

Rules on Cyber Security for the Classification of Marine Units

December 2018
NR 659 DT R00



Rule Note



Documents

Document Sharing Hub

RULES & GUIDANCE NOTES

For document details, see BVR 659/2018



**BUREAU
VERITAS**

Rules on Cyber Security for the Classification of Marine Units

December 2018

**Rule Note
NR 659 DT R00 E**

**Marine & Offshore
8 Cours du Triangle - CS 50101
92937 Paris La Defense Cedex - France
Tel: + 33 (0)1 55 24 70 00
<https://marine-offshore.bureauveritas.com/bv-rules>
© 2018 Bureau Veritas – All rights reserved**



Documents
Document Sharing Hub

GENERAL CONDITIONS

1. INDEPENDENCE OF THE SOCIETY AND APPLICABLE TERMS

- 1.1 The Society shall remain at all times an independent contractor and neither the Society nor any of its officers, employees, servants, agents or subcontractors shall be or act as an employee, servant or agent of any other party hereto in the performance of the Services.
- 1.2 The operations of the Society in providing its Services are exclusively conducted by way of random inspections and do not, in any circumstances, involve monitoring or exhaustive verification.
- 1.3 The Society acts as a services provider. This cannot be construed as an obligation bearing on the Society to obtain a result or as a warranty. The Society is not and may not be considered as an underwriter, broker in Unit's sale or chartering, expert in Unit's valuation, consulting engineer, controller, naval architect, designer, manufacturer, shipbuilder, repair or conversion yard, charterer or shipowner; none of them above listed being relieved of any of their expressed or implied obligations as a result of the interventions of the Society.
- 1.4 The Society only is qualified to apply and interpret its Rules.
- 1.5 The Client acknowledges the latest versions of the Conditions and of the applicable Rules applying to the Services' performance.
- 1.6 Unless an express written agreement is made between the Parties on the applicable Rules, the applicable Rules shall be the Rules applicable at the time of entering into the relevant contract for the performance of the Services.
- 1.7 The Services' performance is solely based on the Conditions. No other terms shall apply whether express or implied.

2. DEFINITIONS

- 2.1 "Certificate(s)" means classification or statutory certificates, attestations and reports following the Society's intervention.
- 2.2 "Certification" means the activity of certification in application of national and international regulations or standards, in particular by delegation from different governments that can result in the issuance of a Certificate.
- 2.3 "Classification" means the classification of a Unit that can result or not in the issuance of a classification Certificate with reference to the Rules. Classification is an appraisalment given by the Society to the Client, at a certain date, following surveys by its surveyors on the level of compliance of the Unit to the Society's Rules or to the documents of reference for the Services provided. They cannot be construed as an implied or express warranty of safety, fitness for the purpose, seaworthiness of the Unit or of its value for sale, insurance or chartering.
- 2.4 "Client" means the Party and/or its representative requesting the Services.
- 2.5 "Conditions" means the terms and conditions set out in the present document.
- 2.6 "Industry Practice" means international maritime and/or offshore industry practices.
- 2.7 "Intellectual Property" means all patents, rights to inventions, utility models, copyright and related rights, trade marks, logos, service marks, trade dress, business and domain names, rights in trade dress or get-up, rights in goodwill or to sue for passing off, unfair competition rights, rights in designs, rights in computer software, database rights, topography rights, moral rights, rights in confidential information (including know-how and trade secrets), methods and protocols for Services, and any other intellectual property rights, in each case whether capable of registration, registered or unregistered and including all applications for and renewals, reversions or extensions of such rights, and all similar or equivalent rights or forms of protection in any part of the world.
- 2.8 "Parties" means the Society and Client together.
- 2.9 "Party" means the Society or the Client.
- 2.10 "Register" means the public electronic register of ships updated regularly by the Society.
- 2.11 "Rules" means the Society's classification rules and other documents. The Society's Rules take into account at the date of their preparation the state of currently available and proven technical minimum requirements but are not a standard or a code of construction neither a guide for maintenance, a safety handbook or a guide of professional practices, all of which are assumed to be known in detail and carefully followed at all times by the Client.
- 2.12 "Services" means the services set out in clauses 2.2 and 2.3 but also other services related to Classification and Certification such as, but not limited to: ship and company safety management certification, ship and port security certification, maritime labour certification, training activities, all activities and duties incidental thereto such as documentation on any supporting means, software, instrumentation, measurements, tests and trials on board. The Services are carried out by the Society according to the applicable referential and to the Bureau Veritas' Code of Ethics. The Society shall perform the Services according to the applicable national and international standards and Industry Practice and always on the assumption that the Client is aware of such standards and Industry Practice.
- 2.13 "Society" means the classification society 'Bureau Veritas Marine & Offshore SAS', a company organized and existing under the laws of France, registered in Nanterre under number 821 131 844, or any other legal entity of Bureau Veritas Group as may be specified in the relevant contract, and whose main activities are Classification and Certification of ships or offshore units.
- 2.14 "Unit" means any ship or vessel or offshore unit or structure of any type or part of it or system whether linked to shore, river bed or sea bed or not, whether operated or located at sea or in inland waters or partly on land, including submarines, hovercrafts, drilling rigs, offshore installations of any type and of any purpose, their related and ancillary equipment, subsea or not, such as well head and pipelines, mooring legs and mooring points or otherwise as decided by the Society.

3. SCOPE AND PERFORMANCE

- 3.1 Subject to the Services requested and always by reference to the Rules, the Society shall:
- review the construction arrangements of the Unit as shown on the documents provided by the Client;
 - conduct the Unit surveys at the place of the Unit construction;
 - class the Unit and enter the Unit's class in the Society's Register;
 - survey the Unit periodically in service to note whether the requirements for the maintenance of class are met.
- The Client shall inform the Society without delay of any circumstances which may cause any changes on the conducted surveys or Services.
- 3.2 The Society will not:
- declare the acceptance or commissioning of a Unit, nor its construction in conformity with its design, such activities remaining under the exclusive responsibility of the Unit's owner or builder;
 - engage in any work relating to the design, construction, production or repair checks, neither in the operation of the Unit or the Unit's trade, neither in any advisory services, and cannot be held liable on those accounts.

4. RESERVATION CLAUSE

- 4.1 The Client shall always: (i) maintain the Unit in good condition after surveys; (ii) present the Unit for surveys; and (iii) inform the Society in due time of any circumstances that may affect the given appraisalment of the Unit or cause to modify the scope of the Services.
- 4.2 Certificates are only valid if issued by the Society.
- 4.3 The Society has entire control over the Certificates issued and may at any time withdraw a Certificate at its entire discretion including, but not limited to, in the following situations: where the Client fails to comply in due time with instructions of the Society or where the Client fails to pay in accordance with clause 6.2 hereunder.
- 4.4 The Society may at times and at its sole discretion give an opinion on a design or any technical element that would 'in principle' be acceptable to the Society. This opinion shall not presume on the final issuance of any Certificate or on its content in the event of the actual issuance of a Certificate. This opinion shall only be an appraisal made by the Society which shall not be held liable for it.

5. ACCESS AND SAFETY

- 5.1 The Client shall give to the Society all access and information necessary for the efficient performance of the requested Services. The Client shall be the sole responsible for the conditions of presentation of the Unit for tests, trials and surveys and the conditions under which tests and trials are carried out. Any information, drawing, etc. required for the performance of the Services must be made available in due time.
- 5.2 The Client shall notify the Society of any relevant safety issue and shall take all necessary safety-related measures to ensure a safe work environment for the Society or any of its officers, employees, servants, agents or subcontractors and shall comply with all applicable safety regulations.

6. PAYMENT OF INVOICES

- 6.1 The provision of the Services by the Society, whether complete or not, involve, for the part carried out, the payment of fees thirty (30) days upon issuance of the invoice.

