition in such state, in order to allow fast and safe recovery from a possible impairment due to a cyber incident.

Suitable documentation on how to execute the above-mentioned operations are to be available to onboard personnel.

9.4.2 Rationale

Controlled shutdown consists in turning a CBS or network off by software function allowing other connected systems to commit/rollback pending transactions, terminating processes, closing connections, etc. leaving the entire integrated system in a safe and known state.

Controlled shutdown is opposed to hard shutdown, which occurs for example when the computer is forcibly shut down by interruption of power.

While in the case of some cyber incidents hard shutdowns may be considered as a safety precaution, controlled shutdown is preferable in case of integrated systems to keep them in a consistent and known state with predictable behaviour. When standard shutdown procedures are not done, data or program and operating system files corruption may occur. In case of OT systems, the result of corruption can be instability, incorrect functioning or failure to provide the intended service.

The reset operation would typically kick off a soft boot, instructing the system to go through the process of shutting down, clear memory and reset devices to their initialized state.

Depending on system considered, the reset operation might have different effects.

Rollback is an operation which returns the system to some previous state. Rollbacks are important for data and system integrity, because they mean that the system data and programs can be restored to a clean copy even after erroneous operations are performed. They are crucial for recovering from crashes ad cyber incidents, restoring the system to a consistent state.

Restarting a system and reloading a fresh image of all the software and data (e.g. after a rollback operation) from a read-only source appears to be an effective approach to recover from unexpected faults or cyber incidents. Restart operations should be however controlled in particular for integrated systems, where unexpected restart of a single component can result in inconsistent system state or unpredictable behaviour.

9.4.3 Requirements details

CBS and networks in the scope of applicability of this Section are to be capable of:

- controlled shutdown allowing other connected systems to commit/rollback pending transactions, terminating processes, closing connections, etc. leaving the entire integrated system in a safe, consistent and known state.
- resetting themselves, instructing the system to go through the process of shutting down, clear memory and reset devices to their initialized state.
- rolling back to a previous configuration and/or state, to restore system integrity and consistency.
- restarting and reloading a fresh image of all the software and data (e.g. after a rollback operation) from a read-only source. Restart time is to be compatible with the system's intended service and is not to bring other connected systems, or the integrated system it is part of, to an inconsistent or unsafe state.

Documentation is to be available to onboard personnel on how to execute the above- mentioned operations in case of a system affected by a cyber incident.

9.4.4 Demonstration of compliance

a) Design phase:

The systems integrator is to include the following information in the Cyber security design description:

- references to product manuals or procedures describing how to safely shut down, reset, restore and restart the CBSs in the scope of applicability of this Section.

b) Construction phase:

No requirements.

c) Commissioning phase:

The systems integrator is to submit Ship cyber resilience test procedure (see [10.3.2]) and demonstrate to the Society that manuals or procedures are established for shutdown, reset and restore of the CBSs in the scope of applicability of this Section. These manuals/procedures is to be provided to the Shipowner.

The above tests may be omitted if performed during the certification of CBSs as per [10.3.2].

d) Operation phase:

- For general requirements to surveys in the operation phase, see [10.4]
- Special survey:

  Subject to modifications of the CBSs, the Shipowner is to demonstrate to the Society the activities in [9.4.4]as per the Ship cyber resilience test procedure.

10 Demonstration of compliance

10.1 General

10.1.1 Evaluation of compliance with requirements in this Section is to be carried out by the Society by assessment of documentation and survey in the relevant phases as specified in the following.

Documentation to be submitted by suppliers to the Society is specified in Ch 5, Sec 2. The approved versions of this documentation are also be provided by the suppliers to the systems integrator as specified in Ch 5, Sec 2, [6.2].

Documents to be provided by the systems integrator are listed in [10.2] and [10.3].

Documents to be provided by the Shipowner are listed in [10.4].

Upon delivery of the ship, the systems integrator is to provide below documentation to the Shipowner:

- Documentation of the CBSs provided by the suppliers (see Ch 5, Sec 2, [6.2])
- Documentation produced by the systems integrator (see sections 5.1 and 5.2)

See also Tab 1 and Tab 2 for a summary of the documents.

Table 1 : Summary of actions and documents

Topic	System integrator			Shipowner			
	Design	Construction	Commissioning	Operation	First annual survey	Annual survey	Special survey
Approved supplier documentation. See [10]		M	M	M			
Zones and conduit diagram. See [10.2.2]	S	M	M	M			
Cyber security design description. See [10.2.3]	S	M	M	M			
Vessel asset inventory. See [10.2.4]	S	M	M	M			
Risk assessment for the exclusion of CBSs **(1)**. See [10.2.5]	S	M	M	M			
Description of compensating countermeasures **(1)**. See [10.2.6]	S	M	M	M			
Ship cyber resilience test procedure. See [10.3.2]		S	D	M			D
Ship cyber security and resilience program. See [10.4.2]: • Management of change (MoC). See [5.2.6], itemc) • Management of software updates. See [5.2.6], itemc) • Management of firewalls. See [6.2.4], item c) • Management of malware protection. See [6.4.4], item c) • Management of access control. See [6.5.4], item c) • Management of confidential information. See [6.5.4], item c) • Management of remote access. See [6.7.4], item c) • Management of mobile and portable devices. See [6.8.4], item c) • Detection of security anomalies. See [7.2.4], item c) • Verification of security functions. See [7.3.4], item c) • Incident response plans. See [8.2.4], item c) • Recovery plans. See [9.2.4], item c)				M	S	D	

(1) If applicable.

Note 1:

- S = Submit: The stakeholder is to submit the document to the Society for verification and approval of compliance with requirements in this Section
- M = Maintain: The stakeholder is to keep the document updated in accordance with procedure for management of change (MoC). Updated document and change management records is to be submitted to the Society as per NR467, Pt C Ch 3 Sec 3.
- D = Demonstrate: The stakeholder is to demonstrate compliance to the Society in accordance with the approved document.

Table 2 : Summary of requirements and documents

Document / Requirement		Reference
Vessel asset inventory (see [5.2])		
• CBS security capabilities	- Provide documentation of product security updates - Provide documentation of dependent component security updates - Provide security updates	Ch 5, Sec 2, [5.1.3] Ch 5, Sec 2, [5.1.4] Ch 5, Sec 2, [5.1.5]
• CBS documentation	- CBS asset inventory - Management of change plan	Ch 5, Sec 2, [3.1.2] Ch 5, Sec 2, [3.1.10]
• Vessel design documentation	Vessel asset inventory	[5.2.6], item a)
• Ship cyber security and resilience program	Management of change	[5.2.6], item d)
	Management of software updates	[5.2.6], item d)
Security zones and network segmentation (see [6.2])		
• CBS security capabilities		
• CBS documentation	Topology diagrams	Ch 5, Sec 2, [3.1.3]
• Vessel design documentation	- Zones and conduit diagram - Design description - Ship cyber resilience test procedure	[6.2.4], item a) [6.2.4], item a) [6.2.4], item c)
• Ship cyber security and resilience program	Management of security zone boundary devices (e.g., firewalls)	[6.2.4], item d)

Document / Requirement		Reference
Network protection safeguards (see [6.3])		
• CBS security capabilities	- Denial of service (DoS) protection - Deterministic output	Ch 5, Sec 2, [4.1.2] and items No. 20 and 24 in Ch 5, Sec 2, Tab 1
• CBS documentation	- Description of security capabilities - Test procedure for security capabilities	Ch 5, Sec 2, [3.1.4] Ch 5, Sec 2, [3.1.5])
• Vessel design documentation	Ship cyber resilience test procedure	[6.3.4], item c)
• Ship cyber security and resilience program		
Antivirus, antimalware, antispam and other protections from malicious code (see [6.4])		
• CBS security capabilities	Malicious code protection	Ch 5, Sec 2, [4.1.2] and items No. 18 in Ch 5, Sec 2, Tab 1
• CBS documentation	- Description of security capabilities - Test procedure for security capabilities	Ch 5, Sec 2, [3.1.4] Ch 5, Sec 2, [3.1.5]
• Vessel design documentation	- Design description - Ship cyber resilience test procedure	[6.4.4], item a) [6.4.4], item c)
• Ship cyber security and resilience program	Management of malware protection	[6.4.4], item d)
Access control (see [6.5])		
• CBS security capabilities	- Human user id. and auth. - Account management - Identifier management - Authenticator management - Authorisation enforcement	Ch 5, Sec 2, [4.1.2] and items No. 1, 2, 3, 4 and 8 in Ch 5, Sec 2, Tab 1
• CBS documentation	- Description of security capabilities - Test procedure for security capabilities	Ch 5, Sec 2, [3.1.4] Ch 5, Sec 2, [3.1.5]
• Vessel design documentation	- Design description - Ship cyber resilience test procedure	[6.5.4], item a) [6.5.4], item c)
• Ship cyber security and resilience program	Management of confidential information	[6.5.4], item d)
	Management of logical and physical access	[6.5.4], item d)
Wireless communication (see [6.6])		
• CBS security capabilities	- Wireless access management - Wireless use control	Ch 5, Sec 2, [4.1.2] and items No. 5 and 9 in Ch 5, Sec 2, Tab 1
• CBS documentation	- Description of security capabilities - Test procedure for security capabilities	Ch 5, Sec 2, [3.1.4] Ch 5, Sec 2, [3.1.5]
• Vessel design documentation	- Design description - Ship cyber resilience test procedure	[6.6.4] item a) [6.6.4] item c)
• Ship cyber security and resilience program		
Remote access control and communication with untrusted networks (see [6.7])		
• CBS security capabilities	- Multifactor authentication - Process / device id. and auth. - Unsuccessful login attempts - System use notification - Access via untrusted networks - Explicit access request approval - Remote session termination - Cryptographic integrity protection - Input validation - Session integrity - Invalidation of session ID	Ch 5, Sec 2, [4.1.3] and items No. 31, 32, 33, 34, 35, 37, 38, 39, 40 and 41 in Ch 5, Sec 2, Tab 2
• CBS documentation	- Description of security capabilities - Test procedure for security capabilities	Ch 5, Sec 2, [3.1.4] Ch 5, Sec 2, [3.1.5]
• Vessel design documentation	- Design description - Ship cyber resilience test procedure	[6.7.4], item a) [6.7.4], item c)
• Ship cyber security and resilience program	Management of remote access and communication with/via untrusted networks	[6.7.4], item d)

Document / Requirement		Reference
Use of mobile and portable devices (see [6.8])		
• CBS security capabilities	Use control for portable devices	Ch 5, Sec 2, [4.1.2] and items No. 10 in Ch 5, Sec 2, Tab 1
• CBS documentation	- Description of security capabilities - Test procedure for security capabilities	Ch 5, Sec 2, [3.1.4] Ch 5, Sec 2, [3.1.5]
• Vessel design documentation	- Design description - Ship cyber resilience test procedure	[6.8.4], item a) [6.8.4], item c)
• Ship cyber security and resilience program	Management of mobile and portable devices	[6.8.4], item d)
Network operation monitoring (see [7.2])		
• CBS security capabilities	- Use control for portable devices - Auditable events - Denial of service (DoS) protection	Ch 5, Sec 2, [4.1.2] and items No. 10, 13 and 24 in Ch 5, Sec 2, Tab 1
	Alarm excessive bandwidth use	NR467, Pt C, Ch 3, Sec 3, [6.1]
• CBS documentation	- Description of security capabilities - Test procedure for security capabilities	Ch 5, Sec 2, [3.1.4] Ch 5, Sec 2, [3.1.5]
• Vessel design documentation	Ship cyber resilience test procedure	[7.2.4], item c)
• Ship cyber security and resilience program	Incident response plans	[8.2.4], item d)
Verification and diagnostic functions of CBS and networks (see [7.3])		
• CBS security capabilities	Security function verification	Ch 5, Sec 2, [4.1.2] and items No. 19 and 9 in Ch 5, Sec 2, Tab 1
• CBS documentation	- Description of security capabilities - Test procedure for security capabilities - Plans for maintenance and verification	Ch 5, Sec 2, [3.1.4] Ch 5, Sec 2, [3.1.5] Ch 5, Sec 2, [3.1.8]
• Vessel design documentation	Ship cyber resilience test procedure	[7.3.4], item c)
• Ship cyber security and resilience program	Verification of security functions	[7.3.4], item d)
Incident response plan (see [8.2])		
• CBS security capabilities		
• CBS documentation	- Description of security capabilities - Test procedure for security capabilities - Information supporting incident response and recovery plans	Ch 5, Sec 2, [3.1.4] Ch 5, Sec 2, [3.1.5] Ch 5, Sec 2, [3.1.9]
• Vessel design documentation	- Design description - Ship cyber resilience test procedure	[8.2.4], item a) [8.2.4], item c)
• Ship cyber security and resilience program	Incident response plans	[8.2.4], item d)
Local, independent and/or manual operation (see [8.3])		
• CBS security capabilities		
• CBS documentation	- Description of security capabilities - Test procedure for security capabilities - Information supporting incident response and recovery plans	Ch 5, Sec 2, [3.1.4] Ch 5, Sec 2, [3.1.5] Ch 5, Sec 2, [3.1.9]
• Vessel design documentation	- Design description - Ship cyber resilience test procedure	[8.5.4], item a) [8.5.4], item c)
• Ship cyber security and resilience program	Incident response plans	[8.2.4], item d)
Network isolation (see [7.2])		
• CBS security capabilities		
• CBS documentation	- Description of security capabilities - Test procedure for security capabilities - Information supporting incident response and recovery plans	Ch 5, Sec 2, [3.1.4] Ch 5, Sec 2, [3.1.5] Ch 5, Sec 2, [3.1.9]
• Vessel design documentation	- Design description - Ship cyber resilience test procedure	[7.2.4], item a) [7.2.4], item c)
• Ship cyber security and resilience program	Incident response plans	[8.2.4], item d)

Document / Requirement		Reference
Fallback to a minimal risk condition (see [8.5])		
• CBS security capabilities	Deterministic output	Ch 5, Sec 2, [4.1.2] and items No. 20 in Ch 5, Sec 2, Tab 1
• CBS documentation	- Description of security capabilities - Test procedure for security capabilities - Information supporting incident response and recovery plans	Ch 5, Sec 2, [3.1.4] Ch 5, Sec 2, [3.1.5] Ch 5, Sec 2, [3.1.9]
• Vessel design documentation	- Design description - Ship cyber resilience test procedure	[8.5.4], item a) [8.5.4], item c)
• Ship cyber security and resilience program	Incident response plans	[8.2.4], item d)
Recovery plan (see [9.2])		
• CBS security capabilities		
• CBS documentation	- Description of security capabilities - Test procedure for security capabilities - Information supporting incident response and recovery plans	Ch 5, Sec 2, [3.1.4] Ch 5, Sec 2, [3.1.5] Ch 5, Sec 2, [3.1.9]
• Vessel design documentation	- Design description - Ship cyber resilience test procedure	[9.2.4], item a) [9.2.4], item c)
• Ship cyber security and resilience program	Recovery plans	[9.2.4], item d)
Backup and restore capability (see [9.3])		
• CBS security capabilities	- System backup - System recovery and reconstitution	Ch 5, Sec 2, [4.1.2] and items No. 26 and 27 in Ch 5, Sec 2, Tab 1
• CBS documentation	- Description of security capabilities - Test procedure for security capabilities - Information supporting incident response and recovery plans	Ch 5, Sec 2, [3.1.4] Ch 5, Sec 2, [3.1.5] Ch 5, Sec 2, [3.1.9]
• Vessel design documentation	Ship cyber resilience test procedure	[9.3.4], item c)
• Ship cyber security and resilience program	Recovery plans	[9.2.4], item d)
Controlled shutdown, reset, restore and restart (see [9.4])		
• CBS security capabilities	System recovery and reconstitution	Ch 5, Sec 2, [4.1.2] and items No. 27 in Ch 5, Sec 2, Tab 1
• CBS documentation	- Description of security capabilities - Test procedure for security capabilities - Information supporting incident response and recovery plans	Ch 5, Sec 2, [3.1.4] Ch 5, Sec 2, [3.1.5] Ch 5, Sec 2, [3.1.9]
• Vessel design documentation	- Design description - Ship cyber resilience test procedure	[9.4.4], item a) [9.4.4], item c)
• Ship cyber security and resilience program	Recovery plans	[9.2.4], item d)
Risk assessment for exclusion of CBS from the application of requirements (see [11])		
• CBS security capabilities		
• CBS documentation		
• Vessel design documentation	Risk assessment for the exclusion of CBSs	[10.2.5]
• Ship cyber security and resilience program		

10.2 During design and construction phases

10.2.1 General

The supplier is to demonstrate compliance to the Society by following the certification process specified in Ch 5, Sec 2, [6].

The systems integrator is to demonstrate compliance by submitting documents in the following subsections to the Society for assessment.

During the design and construction phases, modifications to the design is to be carried out in accordance with the management of change (MoC) requirements in NR467, Pt C, Ch 3, Sec 3.

10.2.2 Zones and conduit diagram

The content of this document is specified in [10.2.2].

10.2.3 Cyber security design description (CSDD)

The content of this document is specified in subsections “Design phase” for each requirement in [4] to [9].

10.2.4 Vessel asset inventory

The content of this document is specified in [5.2].

10.2.5 Risk assessment for the exclusion of CBSs

The content of this document is specified in [11].

10.2.6 Description of compensating countermeasures

If any CBS in the scope of applicability of this Section has been approved with compensating countermeasures in lieu of a requirement in Ch 5, Sec 2, this document is to specify the respective CBS, the lacking security capability, as well as provide a detailed description of the compensating countermeasures. See also Ch 5, Sec 2, [3.1.4] requiring that the supplier describes such compensating countermeasures in the system documentation.

10.3 Upon ship commissioning

10.3.1 General

Before final commissioning of the ship, the systems integrator is to:

a) Submit updated design documentation to the Society (as-built versions of the documents in [10.2])

b) Submit Ship cyber resilience test procedure to the Society describing how to demonstrate compliance with this Section by testing and/or analytic evaluation.

c) Carry out testing, witnessed by the Society, in accordance with the approved Ship cyber resilience test procedure.

10.3.2 Ship cyber resilience test procedure

The content of this document is specified for the Commissioning phase in each subsection “Demonstration of compliance” in [4] to [9].

For each CBS, the required inherent security capabilities and configuration thereof are verified and tested in the certification process of each CBS (see Ch 5, Sec 2). Testing of such security functions may be omitted if specified in the respective subsection "Commissioning phase", on the condition that these security functions have been successfully tested during the certification of the CBS as per Ch 5, Sec 2. Nevertheless, all tests are be included in the Ship cyber resilience test procedure and the decision to omit tests will be taken by the Society. Tests may generally not be omitted if findings/comments are carried over from the certification process to the commissioning phase, if the respective requirements have been met by compensating countermeasures, or due to other reasons such as modifications of the CBS after the certification process.

The Ship cyber resilience test procedure is also to specify how to test any compensating countermeasures described in [10.2.3].

The Ship cyber resilience test procedure is to include means to update status and record findings during the testing, and specify the following information:

- Necessary test setup (i.e. to ensure the test can be repeated with the same expected result)
- Test equipment
- Initial condition(s)
- Test methodology, detailed test steps
- Expected results and acceptance criteria

Before submitting the Ship cyber resilience test procedure to the Society, the systems integrator is to verify that the information is updated and placed under change management; that it is aligned with the latest configurations of CBSs and networks connecting such systems together onboard the ship and to other CBSs not onboard (e.g., ashore); and that the tests documented are sufficiently detailed as to allow verification of the installation and operation of measures adopted for the fulfilment of relevant requirements on the final configuration of CBSs and networks onboard.

The systems integrator is to document verification tests or assessments of security controls and measures in the fully integrated ship, maintaining change management for configurations, and noting in the documented test results where safety conditions may be affected by specific circumstances or failures addressed in the Ship cyber resilience test procedure.

The testing is to be carried out on board in accordance with the approved Ship cyber resilience test procedure after other commissioning activities for the CBSs are completed. The Society may request execution of additional tests.

10.4 During the operational life of the ship

10.4.1 General

After the ship has been delivered to the Shipowner, the Shipowner is to manage technical and organisational security countermeasures by establishing and implementing processes as specified in this Section.

Modifications to the CBSs in scope of applicability of this Section is to be carried out in accordance with the management of change (MoC) requirements inNR467, Pt C, Ch 3, Sec 3. This includes keeping documentation of the CBSs up to date.

The Shipowner, with the support of suppliers, is to keep the Ship cyber resilience test procedure up to date and aligned with the CBSs onboard the ship and the networks connecting such systems to each other and to other CBSs not onboard (e.g. ashore). The Shipowner is to update the Ship cyber resilience test procedure considering the changes occurred on CBSs and networks onboard, possible emerging risks related to such changes, new threats, new vulnerabilities and other possible changes in the ship's operational environment.

The Shipowner is to prepare and implement operational procedures, provide periodic training and carry out drills for the onboard personnel and other concerned personnel ashore to familiarize them with the CBSs onboard the ship and the networks connecting such systems to each other and to other CBSs not onboard (e.g. ashore), and to properly manage the measures adopted for the fulfilment of requirements.

The Shipowner, with the support of supplier, is to keep the measures adopted for the fulfilment of requirements up to date, e.g. by periodic maintenance of hardware and software of CBSs onboard the ship and the networks connecting such systems.

The Shipowner is to retain onboard a copy of results of execution of tests and an updated Ship cyber resilience test procedure and make them available to the Society.

10.4.2 First annual survey

In due time before the first annual survey of the ship, the Shipowner is to submit to the Society a Ship cyber security and resilience program documenting management of cyber security and cyber resilience of the CBSs in the scope of applicability of this Section.

The Ship cyber security and resilience program is to include policies, procedures, plans and/or other information documenting the processes/activities specified in subsections "Demonstration of compliance" in [4] to [9].

After the Society has approved the Ship cyber security and resilience program, the Shipowner is to in the first annual survey demonstrate compliance by presenting records or other documented evidence of implementation ofthe processes described in the approved Ship cyber security and resilience program.

Change of vessel management company will require a new verification of the Ship cyber security and resilience program.

10.4.3 Subsequent annual surveys

In the subsequent annual surveys of the ship, the Shipowner is upon request by the Society to demonstrate implementation of the Ship cyber security and resilience program.

10.4.4 Special survey

Upon renewal of the ship's classification certificate, the Shipowner is to carry out testing witnessed by the Society in accordance with the Ship cyber resilience test procedure. Certain security safeguards are to be demonstrated at Special survey whereas other need only be carried out upon request by the Society based on modifications to the CBSs as specified in subsections "Operation phase" in [4]to [9].

11 Risk assessment for exclusion of CBS from the application of requirements

11.1 General

11.1.1 Requirements

A risk assessment is to be carried out in case any of the CBSs falling under the scope of applicability of this Section is excluded from the application of relevant requirements. The risk assessment is to provide evidence of the acceptable risk level associated to the excluded CBSs.

11.1.2 Rationale

Exclusion of a CBS falling under the scope of applicability of this Section from the application of relevant requirements needs to be duly justified and documented. Such exclusion can be accepted by the Society only if evidence is given that the risk level associated to the operation of the CBS is under an acceptable threshold by means of specific risk assessment.

The risk assessment is to be based on available knowledge bases and experience on similar designs, if any, considering the CBS category, connectivity grade and the functional requirements and specifications of the ship and of the CBS. Cyber threat information from internal and external sources may be used to gain a better understanding of the likelihood and impact of cybersecurity events.

11.1.3 Requirement details

Risk assessment is to be made and kept up to date by the system integrator during the design and building phase and considering possible variations of the original design and newly discovered threats and/or vulnerabilities not known from the beginning.

During the operational life of the ship, the Shipowner is to update the risk assessment considering the constant changes in the cyber scenario and new weaknesses identified in CBS onboard in a process of continuous improvement. Should new risks be identified, the Shipowner is to update existing, or implement new risk mitigation measures.

Should the changes in the cyber scenario be such as to elevate the risk level associated to the CBS under examination above the acceptable risk threshold, the Shipowner is to inform the Society and submit the updated risk assessment for evaluation.

The envisaged operational environments for the CBS under examination is to be analyzed in the risk assessment to discern the likelihood of cyber incidents and the impact they could have on the human safety, the safety of the vessel or the marine

environment, taking into account the category of the CBS. The attack surface is to be analyzed, taking into account the connectivity of the CBS, possible interfaces for portable devices, logical access restrictions, etc.

Emerging risks related to the specific configuration of the CBS under examination are to be also identified. In the risk assessment, the following elements are to be considered:

- Asset vulnerabilities
- Threats, both internal and external
- Potential impacts of cyber incidents affecting the asset on human safety, safety of the vessel and/or threat to the environment
- Possible effects related to integration of systems, or interfaces among systems, including systems not onboard (e.g. if remote access to onboard systems is provided).

11.1.4 Acceptance criteria

Exclusion of a CBS falling under the scope of applicability of this Section from the application of relevant requirements can be accepted by the Society only if assurance is given that the operation of the CBS has no impact on the safety of operations regarding cyber risk. The said exclusion may be accepted for a CBS which does not fully meet the additional criteria listed below but is provided with a rational explanation together with evidence and is found satisfactory by the Society. The Society may also require to submittal of additional documents to consider the said exclusion.

The following criteria are to be met to exclude a system from the scope of applicability of this Section:

a) The CBS is to be isolated (i.e, have no IP-network connections to other systems or networks)

b) The CBS is to have no accessible physical interface ports. Unused interfaces are to be logically disabled. It is not to be possible to connect unauthorised devices to the CBS

c) The CBS must be located in areas to which physical access is controlled

d) The CBS is not to be an integrated control system serving multiple ship functions as specified in the scope of applicability of this Section (see [1.3]

The following additional criteria should be considered for the evaluation of risk level acceptability:

a) The CBS should not serve ship functions of category III

b) Known vulnerabilities, threats, potential impacts deriving from a cyber incident affecting the CBS have been duly considered in the risk assessment

c) The attack surface for the CBS is minimized, having considered its complexity, connectivity, physical and logical access points, including wireless access points;

CHAPTER 4
ADDITIONAL CLASS NOTATION CYBER SECURE

Section 1 CYBER SECURE Notation

1 General

1.1 Application

1.1.1 CYBER SECURE notation

The additional class notation **CYBER SECURE** is assigned to ships complying with a set of requirements to secure the vessel by design, using security mechanisms incorporated in the equipment and networks:

- Equipment identification: As defined in Ship Rules, NR467, Pt C, Ch 3 Sec 3.
- Equipment criticality assessment: Systems criticality is assessed in order to focus the cyber security effort on the right place.
- Design Assessment: assessing the vulnerabilities of networks and systems whose design and plan have been approved regarding:
  - connections to on shore systems
  - networks
  - operational technologies interconnections.
- Monitoring procedures: Compliance procedures are used to anticipate and detect cyber incident by verifying the integrity of the critical equipment. The principle is to have a picture of standard equipment from its initial state, or last known as proper.
- Maintenance procedures: System nominal configuration addressing cyber risks that are to be mitigated by both updating the system and preventing unexpected effects during maintenance operations.
- Incident response procedures: In case of system failure, Shipowner and crew members have to ensure safety and, whenever possible, restore critical systems in a safe state.
- Cyber Risk Assessment: Cyber security is to be assessed for the ship by taking into account Shipowner risks and constraints.
- Cyber Security Policy (for existing ship only): A policy (or management plan) is to define cyber security governance and organization for a Shipowner's fleet (roles, responsibilities, rules).

Assignment of the additional class notation **CYBER SECURE** is subject to compliance with the requirements of this Chapter.

The additional class notation **CYBER SECURE** is completed by a construction marks as defined in Ch 1, Sec 1, [1.2.4].

1.1.2 Approval

The additional class notation **CYBER SECURE** is assigned to a ship in order to reflect the fact that:

- its design complies with cyber security rules on interconnections with on shore systems and aboard systems
- procedures, including monitoring, maintenance and incident response, are delivered with the vessel to ensure the level of cyber security during the vessel lifetime.

- equipment is identified, inventoried, categorized in accordance with Ch 1, Sec 2
- criticality, incident impact and cyber attack likelihood of equipment are assessed in accordance with Ch 1, Sec 3
- on board to on shore connections, ship networks and operational technologies interconnections are designed in accordance with Sec 2, Sec 3 and Sec 4.
- design assessment is performed in accordance with Ch 1, Sec 4
- vital functions, treatment opportunity and risk mitigation are assessed in accordance with Ch 1, Sec 5
- monitoring, maintenance and incident response procedures are delivered in accordance with Ch 1, Sec 6
- For existing ships only: Cyber Security Policy (or management plan) is delivered in accordance with Ch 2, Sec 2.

1.1.3 Construction mark

In compliance with the requirements NR467, Pt A, Ch 2, Sec 1, [2], the additional class notation **CYBER SECURE** is completed by a construction mark as defined in Ch 1, Sec 1, [1.2.4].

For granting "maltese cross" construction mark, the following equipment and system installed onboard the ship are to be recognized by the Society:

- for network protection (see Ch 3, Sec 3): solutions for trafic encryption, firewall and or new generation firewall (NGFW), intrusion and prevention system (IPS)
- for operational technology interconnection protection (see Ch 3, Sec 4): diode network equipment
- in addition, when applicable:
  - Events and logs recorder (ELR) security solutions and in particular ELR workflow, ELR architecture and file formats uses for record event (see Ch 5, Sec 2 and Ch 5, Sec 4)
  - Compliance and Software Registry (CSR) solutions (see Ch 5, Sec 4)
  - Inspection and Decontamination Gate (IDG) solutions (see Ch 5, Sec 4).