6.2 Without prejudice to any other rights hereunder, in case of Client's payment default, the Society shall be entitled to charge, in addition to the amount not properly paid, interests equal to twelve (12) months LIBOR plus two (2) per cent as of due date calculated on the number of days such payment is delinquent. The Society shall also have the right to withhold Certificates and other documents and/or to suspend or revoke the validity of Certificates.

- 6.3 In case of dispute on the invoice amount, the undisputed portion of the invoice shall be paid and an explanation on the dispute shall accompany payment so that action can be taken to solve the dispute.

7. LIABILITY

- 7.1 The Society bears no liability for consequential loss. For the purpose of this clause consequential loss shall include, without limitation:
- Indirect or consequential loss;
 - Any loss and/or deferral of production, loss of product, loss of use, loss of bargain, loss of revenue, loss of profit or anticipated profit, loss of business and business interruption, in each case whether direct or indirect.
- The Client shall defend, release, save, indemnify, defend and hold harmless the Society from the Client's own consequential loss regardless of cause.
- 7.2 Except in case of wilful misconduct of the Society, death or bodily injury caused by the Society's negligence and any other liability that could not be, by law, limited, the Society's maximum liability towards the Client is limited to one hundred and fifty per-cents (150%) of the price paid by the Client to the Society for the Services having caused the damage. This limit applies to any liability of whatsoever nature and howsoever arising, including fault by the Society, breach of contract, breach of warranty, tort, strict liability, breach of statute.
- 7.3 All claims shall be presented to the Society in writing within three (3) months of the completion of Services' performance or (if later) the date when the events which are relied on were first discovered by the Client. Any claim not so presented as defined above shall be deemed waived and absolutely time barred.

8. INDEMNITY CLAUSE

- 8.1 The Client shall defend, release, save, indemnify and hold harmless the Society from and against any and all claims, demands, lawsuits or actions for damages, including legal fees, for harm or loss to persons and/or property tangible, intangible or otherwise which may be brought against the Society, incidental to, arising out of or in connection with the performance of the Services (including for damages arising out of or in connection with opinions delivered according to clause 4.4 above) except for those claims caused solely and completely by the gross negligence of the Society, its officers, employees, servants, agents or subcontractors.

9. TERMINATION

- 9.1 The Parties shall have the right to terminate the Services (and the relevant contract) for convenience after giving the other Party thirty (30) days' written notice, and without prejudice to clause 6 above.
- 9.2 In such a case, the Classification granted to the concerned Unit and the previously issued Certificates shall remain valid until the date of effect of the termination notice issued, subject to compliance with clause 4.1 and 6 above.
- 9.3 In the event where, in the reasonable opinion of the Society, the Client is in breach, or is suspected to be in breach of clause 16 of the Conditions, the Society shall have the right to terminate the Services (and the relevant contracts associated) with immediate effect.

10. FORCE MAJEURE

- 10.1 Neither Party shall be responsible or liable for any failure to fulfil any term or provision of the Conditions if and to the extent that fulfilment has been delayed or temporarily prevented by a force majeure occurrence without the fault or negligence of the Party affected and which, by the exercise of reasonable diligence, the said Party is unable to provide against.
- 10.2 For the purpose of this clause, force majeure shall mean any circumstance not being within a Party's reasonable control including, but not limited to: acts of God, natural disasters, epidemics or pandemics, wars, terrorist attacks, riots, sabotages, impositions of sanctions, embargoes, nuclear, chemical or biological contaminations, laws or action taken by a government or public authority, quotas or prohibition, expropriations, destructions of the worksite, explosions, fires, accidents, any labour or trade disputes, strikes or lockouts.

11. CONFIDENTIALITY

- 11.1 The documents and data provided to or prepared by the Society in performing the Services, and the information made available to the Society, are treated as confidential except where the information:
- is properly and lawfully in the possession of the Society;
 - is already in possession of the public or has entered the public domain, otherwise than through a breach of this obligation;
 - is acquired or received independently from a third party that has the right to disseminate such information;
 - is required to be disclosed under applicable law or by a governmental order, decree, regulation or rule or by a stock exchange authority (provided that the receiving Party shall make all reasonable efforts to give prompt written notice to the disclosing Party prior to such disclosure).
- 11.2 The Parties shall use the confidential information exclusively within the framework of their activity underlying these Conditions.
- 11.3 Confidential information shall only be provided to third parties with the prior written consent of the other Party. However, such prior consent shall not be required when the Society provides the confidential information to a subsidiary.
- 11.4 Without prejudice to sub-clause 11.1, the Society shall have the right to disclose the confidential information if required to do so under regulations of the International Association of Classifications Societies (IACS) or any statutory obligations.

12. INTELLECTUAL PROPERTY

- 12.1 Each Party exclusively owns all rights to its Intellectual Property created before or after the commencement date of the Conditions and whether or not associated with any contract between the Parties.
- 12.2 The Intellectual Property developed by the Society for the performance of the Services including, but not limited to drawings, calculations, and reports shall remain the exclusive property of the Society.

13. ASSIGNMENT

- 13.1 The contract resulting from to these Conditions cannot be assigned or transferred by any means by a Party to any third party without the prior written consent of the other Party.
- 13.2 The Society shall however have the right to assign or transfer by any means the said contract to a subsidiary of the Bureau Veritas Group.

14. SEVERABILITY

- 14.1 Invalidity of one or more provisions does not affect the remaining provisions.
- 14.2 Definitions herein take precedence over other definitions which may appear in other documents issued by the Society.
- 14.3 In case of doubt as to the interpretation of the Conditions, the English text shall prevail.

15. GOVERNING LAW AND DISPUTE RESOLUTION

- 15.1 These Conditions shall be construed and governed by the laws of England and Wales.
- 15.2 The Parties shall make every effort to settle any dispute amicably and in good faith by way of negotiation within thirty (30) days from the date of receipt by either one of the Parties of a written notice of such a dispute.
- 15.3 Failing that, the dispute shall finally be settled under the Rules of Arbitration of the Maritime Arbitration Chamber of Paris ("CAMP"), which rules are deemed to be incorporated by reference into this clause. The number of arbitrators shall be three (3). The place of arbitration shall be Paris (France). The Parties agree to keep the arbitration proceedings confidential.

16. PROFESSIONAL ETHICS

- 16.1 Each Party shall conduct all activities in compliance with all laws, statutes, rules, economic and trade sanctions (including but not limited to UN sanctions and EU sanctions) and regulations applicable to such Party including but not limited to: child labour, forced labour, collective bargaining, discrimination, abuse, working hours and minimum wages, anti-bribery, anti-corruption, copyright and trademark protection, personal data protection (<https://personal.dataprotection.bureauveritas.com/privacypolicy>).
- Each of the Parties warrants that neither it, nor its affiliates, has made or will make, with respect to the matters provided for hereunder, any offer, payment, gift or authorization of the payment of any money, directly or indirectly, to or for the use or benefit of any official or employee of the government, political party, official or candidate.
- 16.2 In addition, the Client shall act consistently with the Bureau Veritas' Code of Ethics. <https://group.bureauveritas.com/group/corporate-social-responsibility>



RULE NOTE NR 659

NR 659

Rules on Cyber Security for the Classification of Marine Units

Chapters **1 2 3 4**

Chapter 1	General Principles
Chapter 2	Additional Class Notation Cyber Managed
Chapter 3	Additional Class Notation Cyber Secure
Chapter 4	Survey Operations

December 2018

CHAPTER 1

GENERAL PRINCIPLES

Section 1 Classification Notations

1	General	11
1.1	General	
1.2	Classification notation	
2	Definitions	11
2.1	Global terms	
2.2	Roles	
2.3	Systems and equipment terms	
3	Documentation management	14
3.1		
4	Documents to be submitted	16
4.1		
5	Regulation and standards	16
5.1		

Section 2 Cyber Risk Analysis

1	General	18
1.1	Framework	
1.2	Workflow	
2	Context establishment	20
2.1	Scope	
2.2	Inventory	
2.3	Process chain	
3	Risk assessment	22
3.1	Criticality level	
3.2	Feared hazard	
3.3	Threats likelihood (K)	
3.4	Exposition (E)	
3.5	Human factor (H)	
3.6	Level (L)	
3.7	Risk calculation	
4	Risk treatment	28
4.1	Residual risks	

CHAPTER 2

ADDITIONAL CLASS NOTATION CYBER MANAGED

Section 1 General

1	General	33
1.1	Application	
2	Document to be submitted	34
2.1	Methodology	
2.2	Documentation updates	

Section 2 Equipment Management

1	Compliance policy	37
1.1	Components identification	
1.2	Compliance monitoring	
1.3	Compliance maintenance	
1.4	Compliance incident response	
2	Equipment security	38
2.1	Equipment security settings	
2.2	Antivirus software	
2.3	Equipment maintenance	
2.4	Equipment monitoring	
2.5	Equipment incident response	

Section 3 System Integration

1	Remote access	42
1.1	Usages	
1.2	Demilitarized Zone (DMZ)	
1.3	Traffic security	
1.4	Remote access monitoring	
1.5	Remote access maintenance	
2	Wireless networks	45
2.1	Wireless identification	
3	Cabled networks	46
3.1	Network identification	
4	Networks	46
4.1	Network monitoring	
4.2	Network maintenance	

Section 4 Vessel Management

1	Governance	48
1.1	Cyber risk analysis	
1.2	Cyber security policy	
1.3	Information protection	
2	Roles and responsibilities	48
2.1	Management	
2.2	Predefined roles	
3	Cyber operations	50
3.1	Operations management	
3.2	Monitoring policy	
3.3	Maintenance policy	
3.4	Incident response policy	
4	Physical security	52
4.1	Management	
4.2	Vessel	
4.3	Removable and mobile medias	
5	Change management plan	53
5.1	Management	
5.2	Change request	
5.3	Change approbation	
5.4	Change homologation	
5.5	Change validation	

CHAPTER 3

ADDITIONAL CLASS NOTATION CYBER SECURE

Section 1 Cyber Secure Class

1	General	57
1.1	Application	
1.2	Ship approval	
2	Documents to be submitted	58
2.1	Documents for equipment	
2.2	Documents for the vessel	
2.3	Documents for security solutions	
2.4	Submitter	

Section 2 Equipment Design

1	General	61
1.1	Application	
1.2	System integration	
1.3	Identification	
2	Development	62
2.1	Context	
2.2	Development platform	
2.3	Development principles	
3	Protection	63
3.1	Context	
3.2	Hardening	
3.3	Access	
3.4	Physical security	
4	Verification	66
4.1	Context	
4.2	Equipment compliance	
4.3	Elements of integrity	
5	Evaluation	68
5.1	Global	
5.2	Antivirus	
6	Commutation	69
6.1	Network policy	
6.2	Industrial Control Systems (ICS)	
7	Preservation	69
7.1	Context	
8	Maintenance	70
8.1	Context	
8.2	Administration guide	
8.3	Operator guide	

9	Monitoring	71
9.1	Architecture	
9.2	Events manager	
9.3	Investigation manager	

Section 3 Vessel Design

1	Architecture	73
1.1	Principles	
1.2	Security mechanisms	
1.3	Design	
2	Network	76
2.1		
2.2	New-generation firewall	
2.3	Intrusion and prevention system	
3	Systems	78
3.1	Cabinet protection	

Section 4 Security Solutions

1	General	79
1.1	Application	
2	Compliance and Software Registry (CSR)	80
2.1	Mechanisms	
2.2	Functionalities	
2.3	Maintenance	
2.4	Security mechanisms	
3	Inspection and Decontamination Gate (IDG)	83
3.1	Mechanisms	
3.2	Functionalities	
3.3	Maintenance	
3.4	Security mechanisms	
4	Events and Logs Recording (ELR)	85
4.1	Mechanisms	
4.2	Functionalities	
4.3	Maintenance	
4.4	Security mechanisms	

Section 5 Vessel Management

1	General	87
1.1	Management	
1.2	Forensics	

CHAPTER 4

SURVEY OPERATIONS

Section 1 General

1	General	91
1.1	Survey	
1.2	Cyber survey manual	
2	Initial inspection	92
2.1	Scope of survey	
3	Annual survey	92
3.1	Scope of survey	
4	Intermediate survey	92
4.1	Scope of survey	
5	Class renewal survey	92
5.1	Scope of survey	

Section 2 Monitoring Survey

1	General	94
1.1		
2	Surveys	94
2.1	Compliance testing	
2.2	Compliance availability testing	
2.3	Equipment accounts testing	
2.4	Remote access events testing	
2.5	Wireless events testing	

Section 3 Infrastructure Survey

1	General	96
1.1		
2	Surveys	96
2.1	White box testing	
2.2	Cabled networks	
2.3	Remote access robustness	
2.4	Remote access logging	
2.5	Wireless networks robustness	
2.6	Black box penetration tests	

Section 4 Equipment Survey

1	General	99
	1.1	
2	Surveys	99
	2.1	Account security settings
	2.2	Operating systems security
	2.3	Features security settings
	2.4	Antivirus solution
	2.5	Software maintenance

Section 5 Maintenance Procedures Survey

1	General	102
	1.1	
2	Surveys	102
	2.1	Recovery plan testing
	2.2	Compliance update
	2.3	Maintenance protection tests
	2.4	Wireless patch management

GENERAL PRINCIPLES

SECTION 1	CLASSIFICATION NOTATIONS
SECTION 2	CYBER RISK ANALYSIS

SECTION 1

CLASSIFICATION NOTATIONS

1 General

1.1 General

1.1.1 Application

These requirements apply to design, construction, commissioning and maintenance of computer based systems where they depend on software for the proper 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 [2.3.1], f), computer based systems 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 notation.

These requirements apply to new building ships and to existing ships.

1.1.2 Cyber risk analysis

A Cyber Risk Analysis methodology is proposed with a standard template detailed in Sec 2. This template and methodology may be used by the Shipowner to perform the Cyber Risk Analysis by himself or use a 3rd party contributor in accordance with a recognized methodology.

1.1.3 Exclusion

Navigation systems required by IMO SOLAS Chapter V, Radio-communication systems required by IMO SOLAS Chapter IV, are not in the scope of this requirement. However gateways and interfaces, when connected to the target of evaluation, are to be included in the scope of this requirement.

Systems may be excluded according to the Cyber Risk Analysis.

1.2 Classification notation

1.2.1 General

The additional class notations **CYBER MANAGED** and **CYBER SECURE** may be assigned to ships or offshore units whose equipment and networks comply with the requirements of this Rule Note.

For an automated approach of cyber security, **CYBER SECURE** class notation should be used.

1.2.2 CYBER MANAGED

CYBER MANAGED is a first level of cyber security. It requires human actions, a strong human organization and a significant amount of procedures to achieve objective.

The **CYBER MANAGED** classification notation corresponds to compliance with a set of requirements dealing with:

- critical equipment
- management
- crew training
- remote access
- change management and
- system integration.

Note 1: **CYBER MANAGED** notation is a way to control security with manual procedures with minor impact for in-service vessels.

1.2.3 CYBER SECURE

The **CYBER SECURE** Classification notation corresponds to compliance with a set of requirements dealing with:

- cyber management
- equipment, and
- vessel secure by design.

CYBER SECURE notation is a way to control security by means of automatic software. It requires dedicated technical equipment for security. The class notation is assigned with construction Mark (⊠ or ⊡ or ●) in accordance with Ship Rules, NR467, Pt A, Ch 1, Sec 2, [3].