1.1.4 Initial survey

Assignment of the additional class notation **CYBER SECURE** is subject to an initial survey by the Society as detailed in Ch 6, Sec 1, [1.1.2].

1.1.5 Maintenance of the notation

In compliance with the requirement of NR467, Pt A, Ch 2, Sec 2 and NR467, Pt A, Ch 5, Sec 17, the maintenance of the additional class notation **CYBER SECURE** is subject to periodical surveys as detailed in Ch 6, Sec 1, [2] to Ch 6, Sec 1, [4], as applicable.

2 Documents to be submitted

2.1 Methodology

2.1.1 Workflow

The delivery workflow is to follow the here below order:

a) "Basic", "Intermediate" and "Detailed" Cyber Inventory are to be built by following Ch 1, Sec 2

b) Cybersecurity by design is to meet requirements described in Sec 2, Sec 3 and Sec 4

c) Criticality assessment is to be built by following Ch 1, Sec 3

d) Design assessment is to be built by following Ch 1, Sec 4.

2.2 Documentation

2.2.1 The documentation listed in Tab 1 is to be submitted for approval.

Table 1 : Documentation to be submitted for notation CYBER SECURE

Document	Reference
Cyber Inventory:	
• Basic Inventory	• Ch 1, Sec 2, Tab 1
• Intermediate Inventory	• Ch 1, Sec 2, Tab 2
• Detailed Inventory	• Ch 1, Sec 2, Tab 3
Criticality Assessment	• Ch 1, Sec 3
Design assessment	• Ch 1, Sec 4
completed by:	
• Plan approval of on board to on shore connections design	• Sec 2, Tab 1
• Plan approval of vessel networks design	• Sec 3, Tab 1
• Plan approval of operational technologies connections design	• Sec 4, Tab 1
Cyber Risk Assessment (for existing ship only)	• Ch 1, Sec 5
Cyber Handbook:	
• Monitoring, maintenance and incident response procedures	• Ch 1, Sec 6
Cyber Security Policy (for existing ships only):	
• Policies	• Ch 2, Sec 2, Tab 1

Section 2 On Board to On Shore Connections

1 General

1.1 Objective

1.1.1 Any system connected from on board to on shore is to be designed in accordance with the rules defines in this Section.

2 Documentation

2.1 Plan approval

2.1.1 Aboard systems connected to on shore are to be described, designed, configured and connected in accordance with the rules defined in this Section.

Topics listed in Tab 1 are to be submitted by the Shipyard for approval by the Society.

Table 1 : On board to on shore connections plan approval

Topic	Rules	Document
Remote access		
Functionalities	[3.1.1]	Every remote access usages are to be detailed in accordance with the rule, explained and justified with a full description.
Public networks	[3.1.2]	When used, public networks connections are to be detailed.
Private networks	[3.1.3]	When used, private networks connections are to be detailed.
Design		
Ashore installations	[4.1.1]	Ashore cartography, security strategy, security equipment, security events management are to be detailed.
Demilitarized Zones		
Architecture	[5.1.1]	The DMZ architecture is to be detailed, explained and justified.
External connections	[5.1.2]	External connections are to be detailed and justified with a network implementation map with description of flows and protocols.
Traffic		
Encryption	[6.1.1]	Traffic encryption mechanisms are to be submitted.
Firewall	[6.1.2]	Firewalls models, strategy, security mechanism implementation and rules (authorized sources and destinations) are to be delivered.
Application firewall	[6.1.3]	Application firewalls models, strategy, security mechanism implementation and rules (Authorized sources and destinations) are to be delivered.
New generation firewall	[6.1.4]	New generation firewalls models, strategy, security mechanism implementation and rules (Authorized sources and destinations) are to be delivered.
Intrusion prevention system	[6.1.5]	Intrusion prevention systems models, strategy, security mechanism implementation and rules (Authorized sources and destinations) are to be delivered.
Remote access		
Management	[7.1.1]	Management security mechanisms of DMZ are to be detailed, explained.
Patch management	[7.1.2]	Patch management is to be detailed.
Audits	[7.1.3]	Auditing is to be detailed.

3 Remote access

3.1

3.1.1 Functionalities

Remote access covers any access to the ship IT or OT from remote point like remote operation centre or manufacturer equipment management and supervision or ship to ship. A basic premise of the remote access point is that its security is not satisfactory.

Three types of remote connections are to be considered:

- Telemetry mode gets or retrieves information by sending orders without any capacity to modify or to operate ship
- Operation mode operates any function of any equipment or modifies operational configuration of the equipment
- Management mode gives full access to any equipment with potentially high privileges or administrative rights.

3.1.2 Public networks

Public networks are opened to anyone with few or no restriction.

Connection to public networks like internet is source of threats and risks. The needs of traffic through public network are to be defined and justified. The implementation of the limitation of public network traffic is to be explained and strictly limited to the needs herein before defined.

When remote access to an equipment is achieved through public network, the following applies:

- Telemetry mode is tolerated for Level 2 and Level 3 equipment when managed through a DMZ. Telemetry mode is authorized for Level 1 equipment
- Operation mode for Level 3 equipment is to be submitted for approval with motivated exception and mitigation measures (Security Measures). DMZ is mandatory for Level 2 and Level 3 equipment. Operation mode is authorized for Level 1
- Management mode for Level 2 and Level 3 equipment is banned without dedicated security solution embedding protocol disruption (e.g. Virtual Machines). Management mode is authorized for Level 1.

For Level 2 and level 3 Systems, accesses from a public network to the ship are to be managed through a Demilitarized Zone (DMZ).

3.1.3 Private networks

Private networks only accept connections from trusted devices. Users out of a private network cannot use physical access points and routers. Private networks are physical, secured environment. Because they are virtual, VPN are, in this case, no to be considered as private networks.

When remote access to an equipment is achieved through private network, the following applies:

- Telemetry mode is authorized for Level 3 equipment when managed through a DMZ. Telemetry mode is authorized for Level 2 and Level 1 equipment without restriction
- Operation mode is authorized for Level 2 and Level 3 equipment when managed through a DMZ
- Management mode is authorized for Level 2 and Level 3 equipment through a dedicated network (e.g. VLAN) managed through a DMZ
- There is no restriction for Level 1 except the traffic encryption.

4 On shore

4.1 Design

4.1.1 Ashore installations

As ashore premises could be a strong vector of attack, they are considered, in term of security, as an untrusted area.

For connections from ashore to on board, ashore network shall be considered as a fully separated network with a need of filtering.

5 Demilitarized Zones

5.1

5.1.1 Architecture

Equipment in DMZ has a limited connectivity to the ship's equipment. (See Fig 2).

The two basic rules are the following:

- the “ship” Network pushes information to the “DMZ” Network.
- the “ground” pulls information from the “DMZ” or the “DMZ” pushes information to the “shore”.

Authorized points of internal connections (inside “DMZ” and outside “ship”) are to be declared. Usage of each point of connection is to be linked to a function described in [3.1.1] and justified.

Authorized points of external connections (inside “DMZ” and outside “Ground”) are to be declared. Usage of each point of connection is to be linked to a function described in [3.1.1] and justified.

The needs of traffic through DMZ are to be defined. The implementation of the limitation of DMZ traffic is to be explained and strictly limited to the needs hereinbefore defined.

Protocols and ports number are to be detailed. Standard port numbers are not to be used. Protocols are to be justified.

DMZ network cables, network equipment and security equipment when used are to be isolated from the ship network. The two networks are to be physically independent.

Note 1: For suppliers' case: A single system may also have its own DMZ integrated by the system's Supplier, offering a tailored level of protection. In such a situation, the Supplier is responsible of its own security and submits elements described in Fig 3.

Note 2: For ashore case: At the opposite, in term of architecture, the DMZ mechanism may be installed ashore. In this case, the DMZ filters the whole fleet flows. The onshore DMZ uses a private link only for ashore connection. See Fig 4.

Figure 1 : DMZ management example

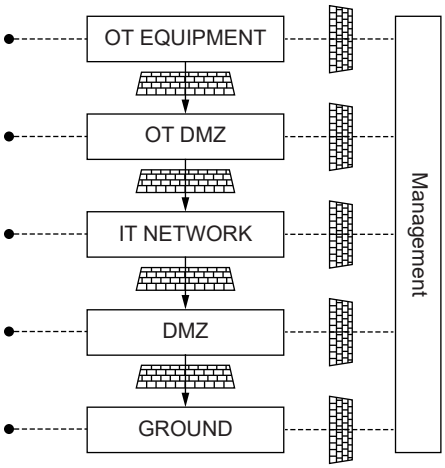


Figure 2 : DMZ example

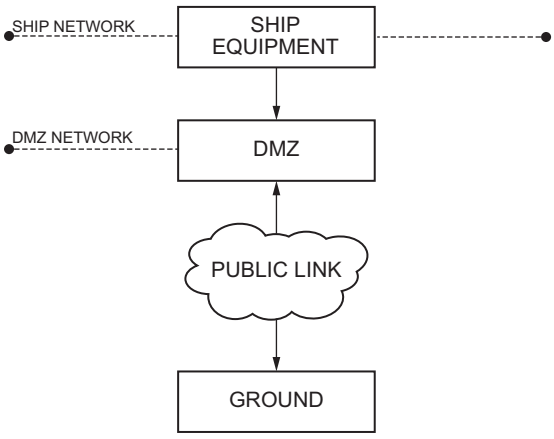


Figure 3 : Supplier example

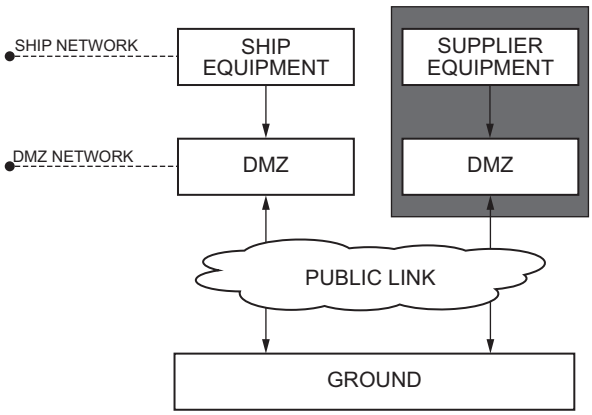
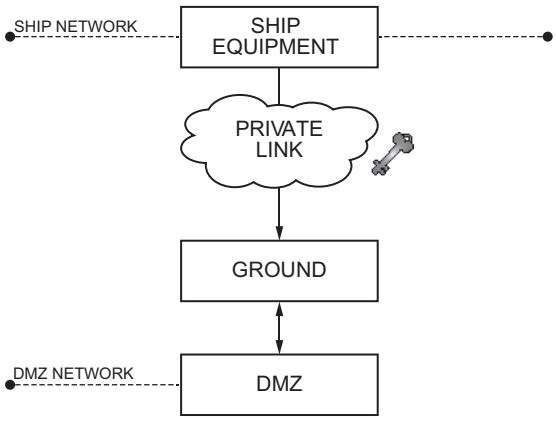


Figure 4 : Ground DMZ example



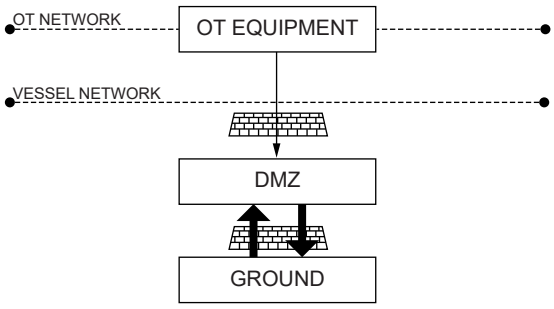
5.1.2 External connections

External connections include (See Fig 5):

- connections going from the “Ground” to the “DMZ”
- connections going from the “DMZ” to the “Ground”.

TCP connections are allowed.

Figure 5 : Example of external traffic



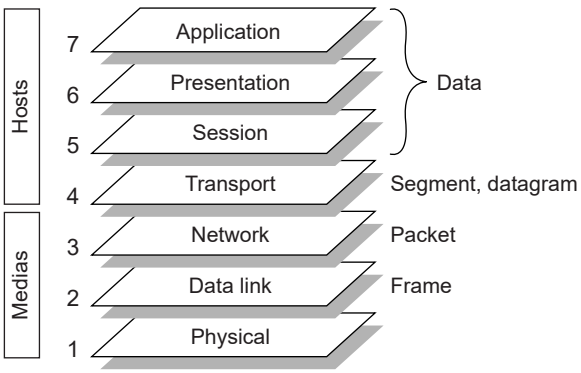
6 Traffic

6.1 Security

6.1.1 Encryption

Encryption is mandatory for external connections. OSI Layer 4 (e.g. TLS) is used on networks. OSI Layer 3 (e.g. IPsec) is to be implemented, when feasible, for connections going through public networks. (See Fig 6).

Figure 6 : OSI layers



6.1.2 Firewall filtering

For remote access security, two firewalls from two different manufacturers are to be used on the ship.

6.1.3 Application firewall

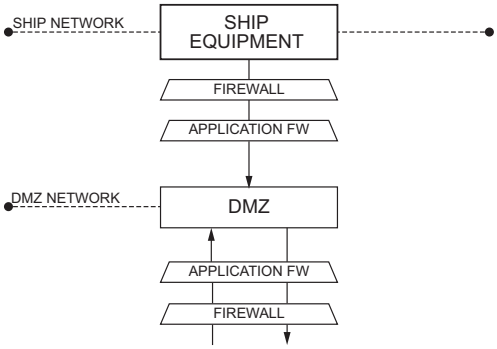
Application firewalls may be used to filter IP Layer 2 through 7 packets. Application protocols may be forged in order to gain privileges or disrupt the availability of the system. Application firewalls are to be used:

- between DMZ and outside “Ground”
- between DMZ and inside “Ship”.

The application firewall blocks detected intrusions and malformed communications.

For example: packets sent to traditional port 80 are checked by the application firewall to remove any traffic except HTTP. Moreover, in order to remove tunnels, data field are also to be checked regarding predefined compliancy of the system. (See Fig 7).

Figure 7 : Example of dual application FW

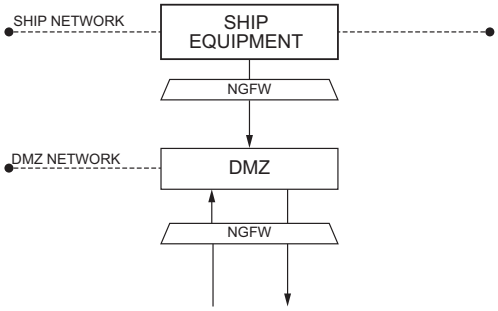


6.1.4 New generation firewall filtering

New generation firewall (NGFW) should be preferred to old-generation Firewalls. (See Fig 8).

NGFW already contain Application Firewall and Identity Awareness.

Figure 8 : Example of NGFW



6.1.5 Intrusion prevention system

Intrusion prevention system (IPS) are used to detect attacks based on a number of different techniques like the use of threat signatures, known exploit attacks, anomalous activity and traffic behaviour analysis.

If detected, suspected packets are dropped.

7 Remote maintenance

7.1

7.1.1 Management

Management mode to:

- DMZ servers (ashore)
- remote access systems and DMZ security equipment (onboard and ashore)
- remotely accessed equipment (onboard).

is to be done from a dedicated network (i.e VLAN).

7.1.2 Patch management

The Shipowner is to be informed on the latest vulnerabilities (CVE) and get updates.

7.1.3 Audits

Equipment, network equipment and security equipment involved in remote maintenance are to automatically record connection, authentication and security events.

Section 3 Ship Networks

1 General

1.1 Objective

1.1.1 Any aboard network is to be designed in accordance with the rules defines in this Section.

2 Documentation

2.1 Plan approval

2.1.1 Networks are to be described, designed, configured and connected in accordance with the rules defined in this Section. Topics listed in Tab 1 are to be submitted by the Shipyard for approval by the Society.

Table 1 : Networks plan approval

Topic	Rules	Document
Network access		
Physical access		
Access	[3.1.1]	Physical protection of Level 3 network equipment is to be detailed.
Cabling	[3.1.2]	Protected cable passageways implementation and cable types are to be detailed.
Identification	[3.1.3]	Network visual identification strategy is to be detailed.
Logical access		
Partitioning	[3.2.1]	Physical and logical partitioning of networks are to be detailed.
Functional cohabitation	[3.2.2]	Rules on functional cohabitation are to be detailed.
Device authentication mechanism	[3.2.3]	Device authentication policy is to be detailed.
Interconnections		
Level 2 to Level 1 interconnections	[3.3.1]	Each interconnection between Level 2 and Level 1 system is to be detailed, explained and justified.
Level 3 to Level 2 interconnections	[3.3.2]	Each interconnection between Level 3 and Level 2 system is to be detailed, explained and justified.
OT connectivity	[3.3.3]	OT network interconnection with other vessel networks is to be detailed, explained and justified.
Wireless networks		
Architecture	[3.4.1]	Wifi networks, strategy, security mechanism implementation and rules are to be delivered.
Wireless Local Area Network	[3.4.2]	WLAN policy is to be delivered.
New generation firewall	[3.4.3]	NG firewalls dedicated to wireless networks are to be listed.
Intrusion prevention system	[3.4.4]	IPS dedicated to wireless networks are to be listed.
Network protection		
Data protection		
Traffic encryption	[4.1.1]	Traffic encryption mechanisms are to be detailed.
IPSec usage	[4.1.2]	IPSec implementation strategy is to be detailed.
Network switch		
Switches security policy	[4.2.2]	Switches policies and configuration and spanning tree usages are to be detailed and justified.
Non-IP traffic	[4.2.1]	Non-IP traffic is to be identified, managed and described.

Topic	Rules	Document
Firewall		
Implementation	[4.3.1]	Firewalls models, strategy, security mechanism implementation and rules (authorized sources and destinations) are to be delivered.
New generation firewall		
Usage	[4.4.1]	New generation firewalls models, strategy, security mechanism implementation and rules (authorized sources and destinations) are to be delivered.
Application firewall	[4.4.2]	Application firewall implementation and rules (Authorized sources and destinations) is to be delivered.
Identity management	[4.4.3]	Identity filtering and authentication mechanisms are to be submitted.
Stateful packet inspection	[4.4.4]	SPI implementation is to be submitted.
Intrusion prevention system		
Usage	[4.5.1]	Intrusion prevention systems models, strategy, security mechanism implementation and rules (Authorized sources and destinations) are to be delivered.
Security events	[4.5.2]	Security events usage and strategy is to be detailed.
Thresholds	[4.5.3]	Events thresholds and false positive identification is to be submitted.

3 Network Access

3.1 Physical access

3.1.1 Access

Access to Level 3 network and equipment is not accepted out of unsecured area. Access control is mandatory.

3.1.2 Cabling

Network integrity of Level 3 systems is reinforced by using closed cable passageway in unsafe areas.

All network cables for category I, II, III systems (as defined in Ship Rules NR467, Pt C, Ch 3, Sec 3, Tab 1 are to be flame retardant and are to be designed, manufactured and tested as per relevant national or international standards. Cables are to be fire resistant type where required by the Society.

The minimum bending radius specified for the cable is to not to be exceeded, especially for optical cables where it may lead to signal loss.

3.1.3 Identification

For Level 3 systems, network are to be visually identifiable from any point by using, for example, coloured cables. Network plugs are to be clearly and physically identified.

3.2 Logical access

3.2.1 Partitioning

As much as possible, each functional network is to be physically separated with dedicated network equipment. This point contributes to the reliability of the ship. If it is not possible, and demonstrated as being, VLAN are to be considered as defined in those rules.

Each segment is to have its own range of Internet Protocol (IP) address.

Standard interfaces should be used for data exchange between different networks. Each network should be designed in compliance with a recognized standard such as IEC Standards - IEC 61158 or IEC 61784, etc.

Segmentation should be such as to prevent loss of essential systems upon a single failure for Level 3 systems, which required redundancy by classification Society.

3.2.2 Functional cohabitation

For IP and non-IP traffic of two distinctive functional areas which are physically connected (which is not encouraged), a logical partition (e.g. VLAN) is to be used for Level 3 equipment.

For example, a VLAN could be considered for each of the following functional areas: servers, operators, administration, remote connection and industrial controllers.

3.2.3 Device authentication mechanism

Level 2 and Level 3 networks connectivity is to rely on an authentication mechanisms involving three parties: the supplicant, the authenticator and the authentication server.

The implementation is to be:

- port-based level access control (IEEE 802.1x)
- any other standard to submit for approval to the Society.

3.3 Interconnections

3.3.1 Level 2 to Level 1

Connections from Level 2 to Level 1 networks are to be avoided as much as possible. This applies to IT and OT networks.

When needed, connections should be achieved through a unidirectional link only, if feasible. The unidirectional link uses an anti-subversion mechanism as security wrapper or diode. It does not use direct connection (ssh, ftp) even if they are secured or enciphered.

3.3.2 Level 3 to Level 2

For connections from Level 3 equipment to Level 2 equipment:

- connections shall be established by using a gateway (see DMZ) in charge of receiving orders from the outside and transferring them to the inside part
- operating systems of gateways are to be hardened as any equipment
- inside the gateway, two separated operating systems with two separated network interface ensure the gateway process through a shared area limited to data exchange (pipes, semaphores, file system...)
- usage of a firewall is required.

3.3.3 OT Connectivity

For Level 2 and Level 3 systems, OT networks are not to be accessible from any part of the ship, except the relevant ones. No network plug are to be installed out of this limited scope. Network cables are not to be directly accessible from the outside.

3.4 Wireless networks

3.4.1 Architecture

The needs of traffic through wireless network are to be defined and justified. The implementation of the limitation of wireless network traffic is to be explained and strictly limited to the needs as defined in Fig 1.

As for cable networks, wireless networks are segregated to the same Level of criticality (e.g. Level 1 to Level 1 is authorized, Level 1 to Level 2 in prohibited). (See Fig 2).

Wireless networks are segregated to the same kind of network (e.g. OT to OT is authorized, OT to IT is prohibited). (See Fig 3).

Wireless usage for management of systems is prohibited.

The usage of wireless networks for Level 3 is to be detailed (endpoints inventory, ports and TCP layers analysis), explained and justified. Security mechanisms are to be detailed (e.g. hidden network, monitoring).

Wireless networks for Level 3 is authorized only if communication:

- is established, and reserved, for the system itself (no interconnection)
- is not used for critical operation (it means that if the wireless network is turned off, there is no issue on operation)
- is not an entry point to critical function (as a rebound point if an attacker takes control of the network).

Figure 1 : Authorized WIFI architecture

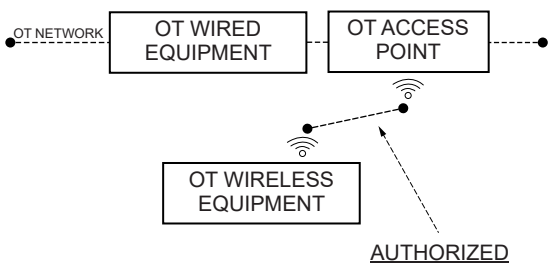


Figure 2 : Prohibited network connection

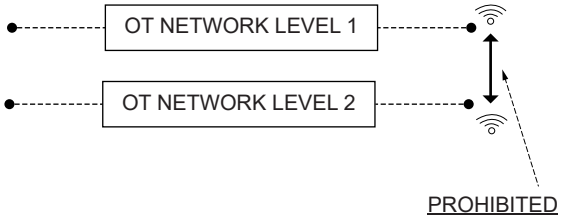
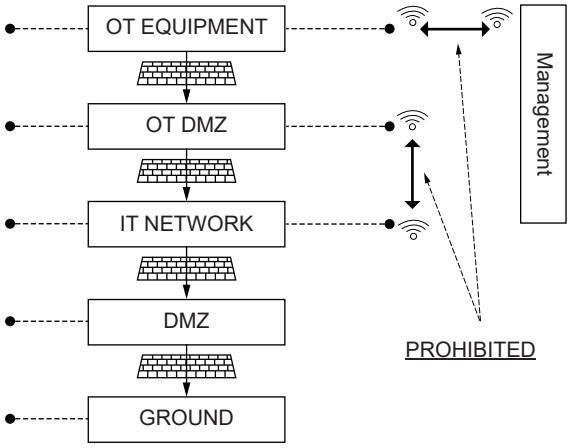


Figure 3 : Prohibited WIFI architecture



3.4.2 Wireless Local Area Network (WLAN)

Wireless Local Area Network (WLAN) is a flexible data communications system that can use either infrared or radio frequency technology to transmit and receive information over the air. (See Fig 4).

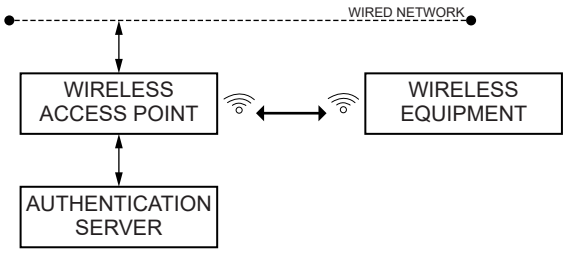
WLAN is to be secure and respond to a WLAN security policy managed by the Wireless Access Point (WAP).

The following is a sample list of basic requirements which have to be, at a minimum, implemented in the WLAN security policy:

- SSID (Service Set Identifier IEEE 802.11b) is not broadcast for Level 2 or Level 3 networks. Operational or industrial wireless networks are never broadcast.
- Radio broadcast levels must be reduced and adjusted at the least need.
- Authentication relies on Wi-Fi Protected Access 3 Enterprise (WPA3-Enterprise). It imposes a per-user authentication through RADIUS and it far more secure than WPA2 passphrase. The WPA3-Enterprise security type uses IEEE 802.1x for the authentication exchange with the backend. The Advanced Encryption Standard (AES) cipher type is used for encryption. WPA3-Enterprise is mandatory from Level 2. Protocol WPA2 with passphrase is authorized for Level 1 only.
- Certificates are managed by using an authentication method compatible with the Extensible Authentication Protocol (EAP) framework. In example: Transport Level Security (EAP-TLS) or Tunnelled Transport Level Security (EAP-TTLS). EAP-MD5, EAP-LEAP are prohibited from Level 2.
- From Level 2, wireless networks are dedicated to a system and cannot be shared.

WLAN is to be introduced from Level 2 wireless networks.

Figure 4 : WLAN architecture example



3.4.3 New Generation Firewall (NFGW)

Access point of the wireless network is installed behind a New Generation Firewall (NGFW), see Fig 5.

The application firewall is used to filter IP Layer 2 through 7.

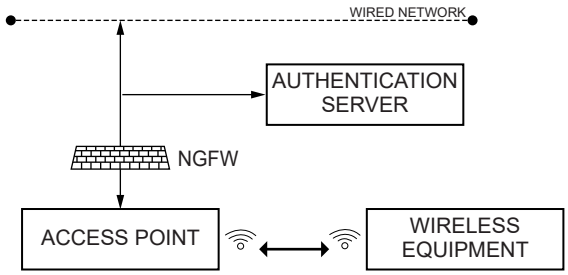
The State-full Packet Inspection (SPI) is used to detect suspicious behaviours.

When available in the NG firewall, Intrusion Prevention System (IPS) is to be configured to detect and drop suspected packets.

3.4.4 Intrusion Prevention System (IPS)

For Level 3 systems using wireless networks, the Wireless Intrusion Prevention System (WIPS) is mandatory. The WIPS detects rogue access points, unauthorized accesses, MAC address spoofing, denial of service attacks or any man in the middle scenarios.

Figure 5 : Wi-Fi and firewall example



4 Network protection

4.1 Data protection

4.1.1 Traffic encryption

At data level, for each protocol used for external connection, key authentication is mandatory instead of password authentication. Key management is to be submitted.

Note 1: Traffic encryption may use solutions recognized by the Society (see Sec 1, [1.1.3])

4.1.2 IPsec usage

When used over public networks, IPsec encryption complies with the following implementation:

- Encapsulation Security Payload (ESP) is used in conformance with RFC 4303 (protocol 50)
- Integrity mechanism are activated
- IPsec is used as a full tunnel mode - transport mode is banned
- Internet Key Exchange (IKE) complies with Version 2 RFC 5996
- Pre-Shared keys (PSK) are deactivated. PKI is (Public Key Infrastructure) is used
- Infrastructure firewalls only accept IKE, ESP and eventually ICMP
- When Network Address Translation (NAT) is used over infrastructure, NAT-Traversal (NAT-T) is activated
- Keys are changed regularly (either by using Perfect Forward Secrecy PFS, either by requesting change every hour)
- When used: MD5 hash, DES encryption and RSA keys are 2048 bits length minimum
- When used: AES, SHA-2 and ECDSA keys are 256 bits length minimum
- Hereinbefore rules are implemented in the “Security Policy Database” of IPsec configuration
- Diffie-Hellman keys algorithms groups 1 and 2 are banned. Groups 14, 15, 19 or 29 are preferred.

4.2 Network switch

4.2.1 Non-IP traffic filtering

For Level 3 equipment, for non-IP traffic between two distinctive areas, the firewall shall filter packets by using source and address identification. For Ethernet non-IP traffic, MAC addresses will be used in respect of the network address plan.

4.2.2 Switches security policy

For Level 2 and Level 3 equipment, the Spanning Tree Protocol is to be applied to network switches to prevent network storms and network becoming paralyzed.

Safety functions implemented in the integrated network are be to implemented in dedicated and autonomous hardware units (switches, etc.)

4.3 Firewall

4.3.1 Implementation

Firewalls are used to filter OSI Layer 2 through 4 packets. (See Fig 6).

OSI Layer 2 is to be filtered by using data link information like MAC address.

OSI Layer 3 is to be controlled by using network information like IP address.

The needs of traffic through Firewall are to be defined. Authorized sources (MAC and IP addresses), protocols and port numbers are to be mastered and filtered by the firewall.

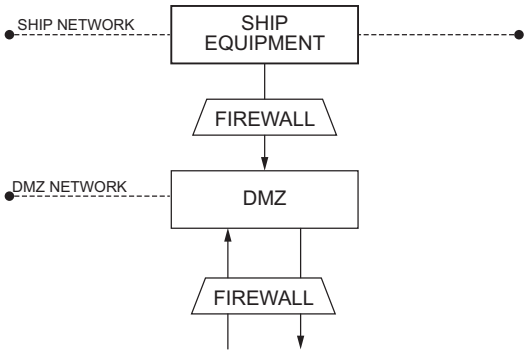
The implementation of the limitation of Firewall traffic is to be explained and strictly limited to the needs hereinbefore defined.

To ensure the control of the security, the traffic is to be blocked by default. This is generally achieved by configuring the last rule of the access line to deny all packets.

Safety policy (rules) are to be implemented. The Safety policy (rules) are to be designed to allow passage of data traffic that is essential for the intended operation of that network.

Note 1: Firewall may have to be recognized by the Society (see Sec 1, [1.1.3]).

Figure 6 : Firewall example



4.4 New-generation firewall

4.4.1 Usage

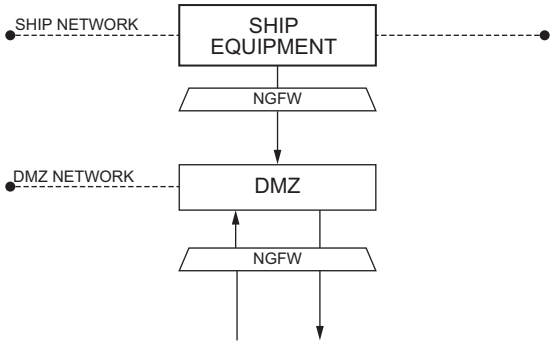
For Level 2 and Level 3 systems, New Generation Firewall (NGFW) are systematically preferred to old-generation Firewalls, see Fig 7.

The following NGFW security functions are turned on:

- firewall
- application firewall
- identity awareness
- state-full packet inspection
- intrusion prevention system.

Note 1: All the NGFW above functions may have to be recognized by the Society (see Sec 1, [1.1.3]).

Figure 7 : New generation firewall



4.4.2 Application firewall

In NGFW, application firewall is to be configured to filter IP Layer 2 through 7 packets.

When needed, the application firewall is also used to offload encryption from servers and manage authentication.

4.4.3 Identity management

For communication from/to Level 3 systems, application firewalls functions from NGFW are used to verify the identity of remote connections and to apply dedicated a policy regarding authorized services, routing tables and TCP ports usage.

For example: Remote monitoring systems requesting highly privileges may be authorized through the firewall but blocked by the application firewall, see Fig 8.

4.4.4 Stateful packet inspection

NGFW contains Stateful Packet Inspection (SPI) technology.

For Level 3 Systems, SPI is to be used to check the consistency of the transaction regarding the historic data.

For example: Packets not assigned to an existing connection are dropped, thereby limiting the risk of hacking (intelligence and discover operations).

NGFW use dynamic tables to store those data and define a state of the connection.

4.5 Intrusion and prevention system (IPS)

4.5.1 Usage

Intrusion prevention systems (IPS) raise up odds of detection and blocking malicious behaviour on networks.

For Level 2 and Level 3 systems, IPS are to be used to detect attacks based on a number of different techniques like the use of threat signatures, known exploit attacks, anomalous activity and traffic behaviour analysis: if detected, suspected packets are dropped.

As they are actives probes, they are helpful in order to block attacks or parts of them. IPS are to be installed in accordance to network architecture and network levels of criticality. IPS systems scope of installation includes virtual networks handled by hypervisors.

Instead of an active behaviour, probes may be configured in a passive mode called intrusion detection system (IDS.) In that case, packets are not blocked anymore.

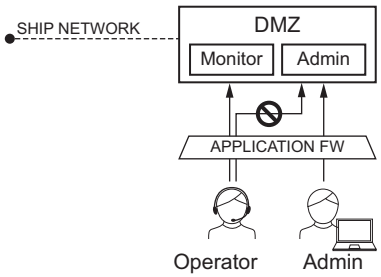
As they could block operational packets, IPS are to be banned for critical and real-time environment. IDS are to be used if feasible.

IPS usage is mandatory for connected Level 3 equipment.

IPS may be integrated in a NGFW or installed ashore in case of ashore connection.

Note 1: Intrusion and prevention systems may have to be recognized by the Society (see Sec 1, [1.1.3]).

Figure 8 : Example of identity verification



4.5.2 Security events

Security events issued by IPS (BLOCKED and ALERTS) are to be recorded and made available.

IPS are to be used to record network activity: origin, destination, timestamps.

Security events referential including code number, diagnostic description and resolution methodology is to be delivered. Scope includes IPS themselves and any security relative events detected by IPS about network behaviour. Unknown MAC or IP address detected on supervised network shall trigger a security event. Missing MAC or IP address on supervised network shall trigger a security event.

4.5.3 Thresholds

For IPS, the number of authorized login failures before alert generation is to be defined. Alert means ELR message and remote access blocking for the incriminated source.

Ship integrator delivers IPS with a dedicated tuning about rules management. This tuning takes into account network cartography, traffic and compliance both in physical and logical. configuration / segmentation.

IPS messages are to be cleaned from irrelevant noise.

The thresholds policy is to be explained in order to be operated.

Section 4 Operational Technologies Interconnections

1 General

1.1 Objective

1.1.1 Operational Technologies are to be interconnected in accordance with the rules defined in this Section.

2 Documentation

2.1 Plan approval

2.1.1 When interconnected to other systems, Operational Technologies interconnections are to be described, designed, configured and connected in accordance with the rules defined in this Section.

Topics listed in Tab 1 are to be submitted by the Shipyard for approval by the Society.

3 OT to IT Interconnections

3.1 Partitioning

3.1.1 Industrial control system (ICS) networks

For Level 2 and Level 3 Systems, Industrial Control Systems (ICS) are to be separated into consistent technical and/or functional areas. Those areas are segregated.

Distributed ICS, or interconnected ICS, (wide supervision of industrial controllers for example) are to use approved IPSEC VPN implementation. Distributed ICS are identifiable by the fact that they are not physically in the same area.

3.1.2 Programmable Logic Controllers (PLC) Segregation

Programmable Logic Controllers (PLC) using dual Ethernet interfaces are not considered as a security component and segregation shall not be trusted.

Table 1 : Operational technologies plan approval

Topic	Rules	Document
Partitioning		
ICS networks	[3.1.1]	When used, distributed ICS architectures are to be detailed.
PLC segregation	[3.1.2]	When used, PLC dual Ethernet interfaces are to be detailed.
Software limitation	[3.1.3]	When connected, OT equipment software is to be limited to a minimum which is to be submitted.
Interconnections		
Usage	[3.2.1]	Interconnected OT systems are to be justified and submitted for approval
ICS DMZ	[3.2.2]	OT connections to vessel network and/or ground systems are to be submitted
DMZ interconnection	[3.2.3]	DMZ interconnections are to be detailed, justified and submitted for approval with a full rationale on interconnection implementation.
Ingoing packets	[3.2.4]	DMZ ingoing packets are to be detailed, justified and submitted for approval with a full rationale on authorized flows.
Outgoing connections	[3.2.5]	Outgoing connections are to be detailed, justified and submitted for approval with a full rationale on authorized flows.
Diodes	[3.2.6]	Diode usage is to be detailed.
Management	[3.2.7]	Management security mechanisms of DMZ are to be detailed
Call-back	[3.2.8]	When used call-back mechanisms are to be detailed.
Physical access	[3.2.9]	When used physical controls are to be detailed.
Logical alerts	[3.2.10]	When used, logical alerts are to be detailed.

3.1.3 Software limitation

The needs of software and tools are to be defined and justified. The installation of software and tools is to be explained and strictly limited to the needs hereinbefore defined.

Unneeded IT tools installed in OT are to be moved to IT network.

Unneeded Level 1 and Level 2 tools installed in a Level 3 Equipment are to be moved to Level 2 Equipment.

Unneeded Level 1 tools installed in Level 2 Equipment are to be moved to Level 1 Equipment.

3.2 Interconnections

3.2.1 Usage

Network interconnections represent threats as they are sources of vulnerabilities. Risk must be considered before connecting networks and equipment. IT and OT systems are traditionally not connected but the situation is changing as ICS, for example, is managed remotely.

As a general principal, the interconnection is to be limited to meeting the needs to strike the appropriate balance between isolation and connection.

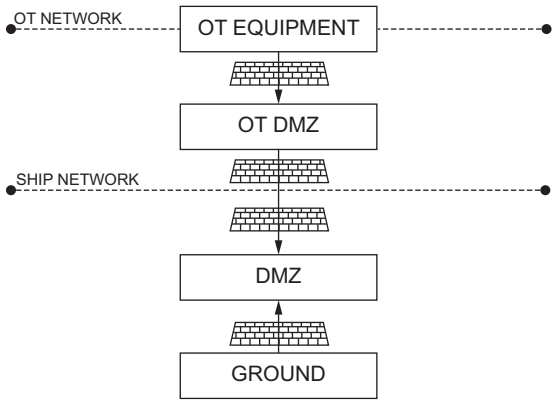
When an OT system is connected, the equipment ensuring the needed function is to be dedicated.

3.2.2 ICE DMZ

OT systems are not to be directly connected to the delimitarized zone (DMZ). An internal DMZ, named “OT DMZ”, is dedicated to communication from “OT Network” to the ground. The Rules developed in [3.2], including related documents to be submitted, fully apply to the “OT DMZ”. (See Fig 1).

OT DMZ are mandatory for Level 3.

Figure 1 : OT DMZ principle

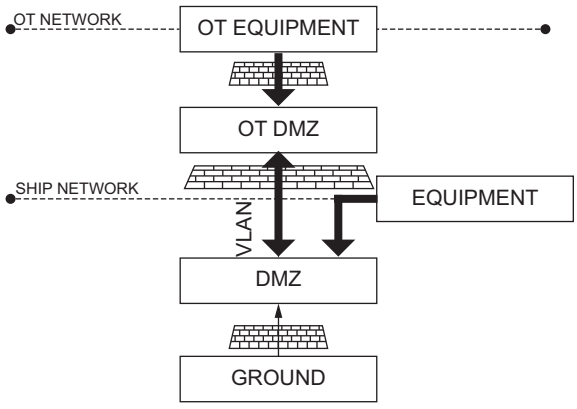


3.2.3 DMZ interconnections

To defeat the risk of hacked delimitarized zone (DMZ), the DMZ has no way to connect to the vessel Network. However, notice that, the “OT DMZ” needs to connect to “DMZ” through the vessel Network (see Fig 2). In this case, connections are authorized through a dedicated VLAN.

TCP (Transmission Control Protocol) connections and UDP (User Datagram Protocol) datagrams are allowed.

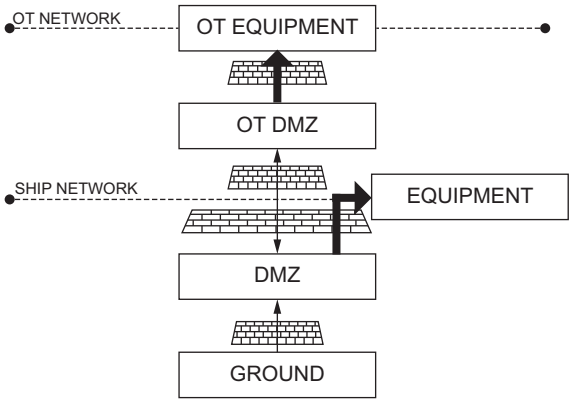
Figure 2 : Example of internal connection to DMZ



3.2.4 Ingoing packets

When necessary, and for UDP (User Datagram Protocol) datagrams only, traffic is authorized in the reverse way. As the protocol is unreliable, it must not be used for safety purpose. Error-correction can be achieved by considering UDP encapsulation of SCTP (Stream Control Transmission Protocol - RFC 6951) (see Fig 3).

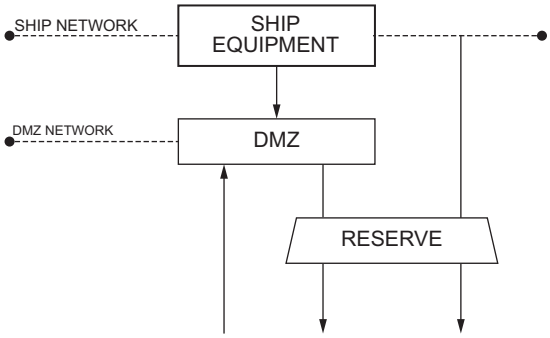
Figure 3 : Example of UDP datagrams from DMZ



3.2.5 Outgoing connections

From Level 2 Equipment, for outgoing connections, connections from the inside “DMZ” to the outside “Ground” are accepted with the usage of a reverse proxy or equivalent technology in term of flow disruption (see Fig 4).

Figure 4 : Reverse proxy example



3.2.6 Diodes

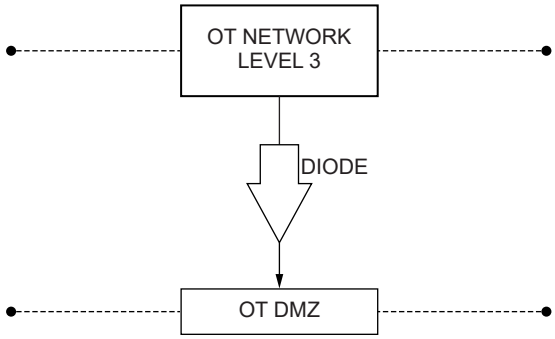
Diodes are security network equipment designed with an analog rupture to enable one-way traffic and disable any packet feedback or network connection in the other way.

Note 1: Diode network equipment may have to be recognized by the Society (see Sec 1, [1.1.3]).

Note 2: If used risk assessment methodology is the one described in Ch 1, App 1:

- The diode installation decrease the connectivity level to index 1 (CY1). (See Fig 5)
- Level 3 OT equipment at risk 3 (see Ch 1, App 1, [3.3.3]) communicating to ground systems, is to use a “one-way” diode network equipment as a mitigation measure.

Figure 5 : Diode usage example



3.2.7 Management

Management, administration, supervision or any action requiring a high level of privilege on Level 2 Equipment, Level 3 Equipment or DMZ are to be done from a dedicated network using a NG Firewall.

Administration functions, roles and users with full or high privilege on any Cat. ABC system of Level 123, are to be isolated from the network by using either a dedicated workstation or a dedicated interface (network card).

The solution is to be connected to a dedicated network who is physically dedicated, or logically partitioned (VLAN). Internet or public access from those points are strictly prohibited (see Sec 2, Fig 1).

3.2.8 Call-back

Remote Access shall be reliable, identified and authenticated by using relevant protocol authentication mechanism (e.g. IPsec) with a encryption key management. If remote access is not trusted, a call-back mechanism is to be used (modem call from ship to shore).

3.2.9 Physical access

Interconnected OT systems are to be installed in locked cabinets. The protective cases are to be designed for the ambient environment and ease of operation and maintenance of the device.

For Level 3 at risk 3 equipment, alarm doors are to be used. Seals are also to be used in order to help visual inspections during patrols.

For critical Level 3 systems not having physical access protection, a 24/7 video protection system is to record access to the system.

3.2.10 Logical alerts

When possible, for interconnected Level 3 Systems, network device alarm functions are to be configured to detect abnormal state changes and notify the user:

- When a link is disconnected or the power is turned off for a network device or network terminal
- When a link not belonging to the network is connected or the power is turned on for a network device or network terminal
- In case of loss of a network device.

CHAPTER 5
TYPE APPROVAL CERTIFICATION

Section 1 General

1 Scope

1.1 General

1.1.1 Application

This Chapter contains requirement for certification of equipment and systems dealing with cybersecurity:

- As a rule, equipment and systems to be certified are to comply at least with the applicable requirements of Sec 2.
- The additional requirements of Sec 3 (completed by Sec 4 and Sec 5 as applicable) may have to be complied with for the following security solutions:
  - Compliance Software Registry (CSR) solutions
  - Inspection and Decontamination Gate (IDG) solutions
  - Events and Logs Recorders (ELR) Solutions.

1.1.2 Correspondence with IEC 62443-3 and IACS UR E27

A correspondence table provided in Tab 1 presents maping between:

- the requirements of IEC 62443-3-3: Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels
- the requirements of IACS UR E27 as listed in Sec 2, Tab 1 and Sec 2, Tab 2
- the requirements of Sec 4 and Sec 5.

Table 1 : Correspondence between this Chapter and the requirements of IEC 62443-3-3

Item No. in Sec 2, Tab 1 and Sec 2, Tab 2	Objectives	Reference in Sec 4 and Sec 5	Reference in IEC 62443-3-3
1	Human user identification and authentication	Sec 4, [3.3.1]	IEC 62443-3-3/SR 1.1
2	Account management	Sec 4, [3.3.1]	IEC 62443-3-3/SR 1.3
3	Identifier management	Sec 4, [3.3.1]	IEC 62443-3-3/SR 1.4
4	Authenticator management	Sec 4, [3.3.1]	IEC 62443-3-3/SR 1.5
5	Wireless access management	Sec 4, [3.2.4]	IEC 62443-3-3/SR 1.6
6	Strength of password-based authentication	Sec 4, [3.3.2]	IEC 62443-3-3/SR 1.7
7	Authenticator feedback	Sec 4, [3.3.3]	IEC 62443-3-3/SR 1.10
8	Authorization enforcement	Sec 4, [3.3.1]	IEC 62443-3-3/SR 2.1
9	Wireless use control	Sec 4, [3.2.4]	IEC 62443-3-3/SR 2.2
10	Use control for portable and mobile devices	Sec 4, [3.4.1]	IEC 62443-3-3/SR 2.3
11	Mobile code	Sec 4, [3.2.1]	IEC 62443-3-3/SR 2.4
12	Session lock	Sec 4, [3.3.3]	IEC 62443-3-3/SR 2.5
13	Auditable events	Sec 4, [7.1.1]	IEC 62443-3-3/SR 2.8
14	Audit storage capacity	Sec 5, [2.3.4] for Compliance and Software Registry (CSR), Sec 5, [4.4.4] for Events and Logs Recording (ELR)	IEC 62443-3-3/SR 2.9
15	Response to audit processing failures	Sec 4, [3.4.5] and Sec 4, [3.4.6]	IEC 62443-3-3/SR 2.10
16	Timestamps	Sec 4, [4.3.3] and Sec 4, [9.2.2] Sec 5, [4.4.10] for Events and Logs Recording (ELR)	IEC 62443-3-3/SR 2.11
17	Communication integrity	Sec 4, [10.1.2]	IEC 62443-3-3/SR 3.1
18	Malicious code protection	Sec 4, [10.1.2]	IEC 62443-3-3/SR 3.2
19	Security functionality verification	Sec 4, [5.1.3]	IEC 62443-3-3/SR 3.3
20	Deterministic output	Sec 4, [3.4.5]	IEC 62443-3-3/SR 3.6
21	Information confidentiality	Sec 4, [3.4.2] and Sec 4, [6.1.3]	IEC 62443-3-3/SR 4.1

Item No. in Sec 2, Tab 1 and Sec 2, Tab 2	Objectives	Reference in Sec 4 and Sec 5	Reference in IEC 62443-3-3
22	Use of cryptography	Sec 4, [3.4.2] and Sec 4, [6.1.3]	IEC 62443-3-3/SR 4.3
23	Audit log accessibility	Sec 4, [7.1]	IEC 62443-3-3/SR 6.1
24	Denial of service protection	Sec 4, [7.1]	IEC 62443-3-3/SR 7.1
25	Resource management	Sec 4, [4.3]	IEC 62443-3-3/SR 7.2
26	System backup	Sec 4, [8.3.6]	IEC 62443-3-3/SR 7.3
27	System recovery and reconstitution	Sec 4, [3.4.5]	IEC 62443-3-3/SR 7.4
28	Emergency power	Sec 4, [3.4.5]	IEC 62443-3-3/SR 7.5
29	Network and security configuration settings	Sec 4, [10.1.2]	IEC 62443-3-3/SR 7.6
30	Least functionality	Sec 4, [3.2.1]	IEC 62443-3-3/SR 7.7
31	Multifactor authentication for human users	Sec 4, [3.3.3]	IEC 62443-3-3/SR 1.1, RE 2
32	Software process and device identification and authentication	Sec 4, [3.3.1]	IEC 62443-3-3/SR 1.2
33	Unsuccessful login attempts	Sec 4, [3.3.3]	IEC 62443-3-3/SR 1.11
34	System use notification	Sec 4, [3.4.5]	IEC 62443-3-3/SR 1.12
35	Access via Untrusted Networks	Sec 4, [7.1.1]	IEC 62443-3-3/SR 1.13
36	Explicit access request approval	Sec 4, [3.4.6]	IEC 62443-3-3/SR 1.13, RE1
37	Remote session termination	Sec 4, [6.1.2]	IEC 62443-3-3/SR 2.6
38	Cryptographic integrity protection	Sec 4, [4.3]	IEC 62443-3-3/SR 3.1, RE1
39	Input validation	Sec 4, [4.3]	IEC 62443-3-3/SR 3.5
40	Session integrity	Sec 4, [4.3]	IEC 62443-3-3/SR 3.8
41	Invalidation of session IDs after session termination	Sec 4, [3.3.3]	IEC 62443-3-3/SR 3.8, RE1

Section 2 Cyber Resilience of On-Board Systems and Equipment

1 General

1.1 Introduction

1.1.1 Technological evolution of vessels, ports, container terminals, etc. and increased reliance upon Operational Technology (OT) and Information Technology (IT) has created an increased possibility of cyber-attacks to affect business, personnel data, human safety, the safety of the ship, and also possibly threaten the marine environment. Safeguarding shipping from current and emerging threats must involve a range of controls that are continually evolving which would require incorporating security features in the equipment and systems at design and manufacturing stage. It is therefore necessary to establish a common set of minimum requirements to deliver systems and equipment that can be described as cyber resilient.

This Section specifies requirements for cyber resilience of on-board systems and equipment.

1.2 Limitations

1.2.1 This Section does not cover environmental performance for the system hardware and the functionality of the software. In addition to this Section, following is to be applied:

- NR467, Pt C, Ch 3, Sec 6 for environmental performance for the system hardware
- NR467, Pt C, Ch 3, Sec 3 for safety of equipment for the functionality of the software.

1.3 Scope of applicability

1.3.1 Refer to Ch 3, Sec 2

For navigation and radiocommunication systems, the application of IEC 61162-460 or other equivalent standards in lieu of the required security capabilities in [4] may be accepted by the Society, on the condition that requirements in Ch 3, Sec 2 are complied with.

1.3.2 Information and Communication Technology (ICT)

Attention is made to the following additional documents on CBSs and Cyber Resilience:

- NR467 Rules for the Classification of Steel Ships, Pt C, Ch 3, Sec 3
- Requirements given in Ch 3, Sec 2
- IACS Recommendation 166 on Cyber Resilience.

Note 1: Non-mandatory recommended technical requirements that stakeholders may reference and apply to assist with the delivery of cyber resilient ships, whose resilience can be maintained throughout their service life.

1.4 Definitions and abbreviations

1.4.1 Attack surface

The set of all possible points where an unauthorized user can access a system, cause an effect on or and extract data from. The attack surface comprises two categories: digital and physical. The digital attack surface encompasses all the hardware and software that connect to an organization's network. These include applications, code, ports, servers and websites. The physical attack surface comprises all endpoint devices that an attacker can gain physical access to, such as desktop computers, hard drives, laptops, mobile phones, removable drives and carelessly discarded hardware.

1.4.2 Authentication

Provision of assurance that a claimed characteristic of an identity is correct.

1.4.3 Compensating countermeasure

An alternate solution to a countermeasure employed in lieu of or in addition to inherent security capabilities to satisfy one or more security requirements.

1.4.4 Computer Based System (CBS)

A programmable electronic device, or interoperable set of programmable electronic devices, organized to achieve one or more specified purposes such as collection, processing, maintenance, use, sharing, dissemination, or disposition of information. CBS on-board include IT and OT systems. A CBS may be a combination of subsystems connected via network. On-board CBS may be connected directly or via public means of communications (e.g. Internet) to ashore CBSs, other vessels' CBS and/or other facilities.

1.4.5 Computer Network

A connection between two or more computers for the purpose of communicating data electronically by means of agreed communication protocols.

1.4.6 Control

Means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be administrative, technical, management, or legal in nature.

1.4.7 Cyber incident

An event resulting from any offensive cyber manoeuvre, either intentional or unintentional, that targets or affects one or more CBS onboard, which actually or potentially results in adverse consequences to an onboard system, network and computer or the information that they process, store or transmit, and which may require a response action to mitigate the consequences. Cyber incidents include unauthorized access, misuse, modification, destruction or improper disclosure of the information generated, archived or used in onboard CBS or transported in the networks connecting such systems. Cyber incidents do not include system failures.

1.4.8 Cyber resilience

The capability to reduce the occurrence and mitigating the effects of incidents arising from the disruption or impairment of operational technology (OT) used for the safe operation of a ship, which potentially lead to dangerous situations for human safety, safety of the vessel and/or threat to the environment.

1.4.9 Defence in depth

Information Security strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and missions of the organization.

1.4.10 Essential Systems

CBSs contributing to the provision of services essential for propulsion and steering, and safety of the ship. Essential services comprise “Primary Essential Services” and “Secondary Essential Services”:

- Primary Essential Services are those services which need to be in continuous operation to maintain propulsion and steering
- Secondary Essential Services are those services which need not necessarily be in continuous operation to maintain propulsion and steering but which are necessary for maintaining the vessel's safety.

1.4.11 Firewall

A logical or physical barrier that monitors and controls incoming and outgoing network traffic controlled via predefined rules.

1.4.12 Firmware

Software embedded in electronic devices that provide control, monitoring and data manipulation of engineered products and systems. These are normally self-contained and not accessible to user manipulation.

1.4.13 Hardening

Hardening is the practice of reducing a system's vulnerability by reducing its attack surface.

1.4.14 Information Technology (IT)

Devices, software and associated networking focusing on the use of data as information, as opposed to Operational Technology (OT).

1.4.15 Integrated system

A system combining a number of interacting sub-systems and/or equipment organized to achieve one or more specified purposes.

1.4.16 Network switch (Switch)

A device that connects devices together on a computer network, by using packet switching to receive, process and forward data to the destination device.

1.4.17 Offensive cyber manoeuvre

Actions that result in denial, degradation, disruption, destruction, or manipulation of OT or IT systems.

1.4.18 Operational technology (OT)

Devices, sensors, software and associated networking that monitor and control onboard systems. Operational technology systems may be thought of as focusing on the use of data to control or monitor physical processes.

1.4.19 OT system

CBSs, which provide control, alarm, monitoring, safety or internal communication functions.

1.4.20 Patches

Software designed to update installed software or supporting data to address security vulnerabilities and other bugs or improve operating systems or applications.

1.4.21 Protocols

A common set of rules and signals that computers on the network use to communicate. Protocols allow to perform data communication, network management and security. Onboard networks usually implement protocols based on TCP/IP stacks or various field buses.

1.4.22 Recovery

Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cyber security event. The Recovery function support s timely return to normal operations to reduce the impact from a cyber security event.

1.4.23 Supplier

A manufacturer or provider of hardware and/or software products, system components or equipment (hardware or software) comprising of the application, embedded devices, network devices, host devices etc. working together as system or a subsystem. The Supplier is responsible for providing programmable devices, sub-systems or systems to the System Integrator.

1.4.24 System

Combination of interacting programmable devices and/or sub-systems organized to achieve one or more specified purposes

1.4.25 System Categories (I, II, III)

System categories based on their effects on system functionality, which are defined in Ship Rules, Pt C, Ch 3, Sec 3.

1.4.26 System Integrator

The specific person or organization responsible for the integration of systems and products provided by suppliers into the system invoked by the requirements in the ship specifications and for providing the integrated system. The system integrator may also be responsible for integration of systems in the ship. Until vessel delivery, this role shall be taken by the Shipyard unless an alternative organization is specifically contracted/assigned this responsibility.

1.4.27 Untrusted network

Any network outside the scope of applicability of this Section.

2 Security Philosophy

2.1 Systems and Equipment

2.1.1 A System can consist of group of hardware and software enabling safe, secure and reliable operation of a process. Typical example could be Engine control system, DP system, etc.

2.1.2 Equipment may be one of the following:

- Network devices (i.e. routers, managed switches)
- Security devices (i.e. firewall, Intrusion Detection System)
- Computers (i.e. workstation, servers)
- Automation devices (i.e. Programmable Logic Controllers)
- Virtual machine cloud-hosted.

2.2 Cyber Resilience

2.2.1 The cyber resilience requirements in Article [4] are be applicable for all systems in scope of Ch 3, Sec 2 as applicable.