Note 1: Since the requirements are mainly focused on design phase, this classification notation is more adapted for new construction than for in-service units.

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 means these Rules for the Classification of Steel Ships (NR467) and 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 4, 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 described in [2.2.2] to [2.2.8] are used in this Rule Note for each stakeholder.

2.2.2 Master

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

2.2.3 Cyber security office

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 delivered in the Cyber Security Policy Ch 2, Sec 4, [2].

2.2.4 Cyber security responsible

The cyber security responsible is, onboard, the executive responsible for establishing and maintaining the class notation Rules. 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 certificated. The cyber security responsible is appointed by the Shipowner and delivered in the Cyber Security Policy Ch 2, Sec 4, [2].

2.2.5 Shipowner

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

2.2.6 Shipyard

The Shipyard is responsible of systems installation and delivery

2.2.7 Vessel integrator

The vessel integrator is in charge of the cyber security of the unit. The vessel integrator is responsible of the integration of systems and equipment ordered by the shipyard or the Shipowner. The scope of applicability covers OT, IT and computer networks. If there are multiple parties proposing pre-integrated systems (as many OT Suppliers generally do), the vessel integrator must pay attention to connexions, 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 connexion or a software. The vessel integrator shall coordinate operations during the different stages of the vessel's life: from design to in-service life. If there are multiple system integrators, the vessel integrator is in charge of their coordination. The role of vessel integrator is under responsibility of the Shipowner or a third-party partner.

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. The supplier provides a description of the software functionality that meets the vessel integrator's specifications, the **CYBER SECURE** class Rules and applicable international or national standards.

2.3 Systems and equipment terms

2.3.1 The following definitions are used in this Rule Note for the various equipment and systems referred to in the requirements:

- a) Administration workstation are industrial systems (OT) of Category A (Cat. A) dedicated to administration of industrial system, servers, firewalls, switches...
- b) Ashore equipment: Refer 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, excluding airtime providers intermediate equipment.
- 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. 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.

- d) Engineering workstation are industrial systems (OT) of Category A (Cat. A) mostly stationary computers dedicated to industrial system process engineering.
- e) Equipment are identifiable 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 virtualized 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.
- f) Industrial systems: 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 system 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 both for OT and IT. For very specific cases, OT is stated in the rule.

- g) Level: The level characterizes the exposure of a system to cyber threats., and is determined with the Cyber Risk Analysis. See definition in Cyber Risk Analysis terms [2.3.3].

Level: formula (L). Level is calculated by using likelihood and impact. Rules apply to equipment depending of their level. Level 1 refers to unexposed equipment. Level 3 refer to very exposed equipment. Level 2 is intermediate.

- h) Onboard equipment: Refer to any IT and OT systems and equipment installed on the ship.
- i) Operator console are industrial systems (OT) of Category A (Cat. A) mostly mobile systems involved in industrial system process engineering and maintenance.
- j) 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 connexion point between different levels of risks. Sub-systems wording is not used in this document.

2.3.2 Cyber class notation terms

The following definitions of specific cyber security related terms are used in this Rule Note:

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

- **Hash:** Any function that can be used to map data of arbitrary size to data of fixed size. The values returned by a hash function are called hash values, hash codes, digests, or simply hashes. One use is a data structure called a hash table, widely used in computer software for rapid data lookup.
- **Monitoring:** Human procedures used to monitor events related to cyber security of equipment and systems.

2.3.3 Cyber risk analysis terms

The following definitions are used this Rule Note in relation to the Cyber Risk Analysis, as detailed in Sec 2.

- a) **Attacker:** formula (AT). Grade, from 1 to 5, which defines the requested competencies to successfully achieve a feared hazard. Attacker is part of the human factor formula.
- b) **Complexity:** formula (CX). Grade, from 1 to 3, which qualifies depth of parameters, amount of technologies and granted privileges of a system. Complexity is part of the exposition formula.
- c) **Connectivity:** formula (CY). Grade, from 1 to 5, which qualifies aperture of a system regarding accesses, exchanges and communications. Connectivity is part of the exposition formula.
- d) **Context establishment:** It is a first step of the Cyber Risk Analysis. This step defines mission and feared hazards (objectives). An inventory of process chain and equipment is also delivered. This step refines the scope of application of these Rules by identifying vital functions.
- e) **Effect:** Consequence of a feared hazard.
- f) **Exposition:** formula (E). Score, from 1 to 5, to measure the attack surface of a system. Complexity and connectivity are part of the formula. Exposition is part of the likelihood formula.
- g) **Feared hazard:** Cyber security events which are susceptible to have a huge impact.
- h) **Human factor:** formula (H). Score, from 0 to 4, to qualify non-technical elements susceptible to affect a cyber-event. Human factor is part of the likelihood formula.
- i) **Impact:** formula (P). Impact qualifies effect of a feared event. Impact may be negligible, acceptable, unacceptable, high or catastrophic.
- j) **Likelihood:** formula (K). Odds of having appearance of a feared hazard. Likelihood is based on human factor and exposition. Likelihood is part of the level and risk formulas.
- k) **Original risk:** The degree of risk from three degrees (negligible, significant, unacceptable) of a feared hazard before application of security measures whose those of the class notation.
- l) **Process chain:** Pieces of equipment which are used, as a technical chain, to achieve a function.
- m) **Risk:** formula (R). The degree of risk from three degrees (negligible, significant, unacceptable) of a feared hazard after application of security measures.
- n) **Security measures:** A list of technical or organisational elements used to reduce probability of appearance of feared hazards. The requirements from this Rule Note are security measures.

- o) Users: formula (U). Grade, from 1 to 4, which defines the awaited competencies to successfully counter a feared hazard. Users is part of the human factor formula.
- p) Vital functions is a short list of functions which are vital for the vessel's mission. Vital means both regarding operational objectives of the vessel and regarding the safety when managed by computer based equipment.

2.3.4 The following abbreviations/acronyms are used in this Rule Note:

AES	: Advanced Encryption Standard
APT	: Advanced Persistent Threat
CSR	: Compliance and Software Registry
CVE	: Common Vulnerabilities and Exposure
DMZ	: Demilitarized Zone
ELR	: Events and Logs Recorder
FIM	: File Integrity Monitoring
FW	: Firewall
GUI	: Graphical User Interface
HTTP	: Hypertext Transfer Protocol
HTTPS	: Hypertext Transfer Protocol Secure
ICS	: Industrial Control Systems
IDG	: Inspection and Decontamination Gate
IDS	: Intrusion Detection System
IOC	: Indicator Of Compromise
IP	: Internet Protocol
IPS	: Intrusion Prevention System
IPSEC	: Internet Protocol Security
LAN	: Local Area Network
MAC	: Media Access Control Address
NGFW	: New Generation Firewall
OSI	: Open Systems Interconnection model
PLC	: Programmable Logic Controller
RADIUS	: Remote Authentication Dial-In User Service
SIEM	: Security Information & Event Management
SNMP	: Simple Network Management Protocol
SPI	: State-full Packet Inspection
SSH	: Secure Shell
SSL	: Secure Sockets Layer
TCP	: Transmission Control Protocol
TLS	: Transport Layer Security
VLAN	: Virtual Local Area Network
VPN	: Virtual Private Networks
WAP	: Wireless Access Point
WLAN	: Wireless Local Area Network
WPA	: Wi-Fi Protected Access.

3 Documentation management

3.1

3.1.1 Roles

All the documents to be delivered are under responsibility of the vessel integrator 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 Privacy and protection of files

Files and/or numeric support are to be managed with a high security level. Human readable files contain a header mentioning the sensitivity level of the document.

Two levels of protection are used. The first level is SENSITIVE and the second one is CONFIDENTIAL.