Additional requirements related to interface with untrusted networks will only apply for systems where such connectivity is designed.

2.3 Essential Systems Availability

2.3.1 Security measures for Essential system are not to adversely affect the systems availability.

2.3.2 Implementation of security measures is not to cause loss of safety functions, loss of control functions, loss of monitoring functions or loss of other functions which could result in health, safety and environmental consequences.

2.3.3 The system is to be adequately designed to allow the ship to continue its mission critical operations in a manner that ensures the confidentiality, integrity, and availability of the data necessary for safety of the vessel, its systems, personnel and cargo.

2.4 Compensating Countermeasures

2.4.1 Compensating countermeasure may be employed in lieu of or in addition to inherent security capabilities to satisfy one or more security requirements.

Compensating countermeasure(s) are to meet the intent and rigor of the original stated requirement considering the referenced standards as well as the differences between each requirement and the related items in the standards, and follow the principles specified in [3.1.4].

3 Documentation

3.1 CBS Documentation

3.1.1 The documents listed in [3.1.2] to [3.1.11] are to be submitted to the Society for review and approval in accordance with the requirements in this Section (see also [6.2]).

3.1.2 CBS asset inventory

The CBS asset inventory is to include the following information:

- List of hardware components (e.g., host devices, embedded devices, network devices):
  - Name
  - Brand/manufacturer
  - Model/type
  - Short description of functionality/purpose
  - Physical interfaces (e.g., network, serial)
  - Name/type of system software (e.g., operating system, firmware)
  - Version and patch level of system software
  - Supported communication protocols
- List of software components (e.g., application software, utility software):
  - The hardware component where it is installed
  - Brand/manufacturer
  - Model/type
  - Short description of functionality/purpose
  - Version of software.

3.1.3 Topology diagrams

a) The physical topology diagram is to illustrate the physical architecture of the system. It is to be possible to identify the hardware components in the CBS asset inventory. The diagram is to illustrate the following:
   - All endpoints and network devices, including identification of redundant units
   - Communication cables (networks, serial links), including communication with I/O units
   - Communication cables to other networks or systems

b) The logical topology diagram is to illustrate the data flow between components in the system. the diagram is to illustrate the following:
   - Communication endpoints (e.g. workstations, controllers, servers)
   - Network devices (switches, routers, firewalls)
   - Physical and virtual computers
   - Physical and virtual communication paths
   - Communication protocols

One combined topology diagram may be acceptable if all requested information can be clearly illustrated.

3.1.4 Description of security capabilities

This document is to describe how the CBS with its hardware and software components meets the required security capabilities in [4.1.2].

Any network interfaces to other CBSs in the scope of applicability of Ch 3, Sec 2 is to be described. The description is to include destination CBS, data flows, and communication protocols. If the System integrator has allocated the destination CBS to another security zone, components providing protection of the security zone boundary (see Ch 3, Sec 2, [6.2.1]) are to be described in detail if delivered as part of the CBS.

Any network interfaces to other systems or networks outside the scope of applicability of Ch 3, Sec 2 (untrusted networks) are be described. The description is to specify compliance with the additional security capabilities in [4.1.3], and include relevant procedures or instructions for the crew. Components providing protection of the security zone boundary (see Ch 3, Sec 2, [6.3.1]) is to be described in detail if delivered as part of the CBS.

A separate chapter shall be designated for each requirement. All hardware and software components in the system shall be addressed in the description, as relevant.

If any requirement is not fully met, this shall be specified in the description, and compensating countermeasures shall be proposed. The compensating countermeasures should:

- Protect against the same threats as the original requirement
- Provide an equal level of protection as the original requirement
- Not be a security control that is required by other requirements in this Section
- Not introduce higher security risk

Any supporting documents (e.g. OEM information) necessary to verify compliance with the requirements shall be referenced in the description and submitted.

3.1.5 Test procedure of security capabilities

This document is to describe how to demonstrate by testing that the system complies with the requirements in [4.1.2] and [4.1.3], including any compensating countermeasures. Demonstration of compliance by analytic evaluation may be specially considered. The procedure is to include a separate chapter for each applicable requirement and describe:

- Necessary test setup (i.e. to ensure the test can be repeated with the same expected result)
- Test equipment
- Initial condition(s)
- Test methodology, detailed test steps
- Expected results and acceptance criteria

The procedure is also to include means to update test results and record findings during the testing.

3.1.6 Security configuration guidelines

This document is to describe recommended configuration settings of the security capabilities and specify default values. The objective is to ensure the security capabilities are implemented in accordance with Ch 3, Sec 2 and any specifications by the System integrator (e.g. user accounts, authorisation, password policies, safe state of machinery, firewall rules, etc.)

The document is to serve as basis for verification of item no. 29 in Tab 1.

3.1.7 Secure development lifecycle documents

This documentation is to be submitted to the Society upon request and is to describe the supplier's processes and controls in accordance with requirements for secure development lifecycle in [5]. Software updates and patching are to be described. The document is to prepare the Society for survey as per [6.3.5].

3.1.8 Plans for maintenance and verification of the CBS

This document is to be submitted to the Society upon request and is to include procedures for security-related maintenance and testing of the system. The document is to include instructions for how the user can verify correct operation of the system's security functions as required by item no. 19 in Tab 1.

3.1.9 Information supporting the Shipowner’s incident response and recovery plan

This document is to be submitted to the Society upon request and is to include procedures or instructions allowing the user to accomplish the following:

- Local independent control (see Ch 3, Sec 2, [8.3])
- Network isolation (see Ch 3, Sec 2, [8.4])
- Forensics by use of audit records (see item no. 13 in Tab 1)
- Deterministic output (see Ch 3, Sec 2, [8.5] and item no. 20 in Tab 1)
- Backup (see item no. 26 in Tab 1)
- Restore (see item no. 27 in Tab 1)
- Controlled shutdown, reset, roll-back and restart (see Ch 3, Sec 2, [9.4]).

3.1.10 Management of change plan

This document is to be submitted to the Society upon request. It is expected that this procedure is not specific for cyber security and is also required by NR467, Pt C, Ch 3, Sec 3.

3.1.11 Test reports

CBSs with Type approval certificate covering the security capabilities of this Section may be exempted from survey by the Society. However, test reports signed by the supplier are to be submitted to the Society, demonstrating that the supplier has completed design, construction, testing, configuration, and hardening as would otherwise be verified by the Society in survey (see [6.3]).

4 System Requirements

4.1 General

4.1.1 This Article specifies the required security capabilities for CBSs in the scope specified in [1.3].

The requirements in this Article [4] are based on the selected requirements in IEC 62443-3-3. To determine the full content, rationale and relevant guidance for each requirement, the reader should consult the referenced standard.

4.1.2 Required security capabilities

The following security capabilities (see Tab 1) are required for all CBSs in the scope specified in [1.3].

4.1.3 Additional security capabilities

The following additional security capabilities (see Tab 2) are required for CBSs with network communication to untrusted networks (i.e. interface to any networks outside the scope of Ch 3, Sec 2).

CBSs with communication traversing the boundaries of security zones shall also meet requirements for network segmentation and zone boundary protection in Ch 3, Sec 2, [6.2] and Ch 3, Sec 2, [6.3].

Table 1 : Required security capabilities

Item No.	Objectives	Requirements
PROTECT AGAINST CASUAL OR COINCIDENTAL ACCESS BY UNAUTHENTICATED ENTITIES		
1	Human user identification and authentication	The CBS is to identify and authenticate all human users who can access the system directly or through interfaces (IEC 62443-3-3/SR 1.1)
2	Account management	The CBS is to provide the capability to support the management of all accounts by authorized users, including adding, activating, modifying, disabling and removing account (IEC 62443-3-3/SR 1.3)
3	Identifier management	The CBS is to provide the capability to support the management of identifiers by user, group and role (IEC 62443-3-3/SR 1.4)
4	Authenticator management	The CBS is to provide the capability to: • Initialize authenticator content • Change all default authenticators upon control system installation • Change/refresh all authenticators • Protect all authenticators from unauthorized disclosure and modification when stored and transmitted. (IEC 62443-3-3/SR 1.5)
5	Wireless access management	The CBS is to provide the capability to identify and authenticate all users (humans, software processes or devices) engaged in wireless communication (IEC 62443-3-3/SR 1.6)
6	Strength of password-based authentication	The CBS is to provide the capability to enforce configurable password strength based on minimum length and variety of character types (IEC 62443-3-3/SR 1.7)
7	Authenticator feedback	The CBS is to obscure feedback during the authentication process (IEC 62443-3-3/SR 1.10)
PROTECT AGAINST CASUAL OR COINCIDENTAL MISUSE		
8	Authorization enforcement	On all interfaces, human users are to be assigned authorizations in accordance with the principles of segregation of duties and least privilege (IEC 62443-3-3/SR 2.1)
9	Wireless use control	The CBS is to provide the capability to authorize, monitor and enforce usage restrictions for wireless connectivity to the system according to commonly accepted security industry practices (IEC 62443-3-3/SR 2.2)
10	Use control for portable and mobile devices	When the CBS supports use of portable and mobile devices, the system is to include the capability to: a) Limit the use of portable and mobile devices only to those permitted by design b) Restrict code and data transfer to/from portable and mobile devices. Note: Port limits / blockers (and silicone) could be accepted for a specific system (IEC 62443-3-3/SR 2.3)
11	Mobile code	The CBS is to control the use of mobile code such as Java scripts, Active X and PDF (IEC 62443-3-3/SR 2.4)

Item No.	Objectives	Requirements
12	Session lock	The CBS is to be able to prevent further access after a configurable time of inactivity or following activation of manual session lock (IEC 62443-3-3/SR 2.5)
13	Auditable events	The CBS is to generate audit records relevant to security for at least the following events: access control, operating system events, backup and restore events, configuration changes, loss of communication (IEC 62443-3-3/SR 2.8)
14	Audit storage capacity	The CBS is to provide the capability to allocate audit record storage capacity according to commonly recognized recommendations for log management. Auditing mechanisms are to be implemented to reduce the likelihood of such capacity being exceeded (IEC 62443-3-3/SR 2.9)
15	Response to audit processing failures	The CBS is to provide the capability to prevent loss of essential services and functions in the event of an audit processing failure (IEC 62443-3-3/SR 2.10)
16	Timestamps	The CBS is to timestamp audit records (IEC 62443-3-3/SR 2.11)
PROTECT THE INTEGRITY OF THE CBS AGAINST CASUAL OR COINCIDENTAL MANIPULATION		
17	Communication integrity	The CBS is to protect the integrity of transmitted information. Note: Cryptographic mechanisms shall be employed for wireless networks (IEC 62443-3-3/SR 3.1)
18	Malicious code protection	The CBS is to provide capability to implement suitable protection measures to prevent, detect and mitigate the effects due to malicious code or unauthorized software. It is to have the feature for updating the protection mechanisms (IEC 62443-3-3/SR 3.2)
19	Security functionality verification	The CBS is to provide the capability to support verification of the intended operation of security functions and report when anomalies occur during maintenance (IEC 62443-3-3/SR 3.3)
20	Deterministic output	The CBS is to provide the capability to set outputs to a predetermined state if normal operation cannot be maintained as a result of an attack. The predetermined state could be: • Unpowered state, • Last-known value, or • Fixed value. (IEC 62443-3-3/SR 3.6)
PREVENT THE UNAUTHORIZED DISCLOSURE OF INFORMATION VIA EAVESDROPPING OR CASUAL EXPOSURE		
21	Information confidentiality	The CBS is to provide the capability to protect the confidentiality of information for which explicit read authorization is supported, whether at rest or in transit. Note: For wireless network, cryptographic mechanisms are to be employed to protect confidentiality of all information in transit. (IEC 62443-3-3/SR 4.1)
22	Use of cryptography	If cryptography is used, the CBS is to use cryptographic algorithms, key sizes and mechanisms according to commonly accepted security industry practices and recommendations (IEC 62443-3-3/SR 4.3)
MONITOR THE OPERATION OF THE CBS AND RESPOND TO INCIDENTS		
23	Audit log accessibility	The CBS is to provide the capability for accessing audit logs on read only basis by authorized humans and/or tools (IEC 62443-3-3/SR 6.1)
ENSURE THAT THE CONTROL SYSTEM OPERATES RELIABLY UNDER NORMAL PRODUCTION CONDITIONS		
24	Denial of service protection	The CBS is to provide the minimum capability to maintain essential functions during DoS events **(1)** (IEC 62443-3-3/SR 7.1)
25	Resource management	The CBS is to provide the capability to limit the use of resources by security functions to prevent resource exhaustion (IEC 62443-3-3/SR 7.2)
26	System backup	The identity and location of critical files and the ability to conduct backups of user-level and system-level information (including system state information) are to be supported by the CBS without affecting normal operations (IEC 62443-3-3/SR 7.3)

Item No.	Objectives	Requirements
27	System recovery and reconstitution	The CBS is to provide the capability to be recovered and reconstituted to a known secure state after a disruption or failure (IEC 62443-3-3/SR 7.4)
28	Alternative power source	The CBS is to provide the capability to switch to and from an alternative power source without affecting the existing security state or a documented degraded mode (IEC 62443-3-3/SR 7.5)
29	Network and security configuration settings	The CBS traffic is to provide the capability to be configured according to recommended network and security configurations as described in guidelines provided by the supplier. The CBS is to provide an interface to the currently deployed network and security configuration settings (IEC 62443-3-3/SR 7.6)
30	Least Functionality	The installation, the availability and the access rights of the following are to be limited to the strict needs of the functions provided by the CBS: • operating systems software components, processes and services • network services, ports, protocols, routes and hosts accesses and any software. (IEC 62443-3-3/SR 7.7)
(1) It is acceptable that the CBS may operate in a degraded mode upon DoS events, but it is not fail in a manner which may cause hazardous situations. Overload-based DoS events are to be considered, i.e. where the networks capacity is attempted flooded, and where the resources of a computer is attempted consumed.		

Table 2 : Additional security capabilities

Item No.	Objectives	Requirements
31	Multifactor authentication for human users	Multifactor authentication is required for human users when accessing the CBS from or via an untrusted network (IEC 62443-3-3/SR 1.1, RE 2)
32	Software process and device identification and authentication	The CBS is to identify and authenticate software processes and devices (IEC 62443-3-3/SR 1.2)
33	Unsuccessful login attempts	The CBS is to enforce a limit of consecutive invalid login attempts from untrusted networks during a specified time period (IEC 62443-3-3/SR 1.11)
34	System use notification	The CBS is to provide the capability to display a system use notification message before authenticating. The system use notification message is to be configurable by authorized personnel (IEC 62443-3-3/SR 1.12)
35	Access via Untrusted Networks	Any access to the CBS from or via untrusted networks is to be monitored and controlled (IEC 62443-3-3/SR 1.13)
36	Explicit access request approval	The CBS is to deny access from or via untrusted networks unless explicitly approved by authorized personnel on board (IEC 62443-3-3/SR 1.13, RE1)
37	Remote session termination	The CBS is to 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 (IEC 62443-3-3/SR 2.6)
38	Cryptographic integrity protection	The CBS is to employ cryptographic mechanisms to recognize changes to information during communication with or via untrusted networks (IEC 62443-3-3/SR 3.1, RE1)
39	Input validation	The CBS shall validate the syntax, length and content of any input data via untrusted networks that is used as process control input or input that directly impacts the action of the CBS. (IEC 62443-3-3/SR 3.5)
40	Session integrity	The CBS is to protect the integrity of sessions. Invalid session IDs are to be rejected (IEC 62443-3-3/SR 3.8)
41	Invalidation of session IDs after session termination	The system is to invalidate session IDs upon user logout or other session termination (including browser sessions) (IEC 62443-3-3/SR 3.8, RE1)

5 Secure Development Lifecycle requirements

5.1 Secure Development Lifecycle (SDLC)

5.1.1 A Secure Development Lifecycle (SDLC) broadly addressing security aspects in following stages is to be followed for the development of systems or equipment:

- Requirement analysis phase
- Design phase
- Implementation phase
- Verification phase
- Release phase
- Maintenance Phase
- End of life phase.

A document is to be produced that records how the security aspects have been addressed in above phases and is to at minimum integrate controlled processes as set out in [5.1.2] to [5.1.8]. The said document is required to be submitted to the Society for approval.

5.1.2

(IEC 62443-4-1/SM-8) The manufacturer is to have procedural and technical controls in place to protect private keys used for code signing, if applicable, from unauthorized access or modification.

5.1.3

(IEC 62443-4-1/SUM-2) A process is to be employed to ensure that documentation about product security updates is made available to users (which could be through establishing a cyber security point of contact or periodic publication which can be accessed by the user) 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 can have, 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

5.1.4

(IEC 62443-4-1/SUM-3) A process is to be employed to ensure that documentation about dependent component or operating system security updates is available to users that includes but is not limited to:

a) Stating whether the product is compatible with the dependent component or operating system security update

5.1.5

(IEC 62443-4-1/SUM-4) A process is to 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

Note 1: The manufacturer is to have QA process to test the update before releasing.

5.1.6

(IEC 62443-4-1/SG-1) A process is to exist to create product documentation that describes the security defence in depth strategy for the product to support installation, operation and maintenance that includes:

a) Security capabilities implemented by the product and their role in the defence in depth strategy

b) Threats addressed by the defence in depth strategy; and

c) Product user mitigation strategies for known security risks associated with the product, including risks associated with legacy code

5.1.7

(IEC 62443-4-1/SG-2) A process is to be employed to create product user documentation that describes the security defence in depth measures expected to be provided by the external environment in which the product is to be used.

5.1.8

(IEC 62443-4-1/SG-3) A process is to be employed to create product user documentation that includes guidelines for hardening the product when installing and maintaining the product. The guidelines are to include, but are not limited to, instructions, rationale and recommendations for the following:

a) Integration of the product, including third-party components, with its product security context

b) Integration of the product's application programming interfaces/protocols with user applications

c) Applying and maintaining the product's defence in depth strategy

d) Configuration and use of security options/capabilities in support of local security policies, and for each security option/capability:
   - its contribution to the product's defence in depth strategy
   - descriptions of configurable and default values that include how each affects security along with any potential impact each has on work practices; and
   - setting/changing/deleting its value

e) Instructions and recommendations for the use of all security-related tools and utilities that support administration, monitoring, incident handling and evaluation of the security of the product

f) Instructions and recommendations for periodic security maintenance activities

g) Instructions for reporting security incidents for the product to the supplier

h) Description of the security best practices for maintenance and administration of the product

6 Demonstration of compliance

6.1 Introduction

6.1.1 Suppliers are to in cooperation with the System integrator determine if the requirements of this Section are mandatory for the CBS, see Fig 1.

6.1.2 Compliance with security requirements is to be demonstrated as indicated in Fig 2. This classification process is ship-specific and is to result in a System certificate.

6.1.3 Type approval is voluntary and applies for CBSs that are standard and routinely manufactured. SeeNR467, Pt C, Ch 3, Sec 3 for definition of System certification and Type approval.

6.1.4 The process in Fig 1 and Fig 2 applies also if other equivalent standards are applied for navigation and radiocommunication equipment (see [1.3]). In such case:

- the process in Fig 1 illustrates if the equivalent standard is mandatory (in lieu of the requirements of this Section)
- the process in Fig 2 illustrates that the certification process is lessened if the CBS has been type approved in accordance with the equivalent standard.

Figure 1 :

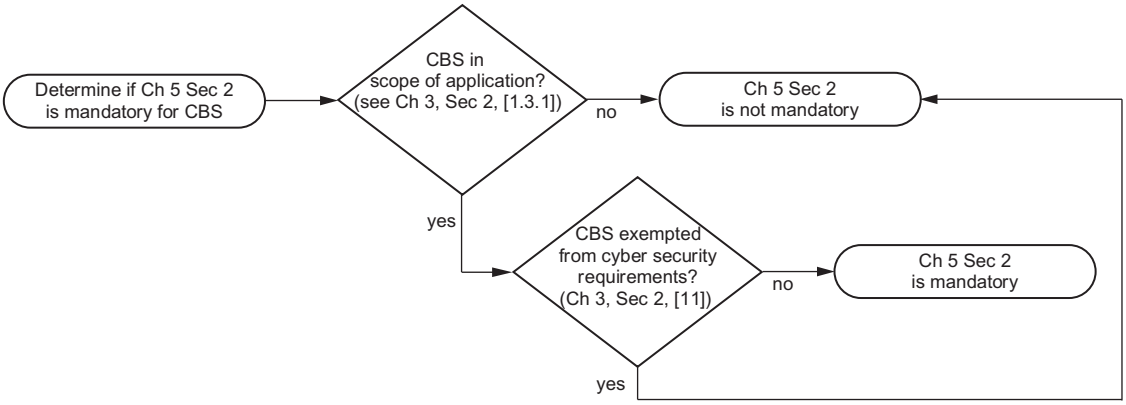
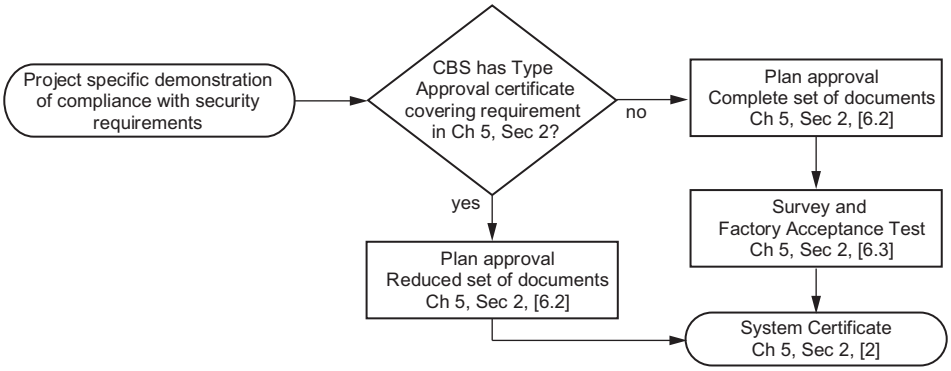


Figure 2 :



6.2 Plan approval

6.2.1

Plan approval is assessment of documents of a CBS intended for a specific vessel. The documents in [3] are required to be submitted by the supplier. The documents are to enable the Society to verify compliance with requirements in this Section.

If the CBS holds a valid Type approval certificate covering the requirements of this Section subject to approval by the Society, the supplier may submit a reduced set of vessel-specific documents to the Society (see Tab 3).

The approved version of the documents are to be included in the delivery of the CBS to the system integrator.

Table 3 : Reduced set of documents to be submitted to the Society, if the CBS holds a valid Type approval certificate covering the requirements of this Section

Document	I/A **(1)**	Requirements
CBS asset inventory (see [3.1.2])	A **(2) (3)**	To be incorporated in Vessel asset inventory (see Ch 3, Sec 2, [5.2])
Topology diagrams (see [3.1.3])	A **(2) (3)**	Enabling System integrator to design security zones and conduits (see Ch 3, Sec 2, [6.2])
Description of security capabilities (see [3.1.4])	A **(2)**	• Required security capabilities (see [4.1.2]) • Additional security capabilities, if applicable (see [4.1.3])
Test procedure for security capabilities (see [3.1.5])	A **(2)**	• Required security capabilities (see [4.1.2]) • Additional security capabilities, if applicable (see [4.1.3])
Security configuration guidelines (see [3.1.6])	I **(2)**	Network and security configuration settings (see item no. 29 in Tab 1)
Secure development lifecycle (see [3.1.7])	A **(2)**	SDLC requirements (see [5])
Plans for maintenance and verification (see [3.1.8])	I **(2)**	Security functionality verification (see item no. 19 in Tab 1)
Information supporting incident response and recovery plans (see [3.1.9]	I **(2)**	• Auditable events (see item no. 13 in Tab 1) • Deterministic output (see item no. 20 in Tab 1) • System backup (see item no. 26 in Tab 1) • System recovery and reconstitution (see item no. 27 in Tab 1)
Management of change plan (see [3.1.10])	I **(2)**	Management of change process (see NR467, Pt C, Ch 3, Sec 3)
Test reports (see [3.1.11])	I **(3)**	Configuration of security capabilities and hardening (see [3.1.6] and [5.1.8])

(1) I: to be submitted for information; A: to be submitted for approval
(2) Required for CBS without type approved security capabilities
(3) Required for CBS with type approved security capabilities

6.3 Survey and factory acceptance test

6.3.1 General

Survey and factory acceptance testing (FAT) is a vessel-specific verification activity required for CBSs that do not hold a valid Type approval certificate covering the requirements of this Section

The objective of the survey and FAT is to demonstrate by testing and/or analytic evaluation that the CBS complies with applicable requirements in this Section. The survey and FAT are to be carried out at the supplier's premises or at other works having the adequate apparatus for testing and inspection.

After completed plan approval and survey/FAT, the Society will issue a System certificate that is to accompany the CBS upon delivery to the system integrator.

The following [6.3.2] to [6.3.5] specify the survey and FAT activities.

6.3.2 General survey items

The supplier is to demonstrate that design, construction, and internal testing has been completed.

It is also to be demonstrated that the system to be delivered is correctly represented by the approved documentation. This is to be done by inspecting the system and comparing the components and arrangement/architecture with the asset inventory (see [3.1.2]) and the topology diagrams (see [3.1.3]).

6.3.3 Test of security capabilities

The supplier is to test the required security capabilities on the system to be delivered. The tests is to be carried out in accordance with the approved test procedure in [3.1.5] and be witnessed/accepted by the Surveyor.

The tests shall provide the class surveyor with reasonable assurance that all requirements are met. This implies that testing of identical components is normally not required.

6.3.4 Correct configuration of security capabilities

The supplier is to test/demonstrate for the Surveyor that security settings in the system's components have been configured in accordance with the configuration guidelines in [3.1.6]. This demonstration may be carried out in conjunction with testing of the security capabilities.

The security settings are to be documented in a report, e.g. a ship-specific instance of the configuration guidelines.

6.3.5 Secure development lifecycle

The supplier is to, in accordance with documentation in [3.1.7], demonstrate compliance with requirements for secure development lifecycle in [5]:

a) Controls for private keys (IEC 62443-4-1/SM-8)

This requirement applies if the system includes software that is digitally signed for the purpose of enabling the user to verify its authenticity.

The supplier is to present management system documentation substantiating that policies, procedures and technical controls are in place to protect generation, storage and use of private keys used for code signing from unauthorized access.

The policies and procedures are to address roles, responsibilities and work processes. The technical controls is to include e.g. physical access restrictions and cryptographic hardware (e.g. Hardware security module) for storage of the private key.

b) Security update documentation (IEC 62443-4-1/SUM-2)

The supplier is to present management system documentation substantiating that a process is established in the organization to ensure security updates are informed to the users. The information to the users is to include the items listed in [5.1.3].

c) Dependent component security update documentation (IEC 62443-4-1/SUM-3)

The supplier is to present management system documentation, as required by [5.1.4], substantiating that a process is established in the organization to ensure users are informed whether the system is compatible with updated versions of acquired software in the system (new versions/patches of operating system or firmware). The information is to address how to manage risks related to not applying the updated acquired software.

d) Security update delivery (IEC 62443-4-1/SUM-4)

The supplier is to present management system documentation, as required by [5.1.5], substantiating that a process is established in the organization ensuring that system security updates are made available to users, and describing how the user may verify the authenticity of the updated software.

e) Product defence in depth (IEC 62443-4-1/SG-1)

The supplier is to present management system documentation, as required by [5.1.6], substantiating that a process is established in the organization to document a strategy for defence-in-depth measures to mitigate security threats to software in the CBS during installation, maintenance and operation.

Examples of threats could be installation of unauthorised software, weaknesses in the patching process, tampering with software in the operational phase of the ship.

f) Defence in depth measures expected in the environment (IEC 62443-4-1/SG-2)

The supplier is to present management system documentation, as required by [5.1.7], substantiating that a process is established in the organization to document defence-in-depth measures expected to be provided by the external environment, such as physical arrangement, policies and procedures.

g) Security hardening guidelines (IEC 62443-4-1/SG-3)

The supplier is to present management system documentation, as required by [5.1.8], substantiating that a process is established in the organization to ensure that hardening guidelines are produced for the system.

The guidelines is to specify how to reduce vulnerabilities in the system by removal/prohibiting /disabling of unnecessary software, accounts, services, etc.

Section 3 Additional Requirements for Type Approval of Security Solutions

1 General

1.1 Application

1.1.1 Type Approval

The Type Approval process is intended to assess equipment designed by using an approach of sensitive components identification, development constraints, hardened protection, code verification and evaluation integration, secure maintenance, preservation of traces and monitoring interfacing.

1.1.2 Security Solutions

Security Solutions are equipment dedicated to improvement and efficiency of cyber security.

Security Solutions are to be type approved as any standard equipment, see [1.1.1].

Three different security solutions are considered:

- the Compliance and Software Registry (CSR) which is an anti-tamper technology installed to prevent changes in operation and/or to detect attacks before/during their occurrence, as defined in Sec 5, [2]
- the Inspection and Decontamination Gate (IDG) which is an anti-malware technology used to detect malicious signatures, suspect behaviours and indicators of compromise during attacks, as defined in Sec 5, [3]
- the Events and Logs Recorder (ELR) which is a forensic technology used to determine paths of attacks and responsibilities after attacks and before during their occurrence, as defined in Sec 5, [4].

2 Document to be submitted

2.1 Methodology

2.1.1 Workflow

For equipment to be type approved, the following steps apply:

- “Basic”, “Intermediate” and “Detailed” Cyber Inventory are to be built by following Ch 1, Sec 2
- Equipment is to be secure by design by following Sec 4
- Criticality assessment is to be built by following Ch 1, Sec 3
- Design assessment is to be built by following Ch 1, Sec 4
- Cyber Handbook is to be built by following Ch 1, Sec 6.

2.1.2 Workflow for security solutions

In addition to the workflow detailed in [2.1.1], the following are to be submitted:

- Compliance and Software Registry (CSR) security solution are to be designed in accordance with Sec 5, [2]
- Inspection and Decontamination Gate (IDG) security solution are to be designed in accordance with Sec 5, [3]
- Events and Logs Recorder (ELR) security solution are to be designed in accordance with Sec 5, [4].

2.2 Documentation

2.2.1 Documentation for Type Approval

The general documentation listed in Tab 1 is to be submitted for approval

In addition the documentation to be submitted for security mechanisms is listed in Tab 2.

2.2.2 Additional documentation for CSR Security Solution

In addition to the documentation detailed in [2.2.1], the documents to be submitted for Compliance and Software Registry (CSR) are listed in:

- Tab 3 for CSR security mechanisms
- Tab 4 are CSR user guide.

2.2.3 Additional documentation for IDG Security Solution

In addition to the documentation detailed in [2.2.1], the documents to be submitted for Intrusion and Detection Gate (IDG) security solution are listed in listed in:

- Tab 5 for IDG security mechanisms
- Tab 6 are IDG user guide.

2.2.4 Additional documentation for ELR Security Solution

In addition to the documentation detailed in [2.2.1], the documents be submitted for Events and Logs Recorder (ELR) security solution are listed in

- Tab 7 for ELR security mechanisms
- Tab 8 for ELR user guide.

Table 1 : General documentation to be submitted for equipment type approval

Document **(1)**	Reference
Cyber Inventory:	
• Basic Inventory	• Ch 1, Sec 2, Tab 1
• Intermediate Inventory	• Ch 1, Sec 2, Tab 2
• Detailed Inventory	• Ch 1, Sec 2, Tab 3
Criticality Assessment	• Ch 1, Sec 3
Design assessment	• Ch 1, Sec 4
completed by:	
• if any: Plan approval of on board to on shore connections design	• Ch 4, Sec 2, Tab 1
• if any: Plan approval of operational technologies connections design	• Ch 4, Sec 4, Tab 1
Cyber Handbook:	
• Handbook scope	• Ch 1, Sec 6, Tab 1 and Ch 1, Sec 6, Tab 2
• Procedures	• Ch 1, Sec 6, Tab 6
(1) To be submitted for approval	

Table 2 : Additional documentation to be submitted for equipment security mechanisms

Topic	Reference	A / I **(1)**
SYSTEM		
Description	Sec 4, [1.2.1]	I
Architecture	Sec 4, [1.2.2]	I
IDENTIFICATION		
Extension	Sec 4, [1.3.1]	I
Security functions	Sec 4, [1.3.2]	A
DEVELOPMENT		
Risk analysis	Sec 4, [2.1.1]	A
Development platform **(2)**	Sec 4, [2.1.2]	I
Secure development **(2)**	Sec 4, [2.1.3]	I
Security assurance plan	Sec 4, [2.1.4]	A
Audits **(2)**	Sec 4, [2.1.5]	I
Principle of least privilege	Sec 4, [2.2.1]	I
Code robustness **(2)**	Sec 4, [2.2.2]	I
SCADA systems	Sec 4, [2.2.3]	I
Secure lifecycle	Sec 4, [2.2.4]	I
Software delivery	Sec 4, [2.2.5]	I
Integrated architecture of security solutions	Sec 5, [1.1.6]	I
PROTECTION		
Extensions hardening **(2)**	Sec 4, [3.2.1]	A
ICS hardening	Sec 4, [3.2.2]	A
Equipment hardening **(2)**	Sec 4, [3.2.3]	A
(1) A: to be submitted for approval; I: to be submitted for information **(2)** May have to be recognized by the Society (see Ch 4, Sec 1, [1.1.3])		

Topic	Reference	A / I **(1)**
Accounts and roles	Sec 4, [3.3.1]	A
Passwords management	Sec 4, [3.3.2]	A
Authentication	Sec 4, [3.3.3]	A
Physical access	Sec 4, [3.4.1]	A
Storage encryption **(2)**	Sec 4, [3.4.2]	A
External connections	Sec 4, [3.4.3]	I
Renewable media usage	Sec 4, [3.4.4]	I
In operation security	Sec 4, [3.4.5]	A
Remotely controlled systems	Sec 4, [3.4.6]	A
VERIFICATION		
Compliance and software registry interface **(2)**	Sec 4, [4.2.1]	A
Elements of integrity	Sec 4, [4.3.1]	A
EVALUATION		
Antivirus solution **(2)**	Sec 4, [5.2.1]	A
COMMUTATION		
Architecture	Sec 4, [6.1.1]	A
Connection management	Sec 4, [6.1.2]	I
Encryption	Sec 4, [6.1.3]	A
Industrial control system	Sec 4, [6.2.4]	I
PRESERVATION		
Logs strategy	Sec 4, [7.1.1]	A
Logs architecture	Sec 4, [7.1.2]	A
MAINTENANCE		
Equipment Administration Guide	Sec 4, [8.1.1]	I
Equipment Operator Guide	Sec 4, [8.1.1]	I
MONITORING		
Events Manager **(2)**	Sec 4, [9.2.3]	A
Investigation manager **(2)**	Sec 4, [9.3.1]	A
(1) A: to be submitted for approval; I: to be submitted for information **(2)** May have to be recognized by the Society (see Ch 4, Sec 1, [1.1.3])		

Table 3 : Documentation to be submitted for CSR security mechanisms

Topic	Reference	A / I **(1)**
ARCHITECTURE		
Principle of information collection and processing	Sec 5, [2.1.6]	A
Inventory of collected information **(2)**	Sec 5, [2.1.6]	A
Software architecture **(2)**	Sec 5, [2.1.6]	A
SECURITY MECHANISMS		
System reliability mechanisms	Sec 5, [2.4.2]	I
Rules integrity mechanisms	Sec 5, [2.4.3]	I
Separated environments	Sec 5, [2.4.4]	A
System integrity mechanisms	Sec 5, [2.4.5]	A
Client protection mechanisms	Sec 5, [2.4.6]	A
Client integrity	Sec 5, [2.4.7]	A
Storage encryption mechanisms	Sec 5, [2.4.8]	I
Network encryption mechanisms	Sec 5, [2.4.9]	I
Removable medias protection	Sec 5, [2.4.10]	I
Access management	Sec 5, [2.4.11]	I
(1) A: to be submitted for approval; I: to be submitted for information **(2)** May have to be recognized by the Society (see Ch 4, Sec 1, [1.1.3])		

Table 4 : Documentation to be submitted for CSR user guide

Topic	Reference	A / I **(1)**
FUNCTIONALITIES		
Supervision and management	Sec 5, [2.2.1]	I
Alerting	Sec 5, [2.2.2]	I
Evaluating	Sec 5, [2.2.3]	I
Countermeasures	Sec 5, [2.2.4]	I
Evaluation of the vulnerability level	Sec 5, [2.2.5]	I
Equipment qualification	Sec 5, [2.2.6]	I
CSR integrity	Sec 5, [2.2.7]	I
Vessel integrity	Sec 5, [2.2.8]	I
IOC on-demand	Sec 5, [2.2.9]	I
MAINTENANCE		
SYSLOG management	Sec 5, [2.3.1]	I
Restoration procedures	Sec 5, [2.3.2]	I
Emergency procedures	Sec 5, [2.3.3]	I
Storage management procedures	Sec 5, [2.3.4]	I
Security events description	Sec 5, [2.3.5]	I
(1) A: to be submitted for approval; I: to be submitted for information		

Table 5 : Documentation to be submitted for IDG security mechanisms

Topic	Reference	A / I **(1)**
ARCHITECTURE		
Workflow and architecture **(2)**	Sec 5, [3.1.4]	A
SECURITY MECHANISMS		
Separated environments	Sec 5, [3.4.2]	A
System integrity mechanisms	Sec 5, [3.4.3]	I
Network protection	Sec 5, [3.4.4]	I
(1) A: to be submitted for approval; I: to be submitted for information **(2)** May have to be recognized by the Society (see Ch 4, Sec 1, [1.1.3])		

Table 6 : Documentation to be submitted for IDG User Guide

Topic	Reference	A / I **(1)**
FUNCTIONALITIES		
On-demand local scans	Sec 5, [3.2.1]	I
On-demand remote scans	Sec 5, [3.2.2]	I
IDG capture points	Sec 5, [3.2.3]	I
Automated remote scans	Sec 5, [3.2.4]	I
Extended IDG	Sec 5, [3.2.5]	I
ELR connection	Sec 5, [3.2.6]	I
MAINTENANCE		
SYSLOG management	Sec 5, [3.3.1]	I
Restoration procedures	Sec 5, [3.3.2]	I
Updates	Sec 5, [3.3.3]	I
Security events	Sec 5, [3.3.4]	I
(1) A: to be submitted for approval; I: to be submitted for information		

Table 7 : Documentation to be submitted for ELR security mechanisms

Topic	Reference	A / I **(1)**
ARCHITECTURE		
Workflow **(2)**	Sec 5, [4.1.4]	A
Architecture **(2)**	Sec 5, [4.1.4]	A
Supervision and management	Sec 5, [4.2.1]	I
Alerting	Sec 5, [4.2.2]	I
Recording **(2)**	Sec 5, [4.2.3]	A
SECURITY MECHANISMS		
Separated environments	Sec 5, [4.4.2]	A
Encryption	Sec 5, [4.4.3]	I
Storage	Sec 5, [4.4.4]	A
Integrity	Sec 5, [4.4.6]	A
Source authentication	Sec 5, [4.4.7]	A
Timeline	Sec 5, [4.4.8]	A
Events signature	Sec 5, [4.4.9]	A
Time synchronization	Sec 5, [4.4.10]	A

(1) A: to be submitted for approval; I: to be submitted for information
(2) May have to be recognized by the Society (see Ch 4, Sec 1, [1.1.3])

Table 8 : Documentation to be submitted for ELR User Guide

Topic	Reference	A / I **(1)**
FUNCTIONALITIES		
Events and logs recording	Sec 5, [4.2.1]	I
MAINTENANCE		
Records management	Sec 5, [4.3.1]	I
System restoration	Sec 5, [4.3.2]	I
Emergency procedures	Sec 5, [4.3.3]	I

(1) A: to be submitted for approval; I: to be submitted for information

Section 4 Additional Requirements for Type Approval of Security Solutions - Design Requirements

1 General

1.1 Application

1.1.1 Responsibilities

This Section applies to equipment suppliers and gives requirements for equipment design in terms of cyber security.

1.2 System integration

1.2.1 Description

When the equipment is part of a pre-integrated system (multiple equipment), a description of the system is to be submitted for information with the following elements:

- purpose of the system
- major requirements
- specific features
- connections (with other systems)
- listing equipment per equipment
- requirements regarding pre-integrated systems as defined in NR467, Pt C, Ch 3, Sec 3, [8].
- the network devices for Category II and III systems, as defined in NR467, Pt C, Ch 3, Sec 3, should be suitable for marine application and should be tested to requirements specified in NR467, Pt C, Ch 3, Sec 6.

  Wireless equipment should be designed and tested as per requirements specified in NR467, Pt C, Ch 3, Sec 6.

1.2.2 Architecture

A network scheme is to present the system with equipment. The network scheme is to be submitted for information.

1.3 Identification

1.3.1 Extensions

Extensions of some pieces of equipment are to be delivered for use by the security solutions mechanisms:

Cat. A equipment extensions are:

- operating system identification
- all applications (developed or off the shelf) and installed on the equipment
- all services (services listening for connections)
- databases (managed, stored and, or, accessed)
- distributed directory information services
- virtual machines and hypervisors

The list of extensions is to be submitted for information.

1.3.2 Security functions

Security functions are groups of security mechanisms implemented within an equipment.

The implementation of the following security functions is to be explained, detailed and justified:

- Development:

  Organisation of equipment protection during development phase.
- Protection:

  System hardening in order to manage integrity, confidentially and availability of code and related data. Protection apply on logical (operating system, services, application) and physical levels.
- Maintenance:

  Workflows and procedures to manage, update and restore equipment.
- Verification:

  Supervision used to check and validate the compliance of the equipment logical processes (operating system, application and services) and ensure they are in a proper state of functioning.

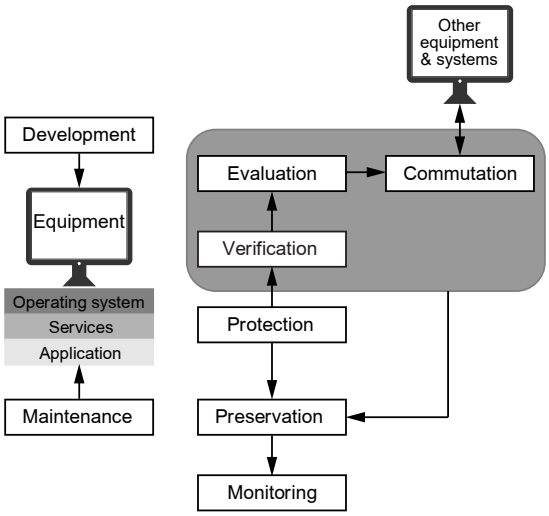
- Evaluation:
  Gate used to scan software, scripts and executable part of code for any malicious content.
- Commutation:
  Network and system services used to redirect information from, and to, the equipment to, and from, other equipment of the system and other systems of the ship.
- Preservation:
  Trace and record logs and events about protection, verification, evaluation, maintenance and commutation.
- Monitoring:
  Alerts at the attention of the cyber security officer in the security operation centre (ashore) and, or, the cyber security responsible (onboard).

For the security functions detailed hereafter, a rationale is to explain, detail and justify if the security functions are assumed by the equipment itself, relying on the system or relying on the vessel systems. Security functions may and should use, in preference, the global security functions used for the vessel (as explained in Compliance and Software Registry in Sec 5, [2]). Nevertheless if the system or equipment cannot exchange or share information with the vessel central system, it is to demonstrate that the equipment ensures the functionalities described in Sec 5 for the following elements:

- verification: Compliance and Software Registry
- evaluation: Intrusion and Decontamination Gate
- preservation: Events and Logs Recorder.

Deliverable: Security functions are to be submitted for approval.

Figure 1 : Equipment security functions



2 Development

2.1 Development platform

2.1.1 Risk analysis

The Supplier is to have and manage a risk analysis for his development platform. This risk analysis is to be reviewed regularly in accordance with the security policy of the company.

Deliverable: Information regarding the risk analysis, major threats and mitigation measures is to be submitted for approval.

2.1.2 Development platform

Commissioning processes should be provided by the systems provider so that testing can be carried out on live systems.

Equipment supplier ensures cyber security of its development by using a secured development platform: code repository, workstations update, servers protection, scans for malicious codes, CVE patch management, pen tests...

When cyber security products recognized by the Society are used (both software and hardware) for the protection of the development activity, a brief rationale explains their management regarding updates and monitoring.

Deliverable: A description of development platform security or the results of audits or a national or an international certification is to be submitted for approval.

2.1.3 Secure development

Developments of the equipment are to be secured though the application of a guideline.

Deliverable: A description of development security measures or the results of audits or a national or international certification is to be submitted for information.

2.1.4 Security assurance plan

Supplier provides a security assurance plan giving all the cyber security measures applied during development and maintenance. This document specifies organisational aspects, human responsibilities and technical means involved in the cyber security. This document is considered as a traceable engagement of responsibility from the supplier.

Deliverable: Supplier's security assurance plan is to be submitted for approval.

2.1.5 Audits

Supplier agrees to be audited by a third party accepted by the Society whom role will be to check compliance with Cyber Security Rules.

Deliverable: A result of audit or a national or an international certification is to be submitted for information.

2.2 Development principles

2.2.1 Principle of least privilege

In order to limit introduction of vulnerabilities in the software, the principle of least privilege is systematically to be used:

- regarding interfaces (accounts, opened ports, processes in memory, human interfaces...)
- regarding complexity in the software (use of libraries in cascade, unknown parts of software...).

Deliverable: A description of application of principle of least privilege is to be submitted for information.

2.2.2 Code robustness

Equipment supplier is to demonstrate how their development workflow ensure a state of the art in cyber security for the development themselves. Quality processes are to be explained. Technical processes used in order to detect malicious part of code, vulnerabilities and software security holes are to be addressed and demonstrated.

Deliverable: Tests results regarding robustness of the code are to be submitted for information.

2.2.3 SCADA systems

Development of good practices is to be defined, applied and verified. Compiler options involved in code improvement (safety and security) are turned on. For SCADA systems, options related to user warnings are activated as they reduce risk of software vulnerabilities.

Deliverable: Compilation rules for SCADA systems are to be detailed, explained and submitted for information.

2.2.4 Secure lifecycle

Regarding the code developed, the Supplier is to ensure security of the relevant technical documentation, source code during a period up to the end of life of the equipment. It means that vulnerabilities will not be published without a corrective patch, code will not be accessible for a public usage and technical aspects (interfaces, protocols...) will not be shared without authorization.

Deliverable: Secure lifecycle principles are to be submitted for information.

2.2.5 Software delivery

Before delivery, equipment software files (installation media, installation packages, operating systems, software) are to be inspected by an antivirus software in order to detect malicious parts of software.

Deliverable: Software delivery principles are to be submitted for information.

3 Protection

3.1 Context

3.1.1 Protection is defined during design phase of the equipment.

Protection of the equipment is in charge to:

- keep data in confidentiality.
- ensure the integrity of variables, configuration files and in-memory parameters
- ensure the integrity of functions (code execution)
- deliver the best level of service in term of code availability and, thus, the best level of effort in term of bug hunting to reduce the risk of code injection (denial of attacks, buffer overflows).

The protection applies to: operating system, services, application.

Protection uses logical or physical security mechanisms.

3.2 Hardening

3.2.1 Extensions hardening

For Level 3 equipment, extensions listed in [1.3.1] are hardened in respect of the principle of least privilege:

- operating system (e.g. Linux, Windows, etc.)
- database (e.g. MySql, Oracle, etc.)

- services (e.g. Apache)
- desktop application (e.g. any local application)
- web browsers (e.g. Internet Explorer)
- virtual machines (e.g. Virtualbox, Docker, etc.)
- distributed directory information (e.g. LDAP).

Hardening principles cover the following topics:

- identification and authentication
- users accounts and groups
- file system configuration (access control list)
- local and remote administration
- boot time security mechanisms
- services configuration, selection and filtering
- memory use, memory limitation
- network configuration and filtering
- auditing policy
- logging configuration
- maintenance operations
- useless components
- any other specific topic.

Note 1: CLIP OS or SELinux are two examples of hardened operating systems with implementation of the principle of least privilege.

Deliverable: For each extension hardening strategy is to be submitted for approval.

3.2.2 ICS hardening

A particular attention should be brought for OT systems hardening. For example:

- useless software, part of software, services, static or dynamic libraries, development code, development libraries, test environment are to be removed
- useless components shall be uninstalled as much as possible, deactivated:
  - default accounts, unused physical ports, unused removable supports, unused system process and services, debug tools, files, development on workstations and industrial controllers shall be deactivated
  - unused files and executables on workstations are to be delated
  - PDF files and reader on SCADA stations are to be delated.
- SCADA (Servers and System Control And Data Acquisition) are to be submitted with runtime only software and files
- if equipment requires development components (e.g. SNCC Control Command), mitigation measures shall be supplied in order to isolate workstation from irrelevant equipment of the network
- operator console have a visual identifier
- physical access restriction to CPU and PLC
- deactivation of remote programming mode
- client IP address restriction.

Deliverable: For ICS systems hardening strategy is to be submitted for approval.

3.2.3 Equipment hardening

Security mechanisms of Cat. A, Cat. B and Cat. C Level 3 equipment or system containing the equipment are approved by a third-party independent authority which ensures verification of the following topics, as far as possible:

- mechanisms on intrusion detection
- connection, communication encryption and firewalling rules
- local data encryption and deletion mechanisms
- protection against malwares and malicious codes
- equipment administration and supervision procedures
- account management, identification, authentication and access control
- physical security.

Deliverable: Security target and certificate of security for the Cat. B equipment is to be submitted for approval by the Supplier.

Note 1: Common criteria evaluation assurance Level EAL3+ is an example of certification.

3.2.4 Use of wireless

Wireless communication shall provide the capability to identify and authenticate all users (humans, software processes, or devices) Engaged in wireless communication (I.E 802.1X for Wi-FI) Wireless protocol that are not implementing such features shall be replaced, or not considered for transmitting control order. Wireless network shall be implement features related to authorization, monitoring and usage restriction according to commonly accepted security industry practices.

3.3 Access

3.3.1 Accounts and roles

For any equipment:

- Different kinds of accounts are used:
  - session accounts are authenticated sessions used to access to operating system
  - application accounts are used to access to application, to display information or to do actions
  - system accounts are used by applications, services and system to authorize sessions, execute software and to manage data both for storage and communications.
- Session and application accounts have separated roles defined for the following functions:
  - account administration
  - system administration
  - everyday maintenance
  - data backup
  - operational usages.

For Level 2 and Level 3 equipment:

- Equipment are designed for logical access with the principle of least privilege.
- Equipment cannot be accessed without authentication mechanism (identification and “password”).
- Equipment have a list of group of users with detailed privileges, directory access and roles. Each role, privilege, network, file and process access shall be justified.
- List of default and predefined accounts and/or groups is to be submitted. Relevant tests are to be submitted so that, at administrator level, usage of predefined accounts may be detected and action to erase them committed.
- Generic accounts shall not be used. When used, usage of generic accounts are justified and submitted for approval.
- Generic accounts with privileges are banned.

Deliverable: Rationale about users is to be detailed, explained and submitted for approval.

3.3.2 Passwords

For any equipment:

- Password are robust. Robustness of password depends of the system and shall be detailed by the supplier. Robustness shall be verified through comparison with password history, usage of a password complexity test and renewal of password at regular period (30, 60, 90 days...) If, for operational, safety or any other demonstrated reason, system have to be accessed without authentication, mitigation measures shall be proposed like physical access control, operation system hardening or limitation of functions.
- Equipment furnish procedures and tools to reset passwords.

For Level 2 and Level 3 equipment:

- Password are encrypted when sent over the network, sent to another process or stored.

Deliverable: Password policy is to be detailed, explained and submitted for approval.

3.3.3 Authentication

For every equipments: the equipment shall be able to prevent further access after a configurable time of inactivity or following activation of manual session lock. Session ID must be unique.

For Level 2 and Level 3 equipment:

- In case of authentication failure, a growing timeout may be used instead of account locking. This rule is recommended, not mandatory.
- The control system shall provide the capability to obscure feedback of authentication information during the authentication process.
- Software changes in systems (modification of data by service) should be secured by two-factor authentication.

For Level 3 equipment:

- A strong authentication shall be applied to equipment (e.g. OTP, smart card).

Deliverable: Authentication policy is to be detailed, explained and submitted for approval.

3.4 Physical security

3.4.1 Physical access

The following Rules apply to Level 3 equipment.

Hardware traps may be used by attackers in order to log keystrokes and record password or transmit them through the air. Traps are threats which can be covered by physical countermeasures and access restriction to hardware connectors like USB.

Equipment physical security is taken into account during design phase in order to lower threats like hardware trapping, robbery or malicious access to information:

- locked door for tower based computers
- locked external connections like usb, Ethernet, local console
- locked box
- lock or badge reader for ICS
- for light, portable or movable equipment, anti-theft mechanism shall be considered like anti-theft cable for laptop, screwed computers, locked cabinet and locked room for removable media storage.

Deliverable: The following topics are to be submitted for approval:

- description of security mechanisms (to the attention of administrators)
- description of mitigation measures (to the attention of cyber security officer)
- operating rules (to the attention of cyber security responsible and operating crew members).

3.4.2 Storage encryption

Physical supports and disks of Level 2 and Level 3 equipment are encrypted. At least, if file system doesn't handle encryption (ICS for example), sensitive and configuration files shall be encrypted or, at least, not clearly written.

Deliverable: Encryption mechanisms strategy and tools are to be submitted for approval.

3.4.3 External connections

The following Rules apply to Level 3 equipment.

- Each usage of external connection is detailed (e.g. USB, Ethernet, Bluetooth ports...).

Deliverable: External connections are to be detailed and submitted for information.

3.4.4 Renewable media usage

The following Rules apply to Level 3 equipment:

- removable media usage is restricted by configuration and use of operating system level mechanisms, BIOS restriction, dedicated software or physical locks
- removable media are natively encrypted except in case of justified operational usage.

Deliverable: Removable media usage and policy are to be explained and submitted for information.

3.4.5 In-operation security

The following rules apply to Level 3 equipment while in-operation:

- critical families of operations are defined for equipment.

A control panel is installed on the bridge and linked to the system in order to visually status the use of critical equipment (e.g. with a red, green signal):

- in proper state (usable) - for example green signal
- at risk (e.g. loss of compliance) - for example yellow signal
- in maintenance (unavailable, cannot be used) - for example red signal.

During Critical operations:

- any local or remote maintenance operation on the equipment is banned
- onboard, the Master can physically turn off any way to gain remote access to the equipment
- during critical operations, the Master turns off remote access to the equipment by using the mechanisms hereinbefore delivered
- after critical operations, the Master turns back on remote access to the equipment
- mechanisms hereinbefore delivered disconnect any network link. The mechanisms is physical and may be an electrical relay or a manual procedure
- the equipment shall provide the capability to display a system use notification message before authenticating. The system use notification message shall be configurable by authorized personnel
- 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.

Deliverable: Procedures and mechanism regarding maintenance during critical operations are to be detailed and submitted for approval.

3.4.6 Remotely controlled systems

The following rules apply to Level 3 equipment using remote control system over networks.

The objective of this rule is to guarantee the safety of delivery of the service of a system in case of failure or compromise of the remote systems used to control the main system:

- remotely controlled systems are to be controlled locally by the use of a Human Machine Interface (HMI)
- local control systems are to be of a robust design suitable for the environmental exposure and the intended operation
- local control systems are to be self-contained and not depend on other systems or external communication links for its intended operation
- facilities for selecting “local” at or near the system is to be provided. When local control is selected, any control signal(s) from the remote control system are to be ignored.

Note 1: Note regarding propulsion: A single failure in a local control system should not cause loss of the system function. For single-engine plants, this normally implies that component redundancy shall be arranged. For multiple engine plants with independent local control systems, the objective could be satisfied provided minimum manoeuvrability for the safe operation of the vessel is maintained after a single failure.

Note 2: Note regarding auxiliary services: For electrically driven units in auxiliary services, the local control should normally be arranged at the motor starter in MCC's and, if applicable, also near the EUC. For machinery systems which due to their complexity requires continuous automatic control, manual control of the individual EUC's may not be feasible. In such cases, local means shall be provided to both monitor the concerned process- and to enable/disable any automatic functions / modes (a typical example is the gas supply system to a gas fuelled engine).

Deliverable: Design, mechanisms and procedures regarding remotely controlled systems are to be detailed and submitted for approval.

4 Verification

4.1 Context

4.1.1 Verification covers solutions in charge to check elements from the equipment regarding a previous, accepted, status.

4.2 Equipment compliance

4.2.1 Compliance and software registry

Compliance of Level 3 equipment is verified by using an automated solution.

Compliance in defined in [2.1.1].

The scope of the compliance covers any elements of the equipment and extensions listed in [1.3.1].

Elements of integrity used by the solution rely on those defined in [4.3].

Depending of the choice regarding security function for verification [1.3.2], the automated solution may be:

- The compliance and Software Registry solution already installed in the vessel under authority of the system integrator. In that case, equipment guarantees implementation of the CSR mechanism which may be:
  - a dedicated service installed in the equipment which sends, upon CSR request, information to the central unit in charge to centralize information and monitor alerts
  - a dedicated software installed in-memory of the equipment which sends information to the CSR in charge to centralize information and monitor alerts
  - a local classical service dedicated which answers to local CSR requests through SSH, SNMP.
- An independent compliance solution designed by the Supplier in respect of Sec 5 Rules regarding Compliance and Software Registry security solution.

For unconnected, standalone Level 3 equipment, an autonomous, standalone and embedded component installed in the memory of the equipment which triggers human readable alerts is accepted. In case of loss of compliance, human readable alerts could be done:

- through an analogic relay (visual, noisy)
- through a computer screen as long as this screen is reliable and always turned on.

Deliverable: Compliance and Software Registry Interfaces are to be submitted for approval to Society.

4.3 Elements of integrity

4.3.1 Deliverable

Deliverable: Elements of integrity as explained in [4.3] are to be submitted for approval to Society.

4.3.2 Compliance integration

Elements of integrity are defined and selected by the Supplier, independently of the solution used onboard to verify compliance of the equipment.

Elements of integrity are a list of sensitive elements defined by the Supplier on which compliance may rely on in order to detect unauthorized changes on the equipment.

Elements of integrity are listed exhaustively, independently of how it will be used.

4.3.3 Operating systems

Elements of integrity for operating system are to be submitted by the Supplier of Cat. A equipment to master compliance monitoring and reveal any loss of integrity at operating system level.