For the SENSITIVE protection mark, the following rules apply:

- the files are not to be transmitted to unauthorized people.
- the files are not to be shared on public servers, public cloud storage, internet web mails, internet web address, internet websites, internet file sharing websites or internet file repository websites.

For the CONFIDENTIAL protection mark, the following requirements apply in addition to those applicable for the SENSITIVE Level:

- Files are kept in an encrypted and safe place both onboard and within Shipowner premises: all materials, documents and elements are encrypted while stored on removable media, endpoints (workstations, tablets, and smartphones), servers, file servers or cloud storage. Accesses to those information require identification and authentication mechanism.
- Files can be transmitted by using encryption procedures. When transferred, documentation is encrypted using a strong and dedicated encryption mechanism. Files are never sent to internet public web address.

3.1.4 Application

Vessel integrator is in charge to communicate its protection policy to relevant parties. However each relevant parties is responsible for the application of the protection policy.

3.1.5 Technical tests file format

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

3.1.6 Privacy and protection

Documents are protected according to [3.1.3].

At SENSITIVE Level:

- Cyber Security Policy
- Cyber Handbook
- Cyber Registry
- Equipment Administration Guide
- Equipment Operator Guide
- CSR User Guide
- ELR User Guide.

At CONFIDENTIAL Level:

- Cyber Risk Analysis
- Cyber Repository
- Cyber Survey Manual
- Equipment Security Mechanisms
- Vessel Cyber Design
- CSR Security Mechanisms
- ELR Security Mechanisms
- IDG Security Mechanisms.

3.1.7 Suppliers documentation

For Cat. A, Cat. B and Cat. C equipment, different documents are to be provided by the Supplier under control of the vessel integrator. A particular attention to the quality of the documentation is required.

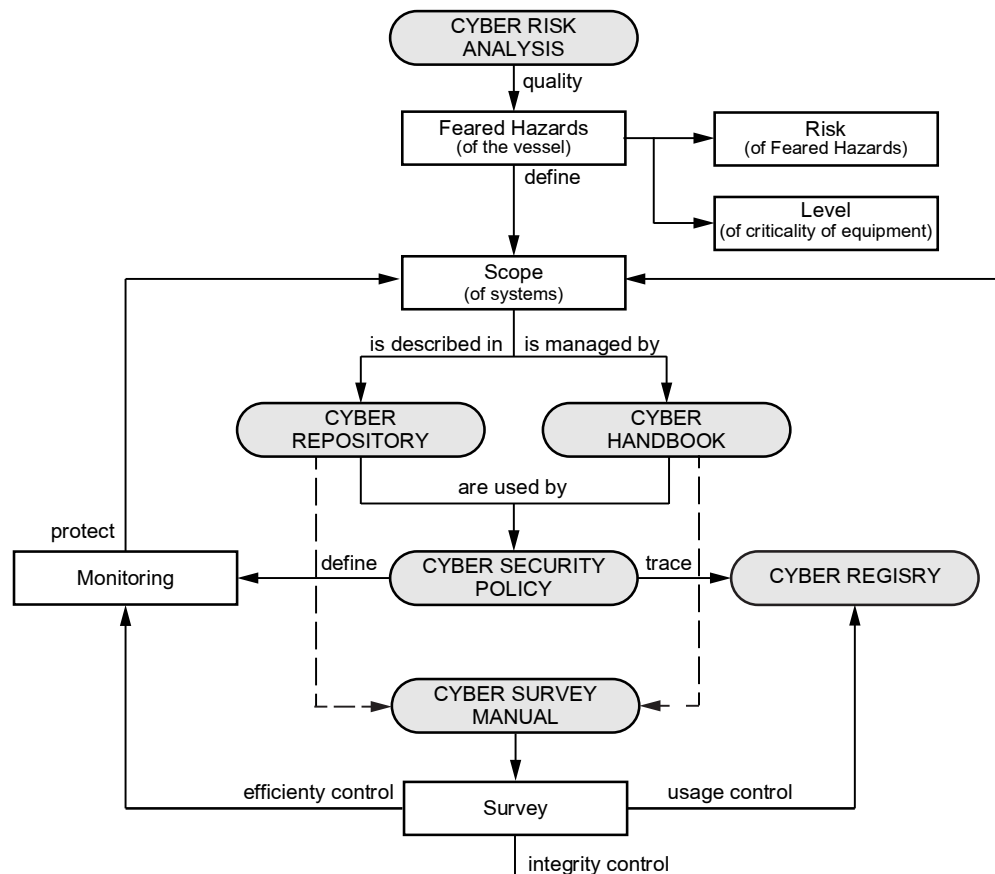
Moreover those documents are to be followed up by the vessel Integrator in order to get new versions in case of new issue. Equipment documentation writing is under Supplier responsibility. Specific elements, configuration or models used for the Equipment or the System are to be detailed.

3.1.8 Workflow

The following workflow and steps hereafter described (see also Fig 1) is to be followed in order to grant one of the additional class notation **CYBER MANAGED** or **CYBER SECURE**:

- The first step is about Cyber Risk Analysis writing which is used to output scope of systems to work on. This scope is defined by the qualification of Feared Hazards and Levels of criticality of equipment.
- The second step is to describe the systems and equipment in the Cyber Repository document, as defined in [4.1.3]. For the **CYBER SECURE** notation, it is an interactive process as the definition impacts the design and thus, the Equipment.
- The third step consists in collecting information about the maintenance of Equipment, such as guides and procedure.
- The fourth step is to set up the Cyber Security Policy, as defined in [4.1.2]. This is composed of human, organisational and technical procedures to use, protect and monitor the systems, taking into account the Cyber Repository and Cyber Handbook.
- The fifth step, is the Cyber Survey Manual which contain step-by-step procedures on systems and monitoring surveys. This document is to be based on the Cyber Handbook procedures.
- The last step is the Cyber Registry delivery which is not directly written during the class notation application. This document is empty but filled during vessel's life and used during surveys.

Figure 1 : Documentation delivery workflow



4 Documents to be submitted

4.1

4.1.1 Cyber risk analysis

The Cyber Risk Analysis is a document which, when issued, is updated during the whole life of the ship during major maintenance phase like system upgrades. To add, delete, modify or update an equipment will impact the Cyber Risk Analysis. The Cyber Risk Analysis is under responsibility of the Shipowner.

4.1.2 Cyber security policy

Cyber Security Policy is the main document for cyber security and cyber operation of the vessel in operation. This document is under responsibility of the Shipowner. It details rules and roles. It is used as a reference for any action on system and equipment by the crew members. The cyber security responsible is in charge to check and verify that the Cyber Security Policy is in place and applied by crew members and external partners. This document is to be printed on board and available at any time.

4.1.3 Cyber repository

The Cyber Repository contains elements, like security mechanisms, regarding systems and equipment inventories, expected and unexpected changes regarding hardware or software and configuration to apply on those assets.

The Cyber Repository is under responsibility of the cyber security Officer. He is in charge to keep it updated during the vessel lifecycle and to check the pertinence, quality and exhaustiveness of information.

The Cyber Repository contains administration tasks which require the highest level of privilege.

Administration tasks are dedicated to administration of the equipment. Administration operations are used in special case only like forensic investigation or software update.

The Cyber Repository is stored and managed ashore.

The Cyber Repository is not to be stored onboard.

4.1.4 Cyber handbook

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.

The Cyber Handbook procedures are under the responsibility of the cyber security responsible.

The Cyber Handbook contains operator tasks which require the intermediate level of privilege.

Operator tasks are dedicated to operational administration and maintenance of the equipment. Operator actions are typically account creation, system backup and so on.

The Cyber Handbook is stored and used onboard.

A Cyber Handbook is also to be delivered for ashore systems.

4.1.5 Cyber registry

The Cyber Registry is under the responsibility of the Master.

Each action, event or operation regarding equipment and systems is recorded and traced in this document.