To achieve this, a detailed list of expected compliance for operating systems, installed components and applications is to be submitted and must include items from the following list:

Scope of compliance for hardened systems and application:

- Any element from [3.2].

Scope of compliance for files:

- operating system detailed version number
- desktop applications installed by the operating system with their detailed version number
- software preinstalled from operating system, manually installed, developed by third party, provided by software editors or simple off-the-shelf component: name, installation date, version, file path.
- mounted volumes and filesystem type and information
- filesystem contents, with directories, files, access controls, sizes, time stamps and file signatures
- filesystem and files encryption when handled at operating system level.

Scope of compliance for operating system configuration:

- supplier-defined sensitive applications and related executable files, configuration files, hives (e.g. Windows Registry)
- accounts, privileges and groups and all elements relevant with access control lists (e.g. file access)
- security and audit policies.

Scope of compliance for network usage:

- network and system services installed by the operating system with their detailed version number.
- connections listed with origin/destination information (e.g. mac ip address, port number,) when they are:
  - listening: accepting connections
  - outgoing: opening outgoing connections from the equipment to another one
  - local only: internal to internal process.
- network shared and mounted volumes
- remotely logged on users.

Scope of compliance for physical components (as they are seen from the operating system):

- network interfaces identifiers (e.g. MAC address)
- identifiable physical components (e.g. chipset)
- identifiable physical support installed (e.g. disk drive, removable media)
- identifiable components checksums (e.g. BIOS (Basic Input/Output System), UEFI (Unified Extensible Firmware Interface))
- USB (Universal Serial Bus) activity history
- removable media usage
- restriction or limitation and any other kind of serial link usage.
- locally logged on users.

Scope of compliance for memory usage:

- running processes, memory access controls, process sizes, relevant process time stamps, relevant process activity and process hashes.
- executed shell commands.

4.3.4 Services

Web Services are process listening for network connections. They can be provided by operating system or installed from a third party software editor, developed and so on.

Compliance of those components is based upon the clear definition of elements defined in [4.3.3]:

- version information
- files restrictions
- process restrictions
- network restrictions
- accounts restrictions.

4.3.5 Databases

Database (e.g. mySQL, Oracle...) means any organized collection of data.

Compliance of those components is based upon the clear definition of elements defined in [4.3.3]:

- version information
- files restrictions
- process restrictions
- network restrictions
- accounts restrictions (administrators, operators and backup operators).

A dedicated section details compliance of databases permissions, users and configuration:

- Access Control from User Table
- Encryption and key management.

4.3.6 Distributed directory information services

Lightweight Directory Access Protocol (Microsoft Active Directory, Open LDAP...) is the industry standard application protocol for accessing and maintaining distributed directory information services.

Compliance of those components is based upon the clear definition of elements defined in [4.3.3]:

- version information
- files restrictions
- process restrictions
- network restrictions
- accounts restrictions (administrators, operators and backup operators)

A dedicated section details compliance for additions, deletions, and changes in LDAP directory services.

4.3.7 Hardware integrity

When available, CSR receives SMART (Self-Monitoring, Analysis and Reporting Technology) or SNMP indicators from equipment to evaluate level of hardware integrity on physical support.

Physical support installed (e.g. disk drive, removable media) may also be checked as required part of the equipment.

4.3.8 Cat. B equipment

Cat. B elements of integrity are to be submitted by the Supplier to master compliance monitoring and reveal any loss of integrity of the appliance.

Cat. B equipment may use, for example, configuration profiles or system firmware by comparing version numbers and checksums.

Network equipment such as routers, firewalls may have a detailed list of expected compliance:

- access control list to network
- serial interfaces and removable media
- configuration files, environment variables; any other information of interest relevant to network appliance compliance.

4.3.9 Cat. C equipment

Cat. C elements of Integrity are to be submitted by the Supplier to master compliance monitoring and reveal any loss of integrity of a single equipment or a whole system.

Cat. C equipment, when available, have a detailed software listing with roles, configuration advices, manufacturers and security management.

The compliance check may use:

- ICS name, brand, model or reference (some devices (e.g.modular PLCs) contain several references
- ICS version of the embedded firmware
- ICS system messages, registry keys
- ICS product version if appropriate
- network interfaces identifiers (e.g. MAC address)
- flow matrix with source, destination
- protocol (e.g. modbus, TCP)
- protocol information (e.g. ports, service)
- programmed support checksums.

4.3.10 Virtual machines

As a virtual machine is considered as an equipment, equipment using virtual machines have to apply the whole scope of Rules of this Section to each virtual machine.

4.3.11 Hypervisors

Hypervisors are processes managing virtual machines.

Compliance of those components is based upon the definition of elements defined in [4.3.3] applied to the hypervisor itself. In example, compliance of network components apply to virtual networks managed by the hypervisor.

For this reason, [4.3.3] fully apply but from an hypervisor point of view. Sensitive files take into account:

- virtual machines profiles (containing virtual hardware definition, virtual disk file path)
- virtual networks (mounted by the hypervisor to connect:
  - virtual machines to virtual machines
  - virtual machines to external networks.

4.3.12 Antivirus

Antivirus is a sensitive process which may stay updated and activated. Any deactivation is detected. Compliance tool shall pay a particular attention to antivirus integrity of the software regarding its binaries, configuration and signatures files on disk and its processes in memory.

Compliance of antivirus is based upon the clear definition of elements defined in [4.3.3]:

- version information
- files restrictions
- process restrictions
- network restrictions
- accounts restrictions.

4.3.13 Other references

The system integrator shall also include the following elements (as defined in Ship Rules, Pt C, Ch 3, Sec 3), depending of their availability and impact in case of loss of integrity:

- about network equipment: any desktop applications information
- about equipment software:
  - any desktop applications information
  - any network and system services information
- about system hardware: any integrated system component information.

5 Evaluation

5.1 Global

5.1.1 Principle

When introduced in an equipment, transmitted by or executed by, parts of code and software may contain malicious part of code. The evaluation is in charge to check those elements and to protect equipment from those threats.

5.1.2 IDG usage

Usage of an Inspection and Decontamination Gate (IDG) depends of the vessel's Integrator as explained in Sec 5, [3.1.3].

5.1.3 Antivirus usage

Usage of an antivirus solution is mandatory on equipment, unless otherwise specified.

Usage of an antivirus solution is banned on Level 2 and Level 3 equipment insuring real-time control of critical operations. In this case mitigation measures are in place to control the risk of logical access to the equipment.

5.2 Antivirus

5.2.1 Deliverable

Deliverable: Antivirus mechanisms as detailed in [5.2] are to be submitted for approval.

5.2.2 Antivirus software

Equipment have an antivirus solution capable of malicious signatures recognition (anti-key loggers, anti-malware, anti-spyware, anti-virus) and malicious behaviour recognition (heuristic analysis).

5.2.3 Antivirus activation

Antivirus cannot be deactivated or uninstalled by users. Antivirus is launched with system rights. Antivirus action or deactivation requires highest administrative privileges.

Antivirus is launched with operating system before local or network, user or system access to system

6 Commutation

6.1 Network policy

6.1.1 Commutation map

For Level 2 and Level 3 equipment, a map of network connection details:

- incoming and outgoing connections
- involved interfaces and networks
- involved processes and services
- list, location and roles of other equipment.

Deliverable: Equipment connectivity through cabled or wireless networks is mastered, detailed and submitted for approval by the Supplier.

6.1.2 Connection inactivity

Level 3 equipment is to propose a delay to ensure the client or server a function to close the connection after this period of inactivity while saving critical resources.

Deliverable: Rules about equipment connection management are to be submitted for information.

6.1.3 Communication encryption

To defeat packets replay over the network, Level 2 and Level 3 equipment network communications are encrypted.

Unsecured protocols are banned (HTTP, FTP (File Transfer Protocol)...) and replaced by secured one (HTTPS, SFTP (Secure File Transfer Protocol)…) in order to guarantee integrity, confidentiality, non-repudiation and authenticity.

In case of technical constraint, other secured system (e.g. Virtual Private Network) are to be submitted as mitigation measures.

Deliverable: Equipment network encryption policies are to be submitted for approval.

6.2 Industrial Control Systems (ICS)

6.2.1 Engineering workstation

Network activities of engineering workstation of OT systems are dedicated to engineering activities.

6.2.2 Operator console

Network activities of operator consoles of OT systems are dedicated to maintenance and operations activities.

Level 2 and Level 3 operator consoles are connected to OT and IT identified networks only.

6.2.3 Administration workstation

Network activities of administration workstations of OT systems are dedicated to administration of infrastructure equipment.

Administration workstation are not used for permanent monitoring.

6.2.4 Deliverable

Deliverable: ICS network policy is to be submitted for information.

7 Preservation

7.1 Context

7.1.1 Logs strategy

At both operating system and application level, equipment use an events and logs policy for extensions as defined in [1.3.1].

For Cat. A, Cat B and Cat. C equipment, the following list gives a scope of events to identify:

- authentication (e.g. login failure, success, user log off)
- accounts management (e.g. user add, delete)
- audit records (e.g. use of privileges)
- administrator actions (e.g. sudo)
- services activities (e.g. started, stopped)
- object access denied
- significant operational events (e.g. engine stopped)
- system activity (e.g. storage events)
- traffic events (e.g. blocked, allowed)
- usage information (e.g. PLC relay activation)
- USB usage.

Cat. B equipment, especially security and network appliances, feed an uninterrupted logging system of events related to their own cyber security and to the function for which they are designed.

Logs and events policy is built in respect of legal regulations and in respect of privacy.

The capability to allocate audit record storage capacity according to commonly recognized recommendations for log management shall be described in policy. Auditing mechanisms shall be implemented to reduce the likelihood of such capacity being exceeded.

Deliverable: Equipment events and logs management policy is to be submitted for approval by the Supplier.

7.1.2 Architecture

At both operating system level and application level, equipment records logs locally.

SYSLOG service is linked to vessel's Events and Logs Recorder (ELR), when available.

Deliverable: Equipment events and logs architecture are to be submitted for approval by the Supplier.

8 Maintenance

8.1 Context

8.1.1 Deliverables

Two documents are to be submitted by the Suppliers:

- An Equipment Administration Guide (see [8.2]):

  This guide is dedicated to the equipment, or system when integrated, and explains administration of the equipment in its relevant context. Administration guide discuss about operations with the highest level of privilege like system restoration, forensics investigation, software installation.
- An Equipment Operator Guide (see [8.3]):

  This guide is dedicated to the ship and explain operational actions for the equipment with the relevant context. Operator guide discuss about operations without the highest level of privilege: users creation, system backup.

Beyond hereinafter requirements, each guide contains administration and maintenance procedures relevant to the equipment

Deliverable: The Equipment Administration Guide and the Equipment Operator Guide are to be submitted for information.

8.2 Administration guide

8.2.1 Administration roles

Administration guide is to detail equipment administration roles and responsibilities for operation with high level of privilege like system restoration, forensics investigation, software installation, etc.

8.2.2 Administration procedures

Supplier is to deliver procedures related to the administration of the equipment.

8.2.3 Installation procedures

Level 2 and Level 3 equipment are to supply procedures and tools to quickly reinstall system by using pre-installed components (disk images) and installation scripts.

Level 3 equipment are to supply procedure and tools to verify equipment compliance after reinstallation.

8.2.4 Compliance state retrieval

Level 3 equipment are to supply procedure and tools to reinstall equipment at configuration level up to last secured and validated equipment version number.

8.2.5 CSR usage

When used, Compliance and Software Registry (CSR) is to be maintained with software updates. The procedure is to be explained.

Supplier's process and rules update procedure are to be submitted in the administration guide. The procedure about how-to get updates is to be submitted.

8.2.6 Vulnerabilities management

Vulnerabilities management take CVE into account and propose a way to properly and securely update systems.

This management is to be explained with manual and automated procedures.

Supplier is to propose a way to inform Shipowner about patch to apply as soon as its equipment, or system, contain a published CVE.

Identified vulnerabilities are to be patched when possible (availability of patch) by following the Supplier's prescriptions.

8.2.7 Advanced persistent threats mitigation measures

Level 3 equipment have a regular manual control procedure in order to help to reduce the impact of undetected advanced persistent threats, performance degradation and remaining vulnerabilities impact.

8.2.8 Hardened operating systems

Level 3 equipment Cat. A operating system are to be hardened with dedicated security rules. Supplier gives procedure of control in regard to applied rules. Tests in order to verify hardening are to be described through a step-by-step procedure. Procedure may be scripted.

8.2.9 Hardened equipment

Supplier is to provide tests in order to verify hardening by a step-by-step procedure for Level 3 equipment Cat. B and Cat. C.

8.2.10 Technical competencies

Supplier is to identify and to provide the necessary technical competencies of the service technicians.

8.3 Operator guide

8.3.1 Maintenance roles

Maintenance guide is to detail equipment maintenance roles and responsibilities for each operation: backup operations, account create, etc.

8.3.2 Maintenance procedures

Each equipment of vessel's inventory is to propose a dedicated and detailed Maintenance Plan.

For maintenance convenience, Supplier contact is to be submitted with useful internet links to website containing technical documentation, data, software maintenance, support and updates. For specific systems, technical contact, email and/or phone number are added.

Supplier is to deliver procedures related to the maintenance of the equipment.

8.3.3 Antivirus maintenance

Equipment antivirus solution is to be kept updated in accordance with cyber security officer recommendation by using a secured update mechanism ensuring integrity of data.

For maintenance operations, antivirus updates are to be available from operator level.

Access to antivirus may be controlled, incorporating the principle of least functionality. A procedure is to be submitted with equipment for cyber security responsible attention. It delivers step by step procedure to verify proper state of antivirus in terms of users' access and privileges.

8.3.4 Integrity check

For Level 2 and Level 3 equipment, procedures for manual verification of the integrity of the equipment are to be submitted. Manual action are to be submitted as script, command lines or software interface checking.

Those procedures may be used, for example, after software updates or to lift doubts of equipment compromising:

- Integrity check is to determine the scope and risks associated to a software maintenance and identify the objectives of testing, the method of testing, the expected time and resources required for the testing process. It should provide clear information on how the tests are carried out and how to verify the success or failure of each tests.
- Test cases are to be selected on the basis of requirements, design specifications, risk analysis and interfaces of the equipment subject to software maintenance.
- The results of the executed tests are to be recorded, including the versions of the software under tests.

8.3.5 Isolation

During Level 3 equipment maintenance operation, crew members have a way to be informed not to use the system or equipment. The way they can be informed may be:

- Organizational: procedures are in place to turn off logical or physical access to the system or equipment.
- Technical: an analog relay is used to unplug the system or equipment from any user action.

8.3.6 Backup procedure

A backup procedure is to be explained for Level 2 and Level 3 equipment in order to save sensitive files, systems and assets. For sensitive information, this procedure is restricted in terms of account rights for operator: operator shall have a backup profile meaning capability to backup files without reading, modifying or written backup files.

8.3.7 Antivirus usage

Maintenance is to use an antivirus solution or the vessel's IDG in order to verify contents and archive results of the operation in the vessel maintenance registry.

8.3.8 Urgent update

Procedures and technical functions are to ensure urgent update of Level 2 and Level 3 equipment without loss of operation in progress. If required by operations, equipment could have to be in the same operational state after reboot (without loose of context). For Cat. C equipment, automate outputs may be in a saved state during software update.

8.3.9 Data providers

When used, usage of data imported from data providers is to be explained. Imported data is to carry out data production and distribution operations in accordance with a quality system, covering:

- data quality (production, delivery, testing and integration)
- standardization of data import
- means to ensure the continuous availability of data maintenances
- prevention/detection/protection from unauthorized modification
- prevention of the distribution of malware.

If used, data providers procedures related to the maintenance of the equipment are to be delivered.

9 Monitoring

9.1 Architecture

9.1.1 Monitoring solution

Monitoring solution is a security solution used by the Shipowner, aboard or, and, ashore, in order to supervise security events. Monitoring solution rely on two monitoring functions installed in the equipment by the Supplier:

- Events Manager is used to log and record events.
- Investigation Manager is used by the monitoring solution to remotely retrieve logical elements of the equipment.

9.1.2 Events manager

Events Manager term is used hereinafter according to one of those definitions:

- equipment send events to ELR when available.
- equipment record events in a local registry

Events Manager is mandatory for Level 2 and Level 3 equipment.

9.1.3 Investigation manager

Investigation Manager term is used hereinafter according to one of those definitions:

- equipment use the CSR client application which ensures the functionalities herein described
- equipment use its own application which ensures the functionalities herein described

Investigation Manager is mandatory for Level 3 equipment.

9.2 Events manager

9.2.1 Events description

Level 2 and Level 3 equipment are to supply a clear description of security events with their code number, diagnostic description and resolution methodology.

Level 3 equipment extensions (Operating systems, Directory Services, Web services, Databases, Desktop Application, Hypervisors, Antivirus) are to be submitted with a security events referential including code number, diagnostic description and resolution methodology.

Scope of alerts is extended to any relevant suspicious network activity (e.g. port scan) well-known and handled by active software of the network facility.

Deliverable: Security Events are to be submitted in the Equipment Administration Guide.

9.2.2 Security thresholds

Scope of events and number of authorized login failures before alert generation are to be defined. Alert means local visual local alert, potential account freezing, log message and access blocking (local growing timeout or remote for the incriminated source).

Deliverable: Security events are to be submitted in the Equipment Administration Guide.

9.2.3 Events record

Events listed in the scope defined in [9.2.1], are to be recorded to the event Manager defined in [9.1.2].

Deliverable: The method used to manage and record events, when available and feasible, is to be submitted for approval.

9.3 Investigation manager

9.3.1 List of supplied elements

Upon security monitoring request, equipment is to supply:

- Software components with a list of:
  - firmware version and checksum
  - component installation timestamps
  - file repository
  - version information for operating system or installed software handled by the operating system components.
- Configuration components with a list of:
  - configuration files
  - environment variables
  - scripts
  - registry
  - hives for operating system component or installed software handled by the operating system.
- Files components with a list of:
  - mounted volumes
  - directories
  - files names and paths
  - files access controls list
  - files sizes
  - files time stamps
  - files checksums.
- Configuration components with a list of:
  - network mounted volumes
  - opened ports
  - listening applications
  - outgoing connections.
- Serial interfaces components with a list of:
  - Universal serial bus activity history.
- Memory components with a list of:
  - running processes
  - memory access controls
  - process sizes
  - process time stamps
  - process activity
  - process hashes
  - memory dump.

Deliverable: The method used to supply, when available and feasible, elements and list of elements is to be submitted for approval.

10 Security Settings

10.1 Equipment security settings

10.1.1 Operating system security settings

Security settings may address the following topics: system services, accounts, local policies, audit policies, events logs management, file access control list, network interfaces configuration, network filtering.

The objective is to master the security mechanisms which are in place and to be able to propose a way to continuously upgrade and enhance security of the equipment.

Security Settings are selected from [4.3].

Note that some of those software elements are susceptible to change during life cycle of the equipment: minor or major updates and other patch management operations change software elements. But, at this point, those software elements must be not be excluded.

In example, here is a non-exhaustive list of elements to rely on:

- Files monitoring includes any file system, mounted volumes, directory, files and their access controls list, sizes, time stamps and checksums. Sensitive files are specified: configurations files, environment variables, hives any other files of interest relevant to operating system.
- Connections monitoring includes network mounted volumes, services, protocols, opened ports, listening applications and outgoing connections.
- Serial interface monitoring mechanisms includes USB (Universal Serial Bus) activity, removable media usage, restriction or limitation and any other kind of serial link usage.
- Memory monitoring handled by the operating system includes running processes, memory access controls, process sizes, relevant process time stamps, relevant process activity and process hashes.

10.1.2 Features security settings

Cat. B and Cat. C Features Security Settings are a set of elements of Integrity.

This set of elements is to be delivered by the system integrator to monitor compliance and reveal any loss of integrity.

Those elements may be, when available:

- features configurations (built on elements listed in [10.1.4])
- system firmware (used to compare version numbers or checksums)
- equipment self-tests procedures or any integrated integrity checking tool
- equipment physical configuration (OT safety switches)
- equipment configuration:
  - Cat. B network equipment such as routers, firewalls may have a detailed list of expected compliance:
    - access control list to network, serial interfaces and removable media
    - configuration files, environment variables.
  - any other information of interest relevant to network appliance compliance.
- security settings may address the following topics:
  - system services
  - accounts management
  - local policies
  - audit policies
  - events logs management
  - network Interfaces configuration
  - network filtering.

10.1.3 Antivirus installation

There are two ways to considerer the notion of antivirus solution.

- Either it is a classic antivirus solution, meaning installed as an application managed by the operating system of the equipment.
- Either the antivirus solution is a remote mechanism as the one described Sec 5, [3.1.3] or directly inspired by this definition.

In the first case, when installed in the equipment, the following requirements are to be followed:

- antivirus cannot be deactivated or uninstalled by users
- antivirus is launched with system rights
- antivirus action or deactivation requires highest administrative privileges
- antivirus is launched with operating system before local or network, user or system access to system.

10.1.4 Features configuration

For each of them, the following elements, when available, are explained:

- roles (description of needs, objectives and data processing)
- connections (listening, outgoing or system only) - listening means accepting connections, outgoing means opening outgoing connections from the equipment to another one, system only refers to internal processes
- access rules (local or remote) - local means that the function can only be managed from a local console
- accounts (administration, running, operation) - administration is the highest privileged access, running is a system oriented account and operation is linked to an operational human user.

Deliverable: Topics regarding Cat. B and Cat. C features configurations are to be detailed, explained and justified.

Section 5 Specific Requirements for Compliance Software Registry (CSR), Inspection and Decontamination Gate (IDG) and Events and Logs Recorders (ELR)

1 General

1.1 Application

1.1.1 Scope

Security solution requirements apply to Suppliers of security equipment, security systems and security services.

1.1.2 Objective

The objective of security solutions is to cover the following security functions, as required in Sec 4, [1.3.2]:

- Verification:
  used to check and validate the compliance of the equipment.
- Evaluation:
  used to scan software, scripts and executable part of code for any malicious content.
- Preservation:
  used to trace and record logs and events.

1.1.3 Definition

The three security solutions are installed onboard and, or, ashore in order to achieve security functions objectives:

- Verification:
  covered by the CSR which is an anti-tamper technology installed to prevent changes in operation and/or to detect attacks before/during their occurrence. Defined in Article [2].
- Evaluation:
  covered by the IDG (Inspection and Decontamination Gate) which is an anti-malware technology used to detect malicious signatures, suspect behaviours and indicators of compromise during attacks. Defined in Article [3].
- Preservation:
  covered by the ELR (Events and Logs Recorder) which is a forensic technology used to determine paths of attacks and responsibilities after attacks and before during their occurrence. Defined in Article [4].

1.1.4 Grouped hunting

The vessel's cyber strategy shall privilege cyber joined operations for the vessel and the fleet. To achieve this objective, integration of components is decided at design phase with the following interactions as requirements:

- Compliance and Software Registry sends suspected files to IDG in order to scan their contents. In return, IDG delivers an applicable score of risk.
- Compliance and Software Registry sends logs of actions, requests and results to the ELR.

1.1.5 Grouped defence

The three security solutions have to consider their self-protection and interact between each of them in order to complete the vessel's cyber strategy:

- IDG and ELR are checked by the CSR as any equipment and, when compromised, will be detected by the CSR as it.
- IDG and CSR events are traced by the ELR as any equipment and, when compromised, will be under investigation by using ELR history.
- CSR and ELR are maintained through the IDG as any equipment and, when in maintenance, are under evaluation of the IDG.

1.1.6 Integrated architecture

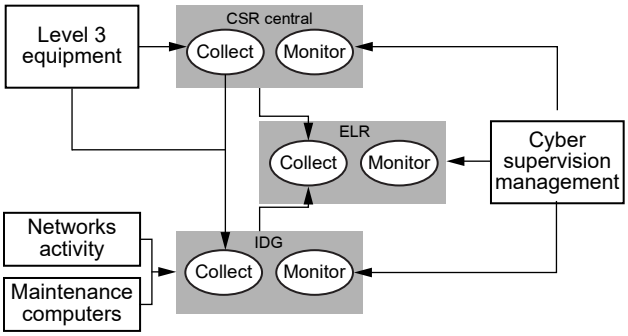
The system integrator is in charge of implementing a strategy of integration for the security solutions (see Fig 1) by using grouped hunting [1.1.4] and grouped defense [1.1.5] concepts.

The strategy considers the scope of elements identified during the Cyber Risk Assessment for:

- Level 3 equipment
- Network activities of Level 3 systems and remote access networks
- Computers and removable media coming from outside of the vessel and used for maintenance operations.

Deliverable: Integrated architecture of security solutions is to be submitted for information by the ship integrator in the ship cyber design.

Figure 1 : Integration of security solutions



2 Compliance and Software Registry (CSR)

2.1 Mechanisms

2.1.1 Definition

Compliance verifies that an equipment is in proper state from a numeric point of view.

The proper state defines the prerequisite, condition and criteria in which hardware, software, variables and data cannot jeopardize functions of the system either for safety or operational reasons.

Thus, the proper state also defines the prerequisite, condition and criteria in which hardware, software, variables and data are known to be in good condition to successfully accomplish operational mission in the respect of safety regulations.

2.1.2 Objectives

The objective of the CSR is to maintain the good shape and the proper state of the ship digital components embedded in systems.

The CSR is a central unit, collecting information from clients and reacting in case of loss of compliance of an equipment.

The CSR is the guardian of the initial, authorized, proper state.

Any alteration on any digital component is sent to the CSR in order to compare, record and raise alerts.

A reliable CSR covers the following cyber challenges:

- FIM (File Integrity Monitoring)
- maintenance operations logging
- configuration compliance monitoring
- process management
- network flows activity.

The CSR respect integrated architecture of security solutions defined by the system integrator in [1.1.6].

2.1.3 Workflow

CSR equipment is used in order to collect equipment compliance information and manage the software registry of the related equipment.

As the main goal of the CSR is to provide a simplified, smart and trusted information at the crew members, the complexity scale should go down as we approach end users.

CSR is, ideally, an appliance, onboard and or remote, which is used to receive information from systems during their runtime.

- Ideally, in the first time, equipment suppliers are to harden systems and integrate traceability components as detailed in Sec 4. Equipment information are sent in CSR database to formalise the related security framework: operating systems, services and applications are hardened, sensitive components are highlighted (e.g. system files or configuration values). Then, rules are supplied.
- In a second time, Shipyard is to integrate equipment with the CSR solution. It is also a good moment to build a “zero state” of the ship and backup every digital support delivered. “Zero state” is sent to the CSR equipment in order to handle system modifications. Digital setting is qualified.
- In a third time, covered equipment are in use at sea and they feed CSR. Changes are to be continuously recorded and changes are computed.
- In the same time, maintenance teams and crew are to respect organizational security rules while using, modifying or updating any equipment. Any legitimate and justifiable technical modification, update, upgrade or alteration is duly signed by the operator and endorsed by the CSR.

- In conclusion, before going at sea, and at sea, CSR is to detect any failure. Crew is to be informed in as soon as alert has been raised up. Any alert, even if cleared, is to be recorded for further maintenance operation at shore.

The compliance flow is structured in order to answer to what, when, who, where, how and why.

2.1.4 Active architecture

Implementation may be under the form of a service installed on each equipment. Each equipment delivers a compatible flow of information ensuring CSR requirements hereinafter described. This flow comes from a tool, a process, respecting rules detailed in this Section (see Fig 2):

- Cat. A operating systems include a security solution in charge of feeding the compliance flow towards the CSR. The CSR client sends packets to CSR central by using UDP transport protocol. A dedicated separate network (e.g. VLAN) is used to collect information.
- CSR management connects to the central by TCP on a separate network (e.g. VLAN).

Collect and monitor services in the CSR central run in separated environments (e.g. separated system accounts, separated virtual machines.)

CSR client furnishes elements to identify integrity of the protected scope. Elements used may be any element of integrity as defined for equipment design (see Sec 4, [4.3]).

The active architecture may also address request to Cat. B equipment such as network switches and firewalls in order to retrieve information regarding Rules in operation. In that case, the collectors use a dedicated separated network (e.g. VLAN) and a secured protocol (e.g. SSH) to connect and get information. (See Fig 3).

Figure 2 : Active architecture example

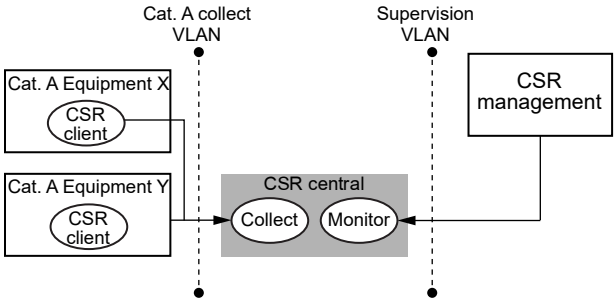
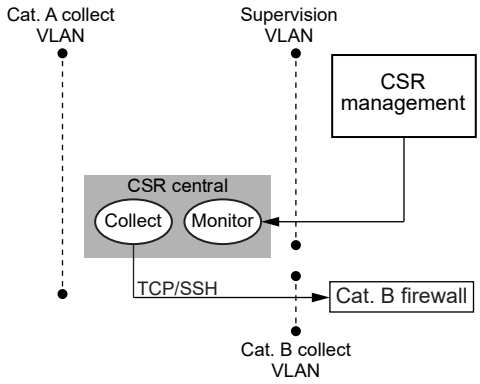


Figure 3 : Cat. B architecture example



2.1.5 Passive architecture

For Cat C equipment, and particularly for OT automation (e.g. PLCs, remote I/O, sensors, actuators, variable speed drives, meters, circuit breakers, switches, physical servers), a passive architecture is recommended to retrieve information regarding the equipment.