Maintenance history and issues of Information Technologies and Operational Technologies Systems and Equipment are recorded and traced in this document.

The Cyber Registry may be in paper (i.e. logbook) or electronic format (i.e. database), stored onboard and, or, ashore (i.e. in the remote operation centre), searchable onboard and ashore, filled manually (i.e. recording of digital assets arrivals and departures), semi-automatically (i.e. copy and paste operations) or automatically (i.e. syslog).

The cyber security responsible is in charge to keep it updated in operation and to ensure exhaustiveness of information.

4.1.6 Cyber survey manual

Cyber Survey Manual contains tests dedicated to the equipment and/or its system. Those tests are performed within the vessel to verify both functional requirements and security mechanisms implementation.

Requirements about Cyber Survey Manual are defined in Chapter 4 of this Rule Note.

5 Regulation and standards

5.1

5.1.1 Purpose

For the purpose of application of this Rule Note, the standards listed in [5.1.2] could be used for:

- the development of hardware or software of computer based systems
- the connexion between systems and the global vessel integration
- the design of the Cyber Risk Analysis
- the management of the vessel and the crew members.

5.1.2 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
- BV-SW-200 / 20170609: Bureau Veritas LIST CEA Tech, Cybersecurity Guidelines for Software Development & Assessment
- CIS-Benchmarks: Centre for Internet Security guidelines to protect systems & platforms
- ENISA BS 7799-3 (Information security management systems)
- IACS UR E22: International Association of Classification Societies On board use and application of computer based systems - Rev.2 June 2016
- IACS No. 153 Recommended procedures for software maintenance of computer based systems on board
- IACS No. 154 Recommendation concerning manual local control capabilities for software dependent machinery systems
- IACS No. 155 Contingency plan for onboard computer based systems

- IACS No. 156 Network Architecture
- IACS No. 157 Data Assurance
- IACS No. 159 Network Security of onboard computer based systems
- IACS No. 160 Vessel System Design
- IACS No. 161 Inventory List of computer based systems
- IACS No. 162 Integration
- IACS No. 163 Remote Update Access
- IACS No. 164 Communication and Interfaces
- IMO MSC-FAL.1: International Marine Organisation - Guidelines on Maritime Cyber Risk Management - Circ.3 - 5 July 2017
- ISO/IEC 27005:2008 (Information security risk management)
- ISO/IEC 15408: Common Criteria for Information Technology Security Evaluation is an international standard for computer security certification. It is currently in version 3.1 revision 5
- ISO/IEC 27001: Information Security Standard, part of the ISO/IEC 27000 family of standards, of which the last version was published in September 2013. It specifies a management system that is intended to bring information security under management control and gives specific requirements
- NIST SP 800-39 (Managing Information Security Risk)
- NIST 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 RISK ANALYSIS

1 General

1.1 Framework

1.1.1 Objective

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

The application of **CYBER MANAGED** or **CYBER SECURE** notation contributes to the reduction of the identified risks.

The Cyber Risk Analysis does:

- enhance technical and human processes to reduce risks
- contribute to the risk management of the Shipowner.

The Cyber Risk Analysis does not:

- develop nor propose a management solution regarding security of information (as it is already defined in the class notation)
- certify nor homologate vessel's system
- deliver an information security policy (as it is under Shipowner responsibility).

1.1.2 Update

The Cyber Risk Analysis is to be updated with the vessel during any changes regarding the infrastructure, the architecture, the networks, the physical implementation of any system and equipment. The Cyber Risk Analysis lifecycle is integrated to the Change Management Plan (as required in Ch 2, Sec 4, [5.3.1]) in the Cyber Security Policy.

The Cyber Security Policy specifies the need for update as defined in Ch 2, Sec 4, [1.1.1].

1.1.3 Delivery

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

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

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

The whole vessel is in the scope of the Risk Analysis as each System shall be checked in order to evaluate its complexity, connectivity and, thus, criticality.

The Cyber Risk Analysis can be written:

- by the vessel integrator itself
- by a third-party partner.

1.1.4 Methodology

The Cyber Risk Analysis may be performed in accordance with the methodology proposed in this Section or those listed in [1.1.5].

1.1.5 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)
- ISO/IEC 27005:2008 (Information security risk management)
- NIST SP 800-39 (Managing Information Security Risk).

However the evaluation of the Level of equipment required in [3.6.3] is to be delivered for every equipment included in the Scope of application defined in [2.3].

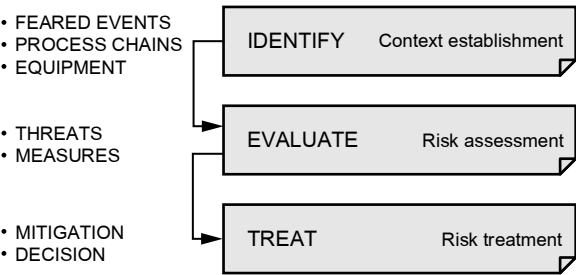
1.2 Workflow

1.2.1 Objective

The Cyber Risk Analysis is divided into 3 steps:

- Context establishment: identifies values on which the scope of the notation strictly apply to (see Fig 1). An inventory of process chain and equipment is also delivered. This step defines the scope of application of the classification notation.
- Risk assessment: evaluates threats and security measures by measuring impacts and likelihoods.
- Risk treatment: identifies either mitigation measures or residual risks, if any.

Figure 1 : Cyber risk analysis workflow



1.2.2 Principle

There are different ways to consider the risk management as it may be used to address different kind of objectives. The Cyber Risk Analysis requested in this notation measures the residual risks regarding feared hazards and, in conclusion, helps the Shipowner to take a decision about mitigation measures to install (see Fig 2).

The entry point is thus the vessel's missions which need vital functions to operate but wish to avoid feared hazards. Vital must be understood here as regarding both operational objectives of the vessel and the safety when managed by computer based equipment.

Vital functions are achieved through process chains which are exposed to threats. Threats are ways to exploit the feared hazards. So, threats affect the risk.

The risks are then reduced by using the already existing security measures listed from:

- organizational and human monitoring procedures defined in Cyber Security Policy document whose rules are shaped from the requirements rules defined in this document.
- survey operations used to control both monitoring operations and equipment themselves. Survey operations are

defined in the Cyber Survey Manual whose requirements are derived from the requirements defined in this document for the applicable classification notation.

- When **CYBER SECURE** notation is assigned:
 - equipment monitoring automation which reinforce the efficiency of monitoring operations
 - equipment secured by design and vessel's infrastructure rules which harden IT and OT equipment
 - equipment survey increases the level of confidence regarding the security of the equipment and, at the end, decreases the likelihood of feared hazards
 - other vessel or Shipowner security measures, both technical and procedural, which are not included in the class notation nor in the Cyber Security Policy.

The residual risks are then mitigated by using decision explained in the Cyber Risk Analysis.

1.2.3 Table of contents

The Cyber Risk Analysis may be delivered by using the guiding thread of this Section. The guiding thread of this Section is summarized in Tab 1.

Figure 2 : Cyber risk analysis overview

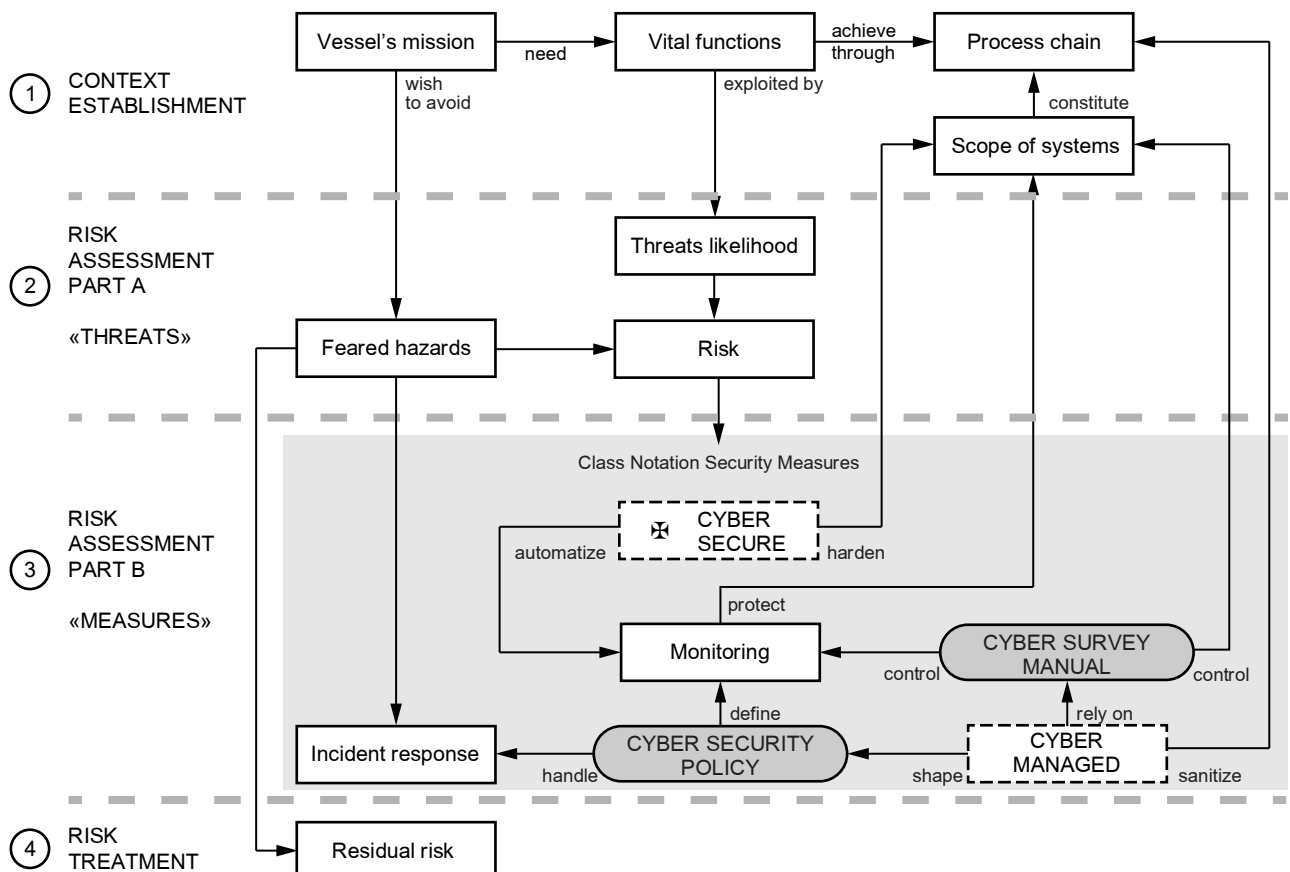


Table 1 : Table of contents of a cyber risk analysis

	Chapter	Reference
IDENTIFICATION	Scope	
	Mission	[2.1.1]
	Vital functions	[2.1.2]
	Inventory	
	Onboard equipment	[2.2.2]
	Onboard systems and architecture	[2.2.3] [2.2.6]
	Ashore equipment	[2.2.4]
	Ashore systems and architecture	[2.2.5] [2.2.6]
	Process chain	[2.3]
RISK ASSESSMENT	Feared hazard	
	Feared hazards and impacts	[3.2.5]
	Threats likelihood	
	Likelihood score	[3.3.4]
	Level of equipment	[3.6.3]
	Evaluation	
	Risk assessment	[3.7.5]
	Conclusion	
	Decisions on risks	[4.1.2]

2 Context establishment

2.1 Scope

2.1.1 Mission

As an introduction, the Cyber Risk Analysis summarizes strategic elements regarding the context of risk of the vessel:

- define external context of usage (i.e. remote controlled, autonomous systems, remote maintenance, IT management, passenger WiFi, etc.) and relevant risks regarding confidentiality, integrity or availability.
- define internal context (i.e. IT & Cyber resources, IT links, company strategic objectives, contractual external actors, identified internal risks, top view of sources of risks from IT users, etc.).

The first part is used to identify the challenges to face. Those challenges may apply both on OT safety systems using computer based equipment (i.e. propulsion) and on IT systems installed onboard and having an impact in term of efficiency of the vessel-s mission (i.e. passengers services).

2.1.2 Vital functions

By using external and internal challenges developed in [2.1.1], vital functions are identified, selected and justified by the Shipowner. Those vital functions may for example concern:

- confidential information (i.e. performances, fuel consumption)

- OT systems (i.e. propulsion systems)
- personal information (i.e. medical)
- safety systems (i.e. dynamic positioning).

In order to achieve this objective, the study may start with an exhaustive approach of large and general groups, followed up with a selection of vital functions. The objective is not to deliver an exhaustive list of functions as vital but to deliver a list of indisputable vital functions whom criticality has been established as a priority.

For remote access type of connexions, refer to Ch 2, Sec 3, [1.1.1].

Schemes of vital functions workflows may be attached (i.e. remote assistance workflow).

2.2 Inventory

2.2.1 Terms

Refer to Sec 1, [2.3.4] for a definition of terms.

2.2.2 Onboard equipment

Onboard equipment listing relies on the software inventory as detailed in Ship Rules, NR467, Pt C, Ch 3, Sec 3, [4.5]. The detailed software inventory is an input for the Cyber Risk Analysis.

2.2.3 Onboard systems

When an equipment if part of a pre-integrated system (multiple equipment as defined in Ship Rules, NR467, Pt C, Ch 3, Sec 3, [8.1]), the system is to be detailed equipment per equipment.

The category of each equipment is to be specified in accordance with the definition from Sec 1, [2.3.3] definition.

Cat. A equipment used into OT systems (Operational Technology) are inventoried and labelled in one of the three following category:

- 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...).

Each equipment is to be linked to those inventoried in the software registry (Ship Rules, NR467, Pt C, Ch 3, Sec 3 about system administration guide).

Tab 2 presents an example of onboard system table.

2.2.4 Ashore equipment

Ashore equipment are identified by using Ship Rules, NR467, Pt C, Ch 3, Sec 3, [4.5]. The detailed inventory is built and delivered as an input.

2.2.5 Ashore systems

Equipment installed ashore and used for IT and OT remote communications are listed in the same way than onboard systems [2.2.3].

Ashore systems are to be detailed in a separated table.

Tab 3 presents an example of ashore system table.

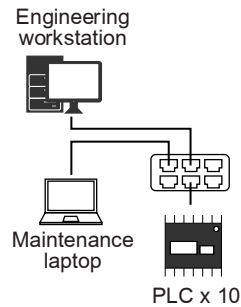
Table 2 : Example of onboard systems table

Type		Equipment category	
		IT	OT
IT	Server	A	-
	Client	A	-
Some system	Switch	-	B
	PLC	-	C
	PC	-	A
	Laptop	-	A
Remote link	Modem	B	-
	Firewall	B	-
	DMZ	A	-
	Switches	B	-
	...	...	-

Table 3 : Example of ashore systems table

Type	Category
Control center	Modem
	Firewall
	Authentication
	VPN
	...

Figure 3 : Example of system architecture



2.2.6 System architecture

For each system, a detailed drawing presents equipment installed within the system. Local connexions, external interconnections and data transportation over the networks are to be detailed (see Fig 3).