The principle of passive discovery probes apply for both OT and IT networks and for Cat. A, cat. B and Cat. C equipment.

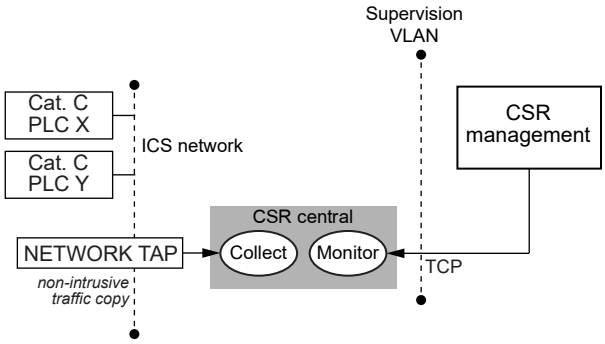
Active architecture is unfeasible on OT equipment because of their opacity, age or natural limitations. The use of a probe connected to the network, through a non-intrusive network tap mechanism, deep packet inspection or port spanning implementation, covers the issue (see Fig 4).

Collect and monitor services in the CSR central are to be executed in separated environments (e.g. separated system accounts, separated virtual machines).

CSR management connects to the central server by TCP on a separate network (e.g. VLAN).

Elements collected through passive architecture may be any element of integrity defined by the equipment itself (see Ch 2, Sec 2, [4.3]).

Figure 4 : Passive architecture example



2.1.6 Submission

Deliverable: Principles of information collection and processing, inventory of collected information and CSR architecture are to be submitted for approval in the documentation describing CSR security mechanisms.

Note 1: Collected information, passive and active architecture may have to be provided by a third-party recognized by the Society (see Ch 3, Sec 1, [1.1.3]).

2.2 Functionalities

2.2.1 Supervision and management

As described in [2.1.3], CSR proposes an external interface to supervise and manage assets, software and every collected information.

Management is to be allowed to request database regarding assets and software for both current and past situations.

Supervision and management functions are proposed through a human interface (http, local).

Procedures details, at a minimum:

- how to access software registry information. For example, procedure to get an inventory of assets; procedure to add a client to the CSR; procedure to export, delete information.
- how to make advanced requests (e.g. like sql language, regular expression). For example, advanced requests may be used to get list of computers having such operating system, or to get versions number of such application or number of assets connected on the network.
- how to manage (list, create, modify, delete) compliance profiles. For example, procedure to modify a compliance profile; procedure to add or to modify files to be checked; procedure to add or to modify or any other relevant information from [2.1.3].
- how to supervise compliance management. For example, procedure to add or modify rules regarding compliance checking; procedure to have rules to enable the early prevention and/or detection and subsequent timely reporting of unusual and/or abnormal activities that may need to be addressed.
- how to detect maintenance operations on equipment.
- how to map and monitor network activity.
- how to make requests about alerts. For example, how to search for alerts regarding loss of compliance.

Software Registry management procedures are to be are to be provided in a CSR User Guide to be submitted for information (see [2.2.11], [2.3.6] and Sec 3, Tab 4.

2.2.2 Alerting

CSR automatically reports any loss of compliance on any equipment, depending of the configuration done through the supervision interface.

Alerts threshold are managed through the same interface.

The reported alerts are, at least, under the following formats: on the screen (web page over http), by an email alert, with a sound alert.

Alerts are sent to the vessel's ELR, when available.

Automated alerts are configured through a human interface (http, local).

2.2.3 Evaluating

CSR is linked to the ship's IDG when available.

If a suspicious binary file or process has been found on an equipment, element is sent to the IDG to evaluate the risk.

Suspicious binary files may be unknown patterns like file hash absent from white and black lists.

IDG may propose different typologies of analysis: multiple sources of signatures, threat intelligence, IOC, advanced heuristic probes and behaviour analysis engines.

Procedures are to detail, at a minimum:

- how to detect, how to classify and how to manage suspicious components - with or without IDG.
- how to connect to the IDG, how to configure transfers over the network, how to retrieve results and how to manage both automatic and manual processing.

2.2.4 Countermeasures

In case of loss of compliance, client may be deactivated, disconnected or banned from the system and/or the network.

Action could also be to block network activity (source, destination) from workstation and/or from a linked active network facility like IPS or FW.

Procedures details delivered tools on how to manage situation in case of loss of compliance.

2.2.5 Vulnerability level

CSR automatically displays level of threat by using updated CVE database confronted to equipment operating system and application version information.

The User Guide contains automatic and manual procedures to check the level of vulnerability of a single equipment, a whole System or the vessel.

2.2.6 Equipment qualification

CSR can be used to easily check equipment compliance in the following situations:

- in case of after re-installation of the equipment: CSR is to be used to validate the compliance of the new installation.
- in case of emergency or disaster on an equipment: CSR is to offer a way to validate baseline information from new equipment. CSR is to be used to validate that the new system actually corresponds to a safe and secure pre-emergency state of equipment.
- in case of software update: CSR is to identify, track and report successful or rejected changes. CSR is to be used in the framework of quality with a process of reporting.

2.2.7 CSR integrity

CSR detects changes of its own configuration (rules, configuration, bios). A GUI or command line tool is provided to verify and validate integrity and reliability of:

- CSR central unit
- compliance controls (e.g. daemons, services) installed on Cat. A
- compliance solutions for Cat. B and Cat. C equipment.

2.2.8 Ship integrity

A function in CSR helps to validate the full scope of equipment covered by the compliance process vessel integrity. A GUI proposes to check the compliance for the full scope of equipment.

2.2.9 IOC on demand

IOC templates are to be usable by CSR for on-demand detection purpose with collected and stored information

2.2.10 Investigation manager

Elements of the equipment as defined in Sec 4, [9.3.1] may be retrieved by the CSR Management.

2.2.11 Deliverable

Deliverable: Procedures regarding functionalities described hereinbefore are to be submitted in the CSR User Guide.

2.3 Maintenance

2.3.1 SYSLOG management

Security events issued by CSR are to be compatible with SYSLOG format.

Security events are both internal events (CSR equipment security events) and client events (loss of compliance of a monitored equipment).

A procedure explains how to configure, to activate and to route the SYSLOG events.

2.3.2 System restoration

Procedures for diagnostic, reinstallation and restoration of the equipment, system or solution are to be written to the attention of operators.

2.3.3 Emergency re-installation

Should an actual emergency or disaster occur on CSR, a procedure is to exist to explain the recovery of the system, the reporting of test results and, according to the results, implementation of an action plan.

2.3.4 Storage management

An alert is to be raised up to security operation centre, the cyber security officer and the cyber security responsible as soon as the alert threshold of CSR storage capacity is reached.

CSR storage capacity is to be upgradable.

Procedures are to explain, at a minimum, how to manage CSR storage capacities issues at sea, how to upgrade storage capacity and how to manage alerts regarding storage management.

2.3.5 Security events description

CSR is to be submitted with a security events referential including code number, diagnostic description and resolution methodology. Scope includes CSR itself, loss of compliance events and any security events.

2.3.6 Deliverable

Deliverable: Procedures regarding maintenance requirements described hereinbefore are to be submitted in the CSR User Guide.

2.4 Security mechanisms

2.4.1 Equipment security

Equipment Security Rules defined in Ch 4, Sec 2 fully apply to CSR.

Equipment security mechanism rules, as defined in [2.4.2] to [2.4.11], are to be submitted (see Sec 3, Tab 3).

2.4.2 System reliability

CSR is to be reliable. Reliability mechanisms, as hardware as software, are explained.

2.4.3 Rules integrity

CSR is to embed its own integrity checksum regarding compliance information transportation. This checksum is used by CSR to validate received information integrity.

2.4.4 Separated environments

Collecting and monitoring services in the CSR central server are to be executed in separated environments (e.g. separated system accounts, separated virtual machines.)

2.4.5 System integrity

CSR is to own its integrity checksum. This checksum is to be used by CSR to validate its system integrity.

Audit process is accurate, complete, timely, authorized and auditable.

2.4.6 Client protection

CSR client components installed on Cat. A equipment are to be installed at kernel-level in a protected process, running with independent execution condition.

CSR components installed on Cat. A equipment are to be launched with operating system before local or network, user or system access to system.

CSR client process are to be activated at any time.

2.4.7 Client integrity

Should an actual emergency or disaster occur on CSR, equipment hosting CSR client process is to have a cache and retry mechanisms.

2.4.8 Protected storage

CSR data storages are to be enciphered with a strong encryption mechanism.

2.4.9 Network protection

CSR network protocol is to use a strong encryption mechanism. Encryption keys are managed by the CSR solution itself. Keys are never to be shared on any other equipment.

2.4.10 Removable media protection

CSR removable media are to be protected and their use restricted according to media restriction rules described in relevant chapter. CSR removable media usage is to be restricted by configuration and use of operating system level mechanisms, BIOS restriction, dedicated software or physical locks.

2.4.11 Access protection

Number of authorized login failures to the facility before alert generation is to be defined.

Alert means security event generation, message and local/remote access locking for the incriminated source.

3 Inspection and Decontamination Gate (IDG)

3.1 Mechanisms

3.1.1 Definition

The IDG is used to scan any equipment for malware and malicious behaviours.

Scope of application is:

- equipment processes
- equipment virtual machines processes
- removable media
- maintenance laptops, computers.

3.1.2 Objectives

IDG is to be proposed onboard in order to inspect any equipment before their use on onboard (e.g. maintenance laptops, BYOD (Bring Your Own Device)):

- through a cabled or wireless network connection (laptop, computers, mobile phones or tablets, diagnostic tools)
- with a physical and local connection on equipment (usb keys, removable media, hard drives).
- the IDG respects Integrated Architecture of Security Solutions defined by the system integrator (see [1.1.6]).

3.1.3 Workflow

IDG can be developed under different formats of logical and physical architecture. The objective is to propose a way to cover a selection of workflows from the following list:

- Requests for analyse which come from the network:

  Analyse may connect to a mounted point, a file directory, one or more files, a process. Elements may be files signatures (hashes) or files themselves:

  - from compliance and registry: automatically (e.g. api mode)
  - from an equipment: automatically (e.g. script mode) or on-demand (e.g. web interface).
- On the fly analyse of network packet:

  A network tapping device gets flow of information on the network and, by using deep packet analyse, extracts binary contents and patterns for analyse (see Fig 5).
- Requests for analyse directly issued by physical interface of an equipment:

  Elements may be USB keys, DVD, memory cards, USB disk, Hard disk and solid state drives (see Fig 6).

3.1.4 Submission

Deliverable: IDG Workflows and Architecture are to be submitted for approval.

Note 1: Workflows and architecture may have to be provided by a third-party recognized by the Society (see Ch 4, Sec 1, [1.1.3]).

Figure 5 : IDG active and passive a IDG architecture

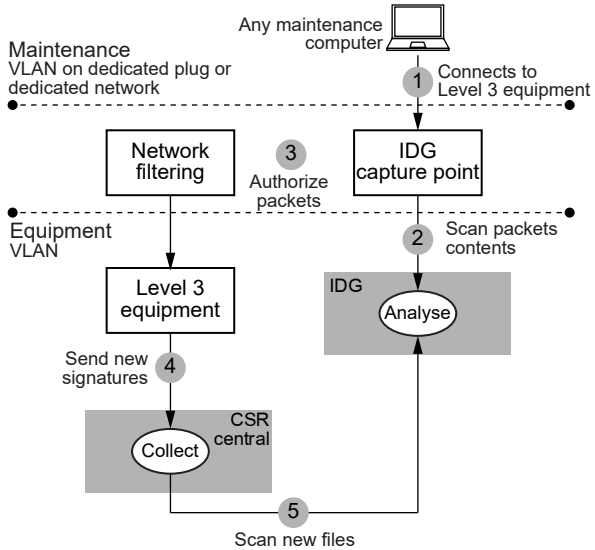
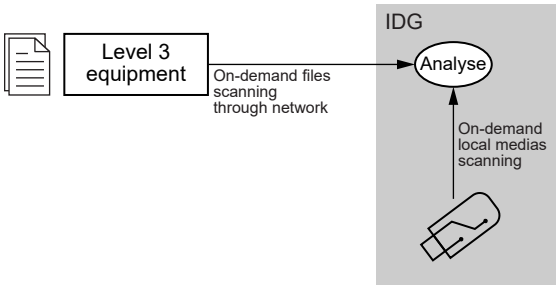


Figure 6 : IDG on-demand scanning



3.2 Functionalities

3.2.1 On demand local scans

For local media scanning (e.g. USB keys, see Fig 6), during inspection, a scoring is to be displayed on a screen and/or printed on a certificate in order to evaluate risk of infection contained on the media.

A decontamination process is to be proposed to the user through a GUI.

If accepted, IDG will try to clean/remove infected files.

At the end, a new inspection process is to be launched. Cleaned and removed files are to be saved in quarantine space on IDG system.

3.2.2 On demand remote scans

A secure web interface is to be proposed on the IDG to remotely send files or mounted volumes for Inspection.

After Inspection, a scoring to evaluate risk of infection contained files is to be displayed on the interface.

3.2.3 IDG capture points

IDG capture points are facilities which deliver on the fly files inspection services. Files are to be analysed over the network through a deep inspection packet process which looks for malware signatures and malicious behaviour.

3.2.4 Automated remote scans

A secure network interface is to be proposed on the IDG to remotely send files for Inspection. Request may come from an IDG capture point or the CSR Central (see Fig 5).

After Inspection, a scoring to evaluate risk of infection contained files is sent to the emitter.

3.2.5 Extended IDG

IDG is to propose an enhanced surface of detection:

Multiple probes (antivirus software) or sandboxes or behaviour detection tools could be used. In cyber operations, files and processes are typically sorted in black and white lists:

- the white ones are well-known and are trusted
- the black ones are well-known as being threats, malwares or virus
- a third category appears, grey signatures, which are not yet categorized.

The not yet categorized shall be inspected through different ways in order to score them and evaluate the situation.

Onboard, such analysis is possible by using online or offline multiple antivirus probe systems (i.e IRMA). Those probes, may contain multiple antivirus systems.

Endpoint or network sandbox may join the IDG to open up unknown files and check behaviour. Based on what they see, network sandboxes will block, allow or quarantine the files.

Analyse workflow may be linked.

3.2.6 ELR connection

Security events (success, alerts) issued by the IDG are to be sent to ELR when available.

3.2.7 Deliverable

Deliverable: Procedures regarding functionalities described hereinbefore are to be submitted for information in the IDG User Guide.

3.3 Maintenance

3.3.1 SYSLOG management

Security events issued by IDG are to be compatible with SYSLOG format.

Security events are both internal events (IDG equipment security events) and client events (e.g. virus detection).

A procedure is to explain how to configure, to activate and to route the SYSLOG events.

3.3.2 System restoration

Procedures for diagnostic, reinstallation and restoration of the equipment, system or solution are to be written to the attention of operators.

3.3.3 IDG updates

Procedures for automated and manual updates of IDG are to be submitted.

3.3.4 Security events

IDG is to be submitted with a security events referential including code number, diagnostic description and resolution methodology.

Scope includes IDG itself and any security relative events detected by IDG about binaries, known risks, unknown risks or suspicious system activity.

3.3.5 Deliverable

Deliverable: Procedures regarding maintenance requirements described herein before are to be submitted for information in the IDG User Guide.

3.4 Security mechanisms

3.4.1 Equipment security

Equipment Security Rules defined in Ch 4, Sec 2 fully apply to IDG.

3.4.2 Separated environments

IDG connectors used to collect information, probes used for analyse and supervision interface are to use strong separated and safe logical environments (e.g. separated virtual machines).

3.4.3 System integrity

IDG is to own its integrity checksum. This checksum is to be used by IDG to validate its system integrity.

Audit process is to be accurate, complete, timely, authorized and auditable.

3.4.4 Network protection

IDG network protocol is to use a strong encryption mechanism. Encryption keys are to be managed by the IDG solution itself. Keys are not shared by any equipment.

3.4.5 Submission

Deliverable: Procedures regarding security mechanisms described hereinbefore are to be submitted for information in the IDG User Guide.

4 Events and Logs Recording (ELR)

4.1 Mechanisms

4.1.1 Definition

The objective of the ELR is to record security events, activity events and systems logs coming from Cat. A, Cat. B or Cat. C equipment and systems. Logs are to be stored with a high level of security in order to have a legal proof in case of investigation during any security event.

A reliable ELR is to cover most of the following cyber challenges:

- access and security events
- system life logs
- maintenance operations logs
- compliance events.

Events are important sensitive events regarding known and expected situations (e.g. authorized or refused login).

Logs are important traces about activities which may cover situations which are not traced by Events (e.g. identification bypass through code injection).

4.1.2 Workflow

Events and logs are generated and delivered by many equipment. The most popular protocol used for logs transmission is SYSLOG, a standard for message logging. The objective of ELR is not to reinvent the wheel but to propose a central unit (e.g. using SYSLOG) to equipment onboard in order to collect equipment events.

When stored, events and logs may be used:

- locally by the cyber security responsible
- remotely, from a remote operation centre by the cyber security officer
- remotely, when stored in a SIEM (Security Information and Event Management)
- regularly, events and logs are copied in a safe place ashore.

Events and logs are then used in case of:

- suspicious of cyber event
- malicious attack discovery
- major advanced persistent threat.

The purpose of events and logs is:

- technical investigations
- responsibilities identification.

4.1.3 Architecture

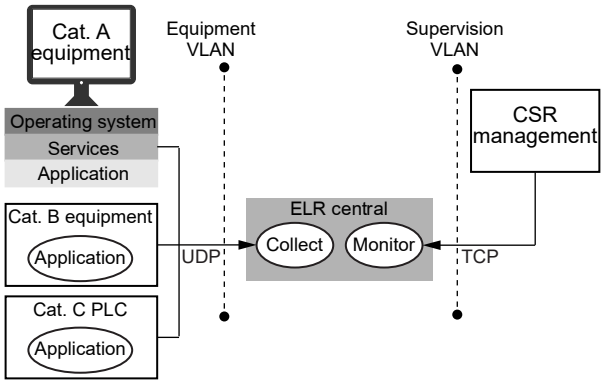
The ELR architecture is simple in term of collect as it only requires to receive information from any equipment. The only point is that events and logs shall be copied in a safe from a remote location, in preference (see Fig 7).

4.1.4 Submission

Deliverable: Workflows and ELR architecture are to be submitted for Approval in the documentation describing ELR security mechanisms.

Note 1: Workflows and architecture may have to be provided by a third-party recognized by the Society (see Ch 4, Sec 1, [1.1.3]).

Figure 7 : Example of ELR architecture



4.2 Functionalities

4.2.1 Supervision and management

The ELR is to propose an external interface to supervise and manage every collected events.

Management is to be allowed to configure ELR behaviour.

Supervision and management functions are proposed through a human interface (http, local).

Procedures are to detail, at a minimum:

- how to access events.
- how to make advanced requests (e.g. like sql language, regular expression). For example, advanced requests may be used to get list of such event).
- how to supervise events collections. For example, procedure to add or modify rules regarding sources of acquisition and file formats.
- how to set up levels and threshold for alerts. For example, how to send an alert regarding such event.

4.2.2 Alerting

The ELR automatically is to report any kind of event as determined at supervision level for any equipment.

The reported alerts are to be, at least, under the following formats: on the screen (web page over http), by an email alert, with a sound alert.

4.2.3 Recording

ELR is to receive all events and logs feeds from all the equipment and record them in a way they can be easily analysed by standard logs analyse systems.

4.2.4 Deliverable

Events and Logs Recorder procedures are to be submitted for information in the ELR User Guide (see Sec 3, Tab 8).

Other Procedures regarding functionalities described hereinbefore are to be submitted as per Sec 3, Tab 7.

Note 1: File format used to record events may have to be recognized by the Society (see Ch 4, Sec 1, [1.1.3]).

4.3 Maintenance

4.3.1 Records management

ELR storage is to be copied in a safe place. A function is to explain how to proceed to copy and to verify integrity of the images.

Copies may be done in a remote location through network connection at quay, or by using a box extraction system with a rotation of storage between the vessel and ashore operation centre (e.g. removable media).

4.3.2 System restoration

Procedures for diagnostic, reinstallation and restoration of the equipment, system or solution are to be written to the attention of Operators.

4.3.3 Emergency procedures

Procedures for emergency extraction of records are to be detailed with location to the equipment.

4.3.4 Deliverable

Deliverable: Procedures regarding maintenance requirements described hereinbefore are to be submitted for information in the ELR User Guide (see Sec 3, Tab 8).

4.4 Security mechanisms

4.4.1 Equipment security

Equipment security rules defined in Ch 4, Sec 2 fully apply to ELR.

4.4.2 Separated environments

ELR connectors used to collect information and supervision interface are to use strong separated and safe logical environments (e.g. separated virtual machines.)

4.4.3 Encryption

ELR uses approved encryption mechanism in order to ensure confidentially and integrity of the storage. As much as possible, in order to ensure integrity of information transfer, events and logs are to be encrypted during network transmission.

4.4.4 Storage

ELR is to use a storage mechanism in order to manage storage space issues and backup of history.

4.4.5 Visual identification

Central unit containing recorders is visually identifiable (e.g. orange coloured box).

Removable media location is visually identifiable (e.g. black arrows with safety message).

4.4.6 Integrity

ELR is to guarantee safety of recorded information. The process in charge of writing files is to be at system level.

Nor administration profiles nor operators profiles shall have other access right than read access.

Backup operator is not to have read access right.

4.4.7 Source authentication

ELR is to use an approved authentication mechanisms in order to guarantee origin of information.

4.4.8 Timeline

ELR is to monitor the IT infrastructure and store events logs to enable the reconstruction, review and examination of the time sequences of operations and the other activities surrounding or supporting operations.

4.4.9 Events signature

Recorded information from ELR are to be used as a legal proof in case of need. Recording events are hashed, building a sealed signature.

Events signature and related timestamps are to be recorded in a safe place, assuring authenticity of the events and logs repository.

4.4.10 Time synchronization

ELR is to use approved, synchronized and independent time feed in order to guarantee logs and events timestamp.

4.4.11 Submission

Deliverable: Procedures regarding security mechanisms described hereinbefore are to be submitted for approval in the ELR User Guide.

CHAPTER 6
SURVEY OPERATIONS

Section 1 General

1 Surveys and survey operations

1.1 Survey

1.1.1 Purpose

The purpose of this Chapter is to give details on the scope of surveys of ships assigned an additional class notation **CYBER MANAGED**, **CYBER RESILIENT** or **CYBER SECURE** which need specific requirements to be verified for the maintenance of the notations.

1.1.2 Initial surveys

Granting of the additional class notation **CYBER MANAGED** is subject to:

- compliance with the requirements of Chapter 2.
- an initial survey detailed in Tab 1.

Granting of the additional class notation **CYBER RESILIENT** or **CYBER SECURE** is subject to:

- compliance with the requirements of Chapter 3 or Chapter 4 as applicable
- a successful initial survey detailed in Tab 2.

1.1.3 Surveys for maintenance of the notations

In accordance with the requirements of NR467, Pt A, Ch 5, Sec 17, [1] and NR467, Pt A, Ch 2, Sec 2, the maintenance of the additional class notation **CYBER MANAGED**, **CYBER RESILIENT** or **CYBER SECURE** is subject to compliance with:

- Annual survey as defined in [2]
- Intermediate survey as defined in [3]
- Class renewal survey as defined in [4].

for which the applicable documentation as defined in [1.1.4] is to be submitted for approval by the Surveyor.

1.1.4 Required documentation for maintenance of the notations

As specified in:

- Ch 2, Sec 1, [2.2] for the additional class notation **CYBER MANAGED**
- Ch 3, Sec 1, [2.2], for the additional class notation **CYBER RESILIENT**
- Ch 4, Sec 1, [2.2], for the additional class notation **CYBER SECURE**.

The required documentation for surveys defined in [1.1.3] are:

- the Cyber Handbook,
- the Cyber Inventory, and
- the Cyber Security Policy.

The documentation specified in this Chapter is to be supplied and maintained during the whole lifecycle of the vessel.

The documentation is to be readily available for examination by the Surveyor.

1.1.5 Surveys procedures

Surveys procedures are a set of the following procedures:

- monitoring procedures, defined in Sec 2
- infrastructure procedures, defined in Sec 3]
- equipment procedures, defined in Sec 4
- maintenance procedures, defined in Sec 5.

The survey procedures are applied onboard under responsibility of the Shipowner by:

- Shipowner teams
- Third-party partner

Note 1: Third-party partner may have to be recognized by the Society (see Ch 4, Sec 1, [1.1.3]).

1.1.6 Survey process

The survey procedures is to verify:

- the good functioning of monitoring procedures
- the level of cyber security of infrastructure
- the level of cyber security of equipment
- the good functioning and efficiency of maintenance procedures

For this purpose, surveys consist of a set of test cases defined in:

- Sec 2, [2] for monitoring procedures
- Sec 3, [1] for infrastructure procedures
- Sec 4, [2] for equipment procedures
- Sec 5, [2] for maintenance procedures

1.2 Cyber survey Application

1.2.1 Application

The scope of application depends on:

- technical scope which may be: Remote access systems, Level 1 systems, Level 2 systems, Level 3 systems, wireless networks or cabled infrastructure. The scope of application covers every equipment connected, connectable or involved as for management, administration, operating or use.
- the applicable classification notation (**CYBER MANAGED**, **CYBER RESILIENT** or **CYBER SECURE**)
- survey type (initial, annual, intermediate or renewal) - survey operations are required by the applicable classification notation.

1.2.2 Scope of survey

The scope of survey is defined from the compliance scope and refined in Chapters dedicated to Initial survey, Annual Survey, Intermediate Survey and Class Renewal Survey.

Depending of the context, the surveys may:

- define test case which address only a representative sample of the scope of survey
- apply to the full scope of survey.

The requested topics are summarized in:

- Tab 1 for the additional class notation **CYBER MANAGED**
- Tab 2 for the additional class notation **CYBER RESILIENT** or **CYBER SECURE**.

Table 1 : Summary of survey process for ships assigned the notation CYBER MANAGED

Survey procedures and survey process	Reference	Type **(1)**	Initial survey	Surveys for maintenance of the notation **CYBER MANAGED**		
				Annual survey	Intermediate survey	Class renewal survey
Monitoring procedures						
Compliance testing	Sec 2, [2.1]	S	X	X	X	X
Equipment accounts testing	Sec 2, [2.2]	S	X		X	X
Remote access events testing	Sec 2, [2.3]	S	X	X	X	X
Wireless events testing	Sec 2, [2.4]	S	X		X	X
Infrastructure procedures						
Cabled networks	Sec 3, [1.2]	S	X		X	X
Remote access robustness	Sec 3, [1.3]	S	X	X	X	X
Remote access logging	Sec 3, [1.4]	S	X	X	X	X
Wireless networks robustness	Sec 3, [1.5]	S	X	X	X	X
Equipment procedures						
Accounts security settings	Sec 4, [2.1]	D	X			
Features security settings	Sec 4, [2.3]	D	X			
Antivirus solution	Sec 4, [2.4]	D	X	X		X
Software maintenance	Sec 4, [2.5]	D	X	X		X
Maintenance procedures						
Recovery plan testing	Sec 5, [2.1]	D	X			X
Maintenance protection tests	Sec 5, [2.3]	D	X	X	X	X
Wireless patch management	Sec 5, [2.4]	D	X	X		X
(1) S: document to be submitted for approval; D: Document to be delivered						

Table 2 : Summary of survey process for ships assigned notation CYBER RESILIENT or CYBER SECURE

Survey procedures and survey process	Reference	Type (1)	Initial survey	Surveys for maintenance of the notations **CYBER RESILIENT** or **CYBER SECURE**		
				Annual survey	Intermediate survey	Class renewal survey
Monitoring procedures						
Compliance testing	Sec 2, [2.1]	S	X	X	X	X
Equipment accounts testing	Sec 2, [2.2]	S	X		X	X
Remote access events testing	Sec 2, [2.3]	S	X	X	X	X
Wireless events testing	Sec 2, [2.4]	S	X		X	X
Infrastructure procedures						
White box testing	Sec 3, [1.1]	S	X	X	X	X
Cabled networks	Sec 3, [1.2]	S	X		X	X
Remote access robustness	Sec 3, [1.3]	S	X	X	X	X
Remote access logging	Sec 3, [1.4]	S	X	X	X	X
Wireless networks robustness	Sec 3, [1.5]	S	X	X	X	X
Black box penetration tests	Sec 3, [1.6]	D	X			
Equipment procedures						
Accounts security settings	Sec 4, [2.1]	D	X			
Operating systems security settings	Sec 4, [2.2]	D	X			
Features security settings	Sec 4, [2.3]	D	X			
Antivirus solution	Sec 4, [2.4]	D	X	X		X
Software maintenance	Sec 4, [2.5]	D	X	X		X
Maintenance procedures						
Recovery plan testing	Sec 5, [2.1]	D	X			X
Compliance update	Sec 5, [2.2]	D	X			
Maintenance protection tests	Sec 5, [2.3]	D	X	X	X	X
Wireless patch management	Sec 5, [2.4]	D	X	X		X

(1) S: document to be submitted for approval; D: Document to be delivered

2 Annual survey

2.1 Scope of survey

2.1.1 Documents to be submitted

The following documents are to be submitted:

- Cyber Inventory, if modified
- Cyber Handbook, if modified
- Cyber Policy, if modified
- test plans or test results, if modified.

2.1.2 Surveys

The annual surveys are summarized in:

- Tab 1 for the additional class notation **CYBER MANAGED**
- Tab 2 for the additional class notation **CYBER RESILIENT** or **CYBER SECURE**

3 Intermediate survey

3.1 Scope of survey

3.1.1 Documents to be submitted

The following documents are to be submitted:

- Cyber Security Policy, if changed
- Cyber Handbook, if changed

3.1.2 Surveys

The intermediate surveys are summarized in:

- Tab 1 for the additional class notation **CYBER MANAGED**
- Tab 2 for the additional class notation **CYBER RESILIENT** or **CYBER SECURE**

4 Class renewal survey

4.1 Scope of survey

4.1.1 Documents to be updated

The following documents are updated:

- Cyber Risk Assessment.

Regarding Level 2 and Level 3 equipment only, the following documents are updated:

- Cyber Inventory (systems identification part).

4.1.2 Documents to be submitted

The following documents are to be submitted:

- Cyber Security Policy, if changed
- Cyber Handbook, if changed

4.1.3 Surveys

The class renewal surveys are summarized in:

- Tab 1 for the additional class notation **CYBER MANAGED**
- Tab 2 for the additional class notation **CYBER RESILIENT** or **CYBER SECURE**

Section 2 Monitoring Procedures Survey

1 Definition

1.1 Monitoring procedures

1.1.1 Monitoring procedures are procedures used onboard by the cyber security officer and, or, cyber security responsible to check security of the systems.

These procedures are to be detailed in the Cyber Security Policy document and rely on Cyber Handbook.

The objective of this survey is to verify the good functioning of randomly selected monitoring procedures and the relevance of those results.

2 Checking monitoring procedures

2.1 Compliance testing

2.1.1 Context

Compliance of the systems is checked by the cyber security Officer by using compliance monitoring procedures.

Compliance monitoring procedures are part of the Cyber Handbook (see Ch 1, Sec 6, [3.1.1] and Ch 1, Sec 6, [3.2]).

2.1.2 Technical scope

Defined by the compliance monitoring procedures.

2.1.3 Evaluation criteria

Survey is successful when the compliance monitoring procedures are well known and correctly implemented by the relevant crew.

2.2 Equipment accounts testing

2.2.1 Context

Accounts monitoring are part of cyber security responsible duties (see Ch 1, Sec 6, [3.2.9]).

The objective of the Survey is to verify consistency of the hereinbefore procedure.

2.2.2 Technical scope

The scope of this Survey apply to at least Level 3 Equipment.

2.2.3 Test result

Cyber Handbook procedures and survey operation are to be compared and gaps are to be highlighted.

2.2.4 Evaluation criteria

The survey is successful when the comparison reveals no gap between Cyber Handbook procedures and Survey operation.

2.3 Remote access events testing

2.3.1 Context

The remote access systems and equipment are defined in the Cyber Inventory in the “Remote Access” Section as defined in Ch 4, Sec 2, [7.1.3]

Depending of the architecture, the technologies and the threats, security events are recorded.

Monitoring of “Remote Access Events” records is explained in the Cyber Handbook (see Ch 1, Sec 6, [3.2.5]).

The objective of this Survey is to validate the good functioning of the procedures described in the dedicated section of the Cyber Handbook.

2.3.2 Technical scope

This Survey applies to Level 3 Equipment only.

2.3.3 Evaluation criteria

The Survey is successful when the relevant procedures from the Cyber Handbook are known and correctly implemented by the dedicated crew

2.4 Wireless events testing

2.4.1 Context

The wireless systems and equipment are listed in the Cyber Inventory document under “Network” Section.

Depending of the architecture, the technologies and the threats, security events are recorded.

Monitoring of “Network Events” records is explained in the Cyber Handbook (see Ch 1, Sec 6, [3.2.6]).

The objective of this Survey is to validate the good functioning of the procedures described in the dedicated section of the Cyber Handbook.

2.4.2 Technical scope

This Survey applies to Level 3 Equipment only.

2.4.3 Evaluation criteria

The Survey is successful when the relevant procedures from the Cyber Handbook are known and correctly implemented by the dedicated crew

Section 3 Checking Infrastructure Cybersecurity

1 Checking Infrastructures procedures

1.1 White box testing

1.1.1 Context

Objective of white box testing is to deliver a health check-up of systems and equipment by using all the information regarding the vessel (e.g. Cyber Inventory) in one hand and, in other hand, to use cyber expertise and knowledge of testers.

1.1.2 Technical scope

The technical scope of white box testing applies to:

- any system or equipment using or involved in remote access
- any system or equipment using or involved in wireless networks
- any system or equipment involved in the network management and security of cabled networks
- any Level 3 equipment of Cat. A, Cat. B and Cat. C.

1.1.3 Test case

By using Cyber Inventory information, a procedure of tests is to be written to:

- check exposure to Common Vulnerabilities and Exposures on operating systems, applications, automation and all network equipment.
- detect presence of known indicators of compromise on Cat. A, Cat B and Cat. C equipment.
- verify integrity of system architecture (e.g. authorized equipment, number of automation, version, etc.)
- search for configuration errors in networks filtering and routing.

Tests are to be non-intrusive and non-destructive. Tests are to be submitted and approved by Society.

1.1.4 Test results

Tests results details applied procedures, tools and methods. An evaluation of the level of security is to be submitted.

1.1.5 Evaluation criteria

The Society evaluates the success of the test regarding the technical scope, the effort (e.g. number of tests), the quality (e.g. technics and tools) and the results.

1.2 Cabled networks

1.2.1 Context

Cabled networks are living part of the infrastructure:

- every day, equipment are connected, disconnected, added, deleted, moved.
- during maintenance operation, network configurations may be changed.

This survey proposes tests to compare onboard cabled networks installation with elements declared in the Cyber Inventory.

1.2.2 Test case

The test case is to rely on the network cartography delivered in the Cyber Inventory as defined in Ch 1, Sec 2.

Test case is to propose an active network scanning (e.g. network scanners or penetration tests) conducted in the cabled networks to ensure that the principles of isolation defined in the architecture are respected.

Tests may use tools, be scripted, or written with a check list of commands to type in console mode during the survey.

Tests are to be launched from different location of the system in order to survey the different paths of weakness and attacks (e.g. in front of and behind a firewall).

Tests are to be non-intrusive and non-destructive. Tests are to be submitted and approved by Society.

1.2.3 Test results

Results are to be compared with the network cartography of the Cyber Inventory in order to find consistency between the two documents.

1.2.4 Evaluation criteria

Survey is successful when network cartography of the Cyber Inventory is consistent with the Results.

Survey is unsuccessful when one or more element of the Network Cartography of the Cyber Inventory is not consistent with the results.

1.3 Remote access robustness

1.3.1 Context

Remote access equipment are used as a remote entry point for the vessel systems and equipment. From an attacker point of view, it represents a key target.

This survey proposes tests to compare ashore and onboard remote access installation with elements declared in the Cyber Inventory.

1.3.2 Technical scope

The technical scope of remote access robustness testing applies to any ashore and onboard Level 2 and Level 3 system and identified in remote access usage in the Cyber Inventory.

1.3.3 Test case

The test case is to rely on the remote access usage delivered in the Cyber Inventory.

Test case is to propose:

- trials to demonstrate encryption on the networks (e.g. packet sniffing)
- active network scanning (e.g. network scanners or penetration tests) conducted outside the vessel, in order to ensure that the DMZ respect the Cyber Inventory
- active network scanning (e.g. network scanners) conducted on each side of firewalls, in order to ensure that the firewall respect its filtering policy
- active network scanning (e.g. network scanners or penetration tests) conducted ashore, in order to ensure that ashore systems respect the Cyber Inventory
- active tests on IPS, when they exist, to ensure that the IPS blocks malicious packets.

Tests may use tools, be scripted, or written with a check list of commands to type in console mode during the survey.

Tests are to be launched from different locations of the system in order to survey the different paths of weakness and attacks (e.g. in front of and behind a firewall).

Tests are to be non-intrusive and non-destructive. Tests are to be submitted and approved by Society.

1.3.4 Test results

The test case is to propose a way to compare remote access usage delivered in the Cyber Inventory in order to:

- check the proper functioning of traffic encryption
- check the good state of DMZ principles
- check the proper functioning of traffic blocking.

1.3.5 Evaluation criteria

Survey is successful when remote access usage of the Cyber Inventory is consistent with the results

Survey is unsuccessful when one or more element of the remote access usage of the Cyber Inventory is not consistent with the results.

1.4 Remote access logging

1.4.1 Context

Remote access equipment are used as a remote entry point for the vessel systems and equipment. From an attacker point of view, it represents a key target.

This survey propose tests to check DMZ events logging coverage and efficiency.

1.4.2 Technical scope

The technical scope of remote access logging testing applies to any ashore and onboard Level 2 and Level 3 system and identified in remote access usage in the Cyber Inventory.

1.4.3 Test case

The test case is to rely on remote access logging.

The test case is to identify the different points of authentication, connection and traffic logging. Then, tests are proposed with the following steps:

a) check of the initial state of the logs by using the procedure described in the Cyber Security Policy.

b) run different kind of trials with the following logic:
   - identify sources and destinations points, from the outside to the vessel and from the vessel to the outside
   - identify different scenarios of accepted and rejected connections
   - identify authenticators.

c) check of the final state of the logs by using the procedure described in the Cyber Security Policy.

Tests may use tools, be scripted, or written with a check list of commands to type in console mode during the survey.

Tests are to be non-intrusive and non-destructive. Tests are to be submitted and approved by Society.

1.4.4 Test results

The test case is to confront the initial state of the logs with the final one. Awaited results of hereinbefore test cases are to be submitted.

1.4.5 Evaluation criteria

Survey is successful when the final state of the logs contains a full record of events executed by the test case with correct time stamp.

Corrections are to be implemented or mitigations measures are to be adopted when elements are missing.

Survey is unsuccessful when events about accepted and rejected connections are missing.

1.5 Wireless networks robustness

1.5.1 Context

Wireless networks represent a vulnerability as they may be listened from a distance and, by resulting, taken in control by a remote attacker.

This survey proposes tests to compare wireless installation with elements declared in the Cyber Inventory.

1.5.2 Technical scope

The technical scope of wireless networks robustness testing applies to any Level 3 wireless system identified in wireless architecture in the Cyber Inventory.

1.5.3 Test case

The test case is to rely on wireless architecture and wireless LAN.

The test case is to propose test to:

- check proper network traffic encryption
- check segregation of the network (physical and logical)
- check transmission range
- check wireless network architecture by using active network scanning (e.g. network scanners or penetration tests).

Tests may use tools, be scripted, or written with a check list of commands to type in console mode during the survey.

Tests are to be non-intrusive and non-destructive. Tests are to be submitted and approved by Society.

1.5.4 Evaluation criteria

Survey is successful when wireless architecture of the Cyber Inventory is consistent with the results

Survey is unsuccessful when one or more element of the wireless architecture of the Cyber Inventory are not consistent with the results.

1.6 Black box penetration tests

1.6.1 Context

Objective of black box penetration testing is to deliver a health check-up of systems and equipment by using an “out of the box” approach.

Black box penetration tests are here to find paths in the system which are undocumented, unknown and, thus, undefined in the test case.

Those tests make sense before vessel commissioning.

A recognized third party is recommended and may be required for the additional class notation **CYBER SECURE** (see Ch 4, Sec 1, [1.1.3]).

1.6.2 Technical scope

The technical scope of black box testing applies to:

- any system or equipment using or involved in remote access
- any system or equipment using or involved in wireless networks
- any system or equipment involved in the network management and security of cabled networks
- any Level 3 equipment of Cat. A, Cat. B and Cat. C.

1.6.3 Test case

By using Cyber Inventory information, a procedure of tests is to be written with the following restrictions:

- A dedicated “black box” environment (physical or virtualized) must be set up
- Code injection is authorized on operating systems, applications, automation and all network equipment
- Hardware security analysis is authorized
- Depending on the scope and the need, software and hardware hacking tools may be employed during black box penetration tests. (e.g. vulnerability exploitation tools, maintaining access tools, reverse engineering tools, remote access control tools, password crackers, rootkits, sniffing, fuzzing, denial of services, packet crafting, tunnelling, proxies, man in the middle, USB implant tools, network implants embedding remote access, wifi pineapple, etc.)
- Equipment forensics may be used to reveal useful information for attackers.

While conducted, black box penetration tests are to be strictly traced and recorded.

Tests are to be limited in time, submitted and approved by Society.

1.6.4 Test results

Tests results are to detail applied procedures, tools and methods. An evaluation of the level of security is to be submitted.

1.6.5 Evaluation criteria

The Society evaluates the success of the test regarding:

- the technical scope (which is to be exhaustive regarding equipment)
- the efficiency of test cases (technics and tools are to be updated)
- the results.

Section 4 Equipment Survey

1 Definition

1.1 Equipment procedures

1.1.1 Equipment procedures are procedures used onboard by the Surveyor to verify the level of cyber security of specific equipment.

2 Surveys process

2.1 Account security settings

2.1.1 Context

Accounts are entries points of the systems. The correct application of the policies applicable on those systems is fundamental. For this reason, the Surveyor will verify consistency between rules and onboard equipment. The rules to refer to are those defined in Cyber Inventory.

2.1.2 Technical scope

The technical scope applies to each Level 2 and Level 3 equipment.

2.1.3 Test case

In order to verify proper implementation of accounts security settings (see Ch 1, Sec 6, [3.2.7]), relevant tests are to be submitted.

Robustness of password is to be verified with a procedure which tries to create an account, in order to check that the policy is applied. At the end of the survey, the created account is to be deleted through a relevant procedure.

Tests are to be written in accordance with the topics detailed in the Cyber Inventory. Tests will try different pattern to verify a list of cases.

2.1.4 Test results

Tests case is to contain awaited results for each case.

2.1.5 Evaluation Criteria

Survey is successful when all test successfully achieved.

Corrections are to be implemented or mitigations measures are to be adopted for tests identifying non-conformances. survey is systematically unsuccessful when:

- equipment can be accessed without authentication mechanism (identification and “password”)
- generic and default accounts can be used
- one or more password is weak.

2.2 Operating systems security

2.2.1 Context

Operating systems are the core of equipment. For equipment with a high level of Risk (Level 3), operating systems security settings are checked in accordance with the information delivered in the Cyber Inventory.

2.2.2 Technical scope

The technical scope applies to each Cat. A Level 3 equipment.

2.2.3 Test case

In order to verify proper implementation of operating systems security settings, relevant tests are to be submitted. Tests are to be written in accordance with the topics detailed in the Cyber Inventory.

Depending of the contents of the rules detailed in the Cyber Inventory Test may address: system services, accounts, local policies, audit policies, events logs management, file access control list, network interfaces configuration, network filtering, etc.

At a minimum, the test will check: connections (listening and outgoing), in-memory processes, in-operation services and ran applications.

Tests may use tools, be scripted, or written with a check list of commands to type in console mode during the survey.

2.2.4 Test results

Tests case is to contain awaited results for each case.

2.2.5 Evaluation Criteria

Survey is successful when the tests do not show any inconsistency between the equipment and the Rules delivered in the Cyber Inventory.

Corrections are to be implemented or mitigations measures are to be adopted for tests identifying non-conformances. survey is systematically unsuccessful when:

- unexpected connection, process, service or application have been detected
- events logs management is off or inefficient.

2.3 Features security settings

2.3.1 Context

Features security settings are elements installed on Cat. B and Cat. C equipment used to deliver or help security mechanisms. Features are predefined in the Cyber Inventory. The Surveyor is in charge to check the accuracy of their implementation.

2.3.2 Technical scope

The technical scope applies to each Cat. B and Cat. C Level 3 equipment.

2.3.3 Test case

In order to verify proper implementation of features security settings, relevant tests are to be submitted. Tests are to be written in accordance with the topics detailed in the Cyber Inventory.

When detailed in the Cyber Inventory, the following are to be tested:

- equipment self-tests procedures or any integrated integrity checking tool
- equipment physical configuration (OT safety switches)
- equipment system services, accounts policies, events logs management, network interfaces configuration, network filtering.

Tests may use manual operation, numeric tools, scripts or a check list of command line to type in console mode during the survey.

2.3.4 Test results

Tests case is to contain awaited results for each case.

2.3.5 Evaluation Criteria

Survey is successful when the tests do not show any inconsistency between the equipment and the rules delivered in the Cyber Inventory.

Corrections are to be implemented or mitigations measures are to be adopted for tests identifying non-conformances. Survey is systematically unsuccessful when:

- OT safety switch is in a wrong position
- unexpected connection, process, service or application have been detected
- events logs management is off or inefficient.

2.4 Antivirus solution

2.4.1 Context

The antivirus solution represents a first barrier against viruses and malwares. This first-aid tool is also a path of weakness as it needs to be periodically updated, properly launched and correctly installed.

The survey has to demonstrate the good coverage of the antivirus solution.

2.4.2 Technical scope

The technical scope applies to each Cat. A Level 3 equipment.

2.4.3 Test case

Trials are to propose procedures to:

- proof installation of antivirus software.
- warranty efficiency on operation: an example of fake virus signature is often proposed by the antivirus vendors in order to verify detection systems
- check availability of the antivirus solution: tests are to be done without restarting the equipment, in order to take into account the duration of run of the equipment and thus the ability of the antivirus solution to be up after a large amount of time
- demonstrate detection of loss of antivirus compliance: this test can rely on the survey already described in Sec 2, [2.1]
- verify update capabilities of the antivirus solution.

Tests may use manual operation, numeric tools, scripts or a check list of command line to type in console mode during the survey.

2.4.4 Test results

Tests case is to contain awaited results for each case.

2.4.5 Evaluation Criteria

Survey is successful when the tests are perfectly successful.

Corrections are to be implemented or mitigations measures are to be adopted for tests identifying the following:

- results are unsuccessful.
- the equipment manufacturer do not publish updates anymore for the antivirus solution (e.g. unsupported version).

Survey is systematically unsuccessful when:

- antivirus solution is not present or not available
- antivirus solution has not been updated during the last two weeks before survey
- records contain no trace of regularly application of updates.

2.5 Software maintenance

2.5.1 Context

The software maintenance through patch management directly contributes to assurance of cyber security.

The survey demonstrates the regular, correct and in time application of patches delivered by software editors.

2.5.2 Technical scope

The technical scope applies to each Cat. A, Cat. B and Cat. C Level 3 equipment.

2.5.3 Test case

Trials are to propose procedures to:

- proof usage of patch management (see Ch 1, Sec 6, [3.3.2])
- proof follow up of supplier's corrective patches according to the supplier patch's policy
- check records for updates.

Tests may use manual operation, numeric tools, scripts or a check list of command line to type in console mode during the Survey.

2.5.4 Test results

Tests case is to contain awaited results for each case.

2.5.5 Evaluation Criteria

Survey is successful when the tests are perfectly successful.

Corrections are to be implemented or mitigations measures are to be adopted for tests identifying the following:

- results are unsuccessful.
- the equipment manufacturer do not publish updates anymore for the equipment (e.g. unsupported version).

Survey is systematically unsuccessful when:

- patch management is not available or unused
- equipment was not successfully updated
- records contain no trace of regularly application of updates.

Section 5 Checking Maintenance Procedures

1 Definition

1.1 Maintenance procedures

1.1.1 Maintenance procedures are procedures used onboard by the cyber security responsible to maintain level of cyber security of the systems.

Those procedures are to be detailed in Cyber Security Policy document and rely on Cyber Handbook.

The objective of this survey is to verify the good functioning of randomly selected maintenance procedures and their efficiency.

2 Surveys

2.1 Recovery plan testing

2.1.1 Context

Recovery plan usually relies on equipment maintenance guides, backups and last known configurations, states and parameters. Recovery plan is the only solution to come back in a previously defined safe situation. As recovery plans are used in emergency response to incident, there is no place for imprecision, lack of information or crew's autonomy. The Surveyor checks that the procedure works on the first time, without any issue and with a successful return in operation.

Restoration of data backup conduct in Ch 2, Sec 2, [4.3.5] must be tested on a representative scale of IT and OT systems.

Procedures described in Ch 2, Sec 2, [4.3.6] are applied.

2.1.2 Technical scope

The technical scope of recovery plan testing applies to:

- any system or equipment using or involved in remote access
- any Level 3 equipment of Cat. A, Cat. B and Cat. C.

2.1.3 Test case

For targeted equipment a set of trials (the test case) is to be defined in order to verify efficiency of the recovery plan.

Test case is to be non-destructive.

The survey procedure is to present a way to follow this step-by-step actions:

- identification of disaster recovery plan from the Cyber Security Policy as defined in Ch 2, Sec 2, [4.3.6]
- selection of equipment from the survey scope
- identification of critical functionalities of the equipment
- definition of the non-regression tests. non-regression tests explain how to verify the correct functioning of identified critical functionalities
- use of non-regression tests and record of results, behaviors and any information regarding the good functioning
- when possible, backup of the equipment by, for example:
  - making a backup of the files on a safe place (e.g. reserved disk space, removable media, etc.)
  - taking pictures or screenshots of configurations
  - writing down sensitive elements regarding configuration.
- modification, and trace, of the equipment.

2.1.4 Test results

The following processing steps are to be described:

- application of the recovery plan procedure. The survey is to trace results of this application:
  - convenience of the procedure
  - ease of reading
  - inconsistencies in the procedure
  - errors during application of the procedure.
- if recovery plan is successfully finished, the equipment is to be restarted. Survey is to trace restart events, checking for warnings, abnormalities or errors
- presence of modifications operated before application of the recovery plan is done. If those modifications are missing, the survey may continue
- use of non-regression tests and record of results, behaviors and any information regarding the good functioning.

2.1.5 Evaluation Criteria

Survey is successful when this last step is successfully achieved.

Corrections are to be implemented or mitigations measures are to be adopted in case of any trouble during the application of the recovery plan.

2.2 Compliance update

2.2.1 Context

The efficiency of the compliance monitoring at sea relies on the capacity to compare the current state of the equipment to a state of reference, known as accepted.

In case of equipment modification, or any update, upgrade and change, the state of reference shall be maintained.

Surveyor verifies that the compliance procedures exist and that updates have been applied periodically.

2.2.2 Technical scope

The technical scope of compliance update testing applies to:

- any system or equipment using or involved in remote access
- any system or equipment using or involved in wireless networks
- any system or equipment involved in the network management and security of cabled networks
- any Level 3 equipment of Cat. A, Cat. B and Cat. C.

2.2.3 Test case

The survey procedure is to present a way to follow this step-by-step actions:

- identification of compliance update procedures from the Cyber Security Policy defined in Ch 2, Sec 2, [4.2.3]
- identification of a scope of testing
- identification of application of those procedures with past updates in the records.

2.2.4 Test results

On the identified scope of testing, update procedures are to be applied. Survey traces results of this trial:

- convenience of the procedure
- ease of reading
- inconsistencies in the procedure
- errors during application of the procedure.

2.2.5 Evaluation Criteria

Survey is successful when:

- tests of compliance update achieved successfully
- the records contain successful update operation in accordance with the update procedure.

2.3 Maintenance protection tests

2.3.1 Context

The protection of maintenance operation increases safety and reduces risk of misuse of an equipment during its maintenance.

Surveyor is in charge of controlling applicability and good functioning of randomly selected procedures and technical solution used to protect an equipment during its maintenance.

2.3.2 Technical scope

The technical scope of maintenance protection testing applies to any Level 3 system or equipment using or involved in remote access.

2.3.3 Test case

The test case is to propose:

- a non-destructive set of tests
- an exhaustive identification of systems impacted by isolation procedure during their maintenance
- a test case procedure per equipment.

Each test case is to contain:

- a rationale about the risks covered by the procedure
- the reference to the procedure detailed in the Cyber Security Policy as defined in Ch 2, Sec 2, [4.1.4].

2.3.4 Tests results

The test case is to give a way to determine a result for each of those actions:

- verify that equipment is running before application of the protection procedure
- apply the protection procedure from the Cyber Security Policy
- verify that equipment cannot be used from the bridge during application of the protection procedure
- apply the restart procedure of the protection procedure from the Cyber Security Policy
- verify that equipment is available.

2.3.5 Evaluation Criteria

Survey is successful when:

- the identified systems match the systems described in the Cyber Inventory in the "Equipment Security Identification" Chapter.
- The test results scored a successful result for each step of each system.

2.4 Wireless patch management

2.4.1 Context

Wireless network security partially relies on the efficiency of its updates. The Surveyor is in charge to check that:

- the updates patch management process is usable
- updates are periodically applied
- the equipment manufacturer publish updates
- the last updates have been applied.

2.4.2 Technical scope

The technical scope of compliance update testing applies to any system or equipment using or involved in wireless networks.

2.4.3 Test case

The survey procedure is to present a way to follow this step-by-step actions:

- identification of wireless update procedures from the Cyber Security Policy defined in Ch 2, Sec 2, [4.2.3]
- identification of a scope of testing
- by using the update procedures, identification of manufacturers sources of updates (e.g. websites)
- identification of application of those procedures with past updates in the records.

2.4.4 Test results

On the identified scope of testing, update procedures are to be applied. Survey is to trace results of this trial:

- convenience of the procedure
- ease of reading
- inconsistencies in the procedure
- errors during application of the procedure.

2.4.5 Evaluation Criteria

Survey is successful when:

- update patch procedure has been successfully applied with the last updates
- updates have been regularly applied
- the equipment manufacturer publishes regular updates.

Corrections are to be implemented or mitigations measures are to be adopted if the two first conditions have been successfully achieved but the Equipment manufacturer do not publish updates anymore for the Equipment (e.g. because of end of life of the product).

Survey is unsuccessful if one of the two first conditions is not fulfilled.

CHAPTER 7
EXISTING SHIPS ASSIGNED CYBER NOTATIONS PRIOR TO JANUARY 2023

Section 1 CYBER MANAGED PREPARED Notation

Section 1 CYBER MANAGED PREPARED Notation

1 General

1.1 Scope

1.1.1 The requirements of this Section apply to ships assigned the additional class notation **CYBER MANAGED PREPARED** prior to 1st January 2023.

After commissioning, the additional class notation **CYBER MANAGED PREPARED** may be replaced by **CYBER MANAGED** when the ships comply with requirements defined in Ch 1, Sec 1, [1.2.2], regarding:

- cyber management
- crew training.

1.2 Workflow

1.2.1 The following steps are to be implemented by the Shipowner when the additional class notation **CYBER MANAGED** is intended to be assigned:

- The first step is to deliver a Cyber Risk Assessment for the vessel based on the levels of criticality delivered by the Shipyard during the construction phase. This step is Shipowner oriented and helps to introduce and consider operations needs besides design needs as explained in Ch 1, Sec 5.

  Cyber Risk Assessment is to be built by following Ch 1, Sec 5
- The second step is to build the Cyber Security Policy, as defined in Ch 2, Sec 2. This document, that will be enforced on all Shipowner's vessels, is composed of human, organisational and technical procedures to use, protect and monitor the systems, taking into account the output of the Cyber Risk Assessment.
- The third and final step, is to update procedures of the Cyber Handbook document by checking their applicability with Shipowner’s rules, organization and means as detailed in the Cyber Security Policy.

  Cyber Handbook is to be updated by following Ch 1, Sec 6 instructions whose workflow is detailed in Tab 2:
  - The Cyber Handbook delivered by the Shipyard for the additional class notation **CYBER MANAGED PREPARED**
  - Procedures relevant to identified equipment are to be added to the retrieved Cyber Handbook document.

1.3 Documents to be submitted

1.3.1 The documentation to be submitted for approval is listed in Tab 1.

Table 1 : Documentation to be submitted for prepared ships to be assigned CYBER MANAGED notation

Document	Reference
Cyber Risk Assessment	Ch 1, Sec 5
Cyber Inventory: update of basic inventory, if new equipment added by the Shipowner	Ch 1, Sec 2, Tab 1
Cyber Security Policy	Ch 2, Sec 2, Tab 1
Cyber Handbook: update of Cyber handbook	see Tab 2

Table 2 : Shipowner procedures for prepared ships to be assigned CYBER MANAGED notation

Procedure	Rule	Applicability				
		Network **(1)**			System **(1)**	
		ONE	INE	SNE	L3S	OVS
Monitoring procedures						
Management	Ch 1, Sec 6, [3.2.1]	X	X	X	X	X
Maintenance procedures						
Patch management	Ch 1, Sec 6, [3.3.2]	X		X		X
Maintenance management	Ch 1, Sec 6, [3.3.3]	X			X	X
Antivirus management	Ch 1, Sec 6, [3.3.5]					X
Accounts management	Ch 1, Sec 6, [3.3.7]					X
Incident Response procedures						
Loss of compliance	Ch 1, Sec 6, [3.4.1]	X		X	X	X
Availability management	Ch 1, Sec 6, [3.4.4]			X	X	

(1) See Ch 1, Sec 6, [2.2.1] for definition of ONE, INE, SNE, L3S and OVS

BUREAU VERITAS MARINE & OFFSHORE

Tour Alto
4 place des Saisons
92400 Courbevoie - France
+33 (0)1 55 24 70 00

marine-offshore.bureauveritas.com/rules-guidelines

BUREAU VERITAS

Shaping a World of Trust