2.3 Process chain

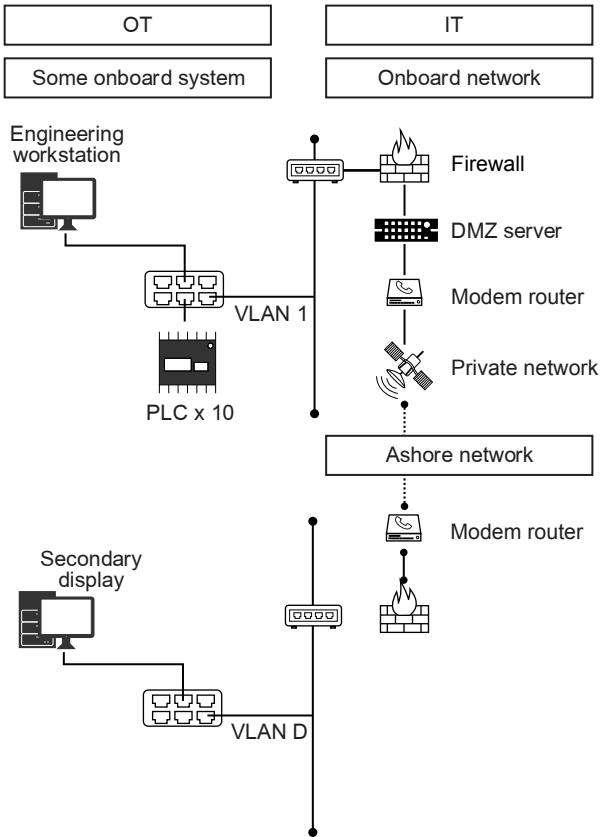
2.3.1 Systems and equipment are linked to the vital functions. The objective of process chain is to identify equipment which are essential to deliver the services of the vital functions.

A logical and a physical scheme develop the process chain of each vital functions (i.e. ground computer, satellite link, vessel IT router, vessel VLAN over the IP network, OT firewall, SCADA computer, automation) (see Fig 4).

Table 4 : Process chain table example

Type	Category	Location
Some system	PLC	OT C
	Switch	OT B
	PC	OT A
Network	Switch X	IT B
Remote link	DMZ	IT A
	Firewall	IT B
	Modem router	IT A
Control center	Modem router	IT B
	Firewall	IT B
	Switch VLAN D	IT A
	PC Display	IT A

Figure 4 : Process chain example



The chain of equipment is to be detailed in a table by using a logical chain of succession.

A brief description of the chain is explained. Example presented in Tab 4 could be described as for example 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”.

3 Risk assessment

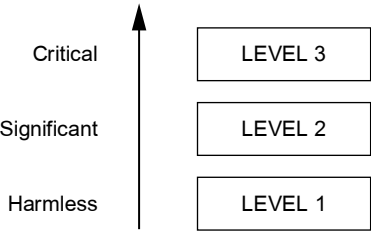
3.1 Criticality level

3.1.1 Definition

The level of criticality of an equipment is referred to as “Level” in this Rule Note.

The Level does not take into account the benefits of security measures applied by the class 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 human processes depend on the assigned Level (see Fig 5).

Figure 5 : Scale of criticality



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 and Shipowners.

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

Each equipment and system is classified by assigning of the 3 following levels, depending of their exposition, consequences and threat.

- Level 1: IT or OT systems for which risk of attack is low. May be connected. They are supervised.
- Level 2: IT or OT for which risk of attack is significant. Mandatory and specific rules appear.
- Level 3: IT and OT systems for which risk of attack is high. Use of dedicated procedures, systems or functions appear.

3.1.2 Level assignment

Systems are associated to a Level by using the methodology described in [3.1.3].

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.

3.1.3 Methodology

The criticality level (Level 1, Level 2 or Level 3) is calculated depending on 2 parameters: Likelihood and Impact (see Fig 6).

- The likelihood considers user access and considered skill level of the attacker, and is subdivided in the two following indexes:
 - exposition, taking into account the connectivity and complexity of the system

- human factor, taking into account the risks coming from users and external, malicious users.
- Impact is related to the feared hazards and their consequences on the vital functions, as detailed in [3.2].

3.2 Feared hazard

3.2.1 Objective

This step analyses impact on vital functions by developing scenarios of feared hazards and of their consequences in order to determine the impact index. These scenarios are to be summarized by means of a table (see Tab 5), to be submitted for information.

3.2.2 Hazards

Each scenario is presented and briefly developed in order to help to determine, evaluate and justify score of impact.

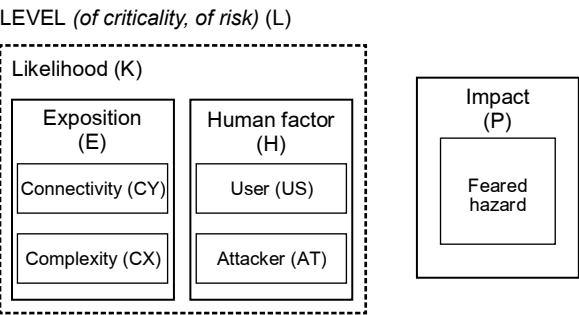
Operational and practical situations are preferred to global or general approaches.

3.2.3 Effects

The Shipowner shall consider the following effects:

- Operational effects
 - Impacts on the mission: direct or indirect impact regarding the vessel's mission (i.e. service cannot be delivered anymore, loss or disclosure of information, loss of control on automation, etc.) at sea or at quay.
 - Impacts on command chain: direct or indirect impact regarding the vessel's control (i.e. unusable systems, equipment encryption, vessel hijacking, etc.) at sea or at quay.
- Human effects
 - Direct or indirect consequence on integrity of the persons (i.e. divers' injury while undersea, loss of walkway stability during people transfer, air-conditioning system disruption, etc.).
- Shipping effects:
 - Direct or indirect consequence on integrity of the goods (i.e. loss of containers, loss of safety protection for hazardous materials, etc.).
- Financial effects:
 - Direct or indirect financial consequences (i.e. loss of corporate image, loss of customers, discounts, fines, insurance premium accrual, etc.).

Figure 6 : Level of criticality components



3.2.4 Impact (P)

The impact index P is determined according to the following definitions:

- Impact 1 (P1): Negligible. system could be shutdown without any significant effect. No human nor environmental impacts are involved.
- Impact 2 (P2): Acceptable. Shutdown of the system means a pointed disrupt of the service. Event could lead to labour disruption because of medical treatment. Environmental impact is in the standard margin and has no consequence but to be declared to authorities.
- Impact 3 (P3): Unacceptable. Loss of system activity is significant. Shipowner request investigations from a third-party committee. Human impact could lead to permanent disability. Environmental impact is limited.
- Impact 4 (P4): High. Loss of system is permanent and no standard restoration process can help to restart the system in its operational state. Ship is off. The regulatory asks for investigation. Human impact could lead to death. Significant pollution conducts to people evacuation.
- Impact 5 (P5): Catastrophic. Loss of ship systems or ship itself. Fleet is off due to investigation regarding scope of cyber-attack. Major pollution with long-term environmental consequences and multiple death could appear.

3.2.5 Delivery

A table presenting the following elements is to be submitted (see Tab 5):

- feared hazards
- location (at sea, at quay)
- source of event (people and, or, technologies involved in the hazard)
- effects (as described hereinbefore)
- impact (as described hereinbefore).

Table 5 : Hazard impact example

Hazard	Location	Threats	Effect	Impact (P)
Loss of propulsion	At sea	Loss of equipment compliance	Delays Marine rescue	4
Loss of control	Fulltime	Encrypted station (ransomware)	Manual control	4
Passengers doors locked	At sea	Private remote control	Panic	5

Table 6 : Threats likelihood delivery example

Threats	source	CX	CY	E	US	AT	H	K
Some system "PC OT A"								
Loss of equipment compliance	Human error	2	2	2	1	2	1	3
Encrypted station	Common ransomware	2	2	2	1	3	2	4
Private remote control	Targeted attack	2	2	2	1	4	2	4
Note 1: CX : Complexity = E : Exposition K : Likelihood AT : Attackers CY : Connectivity = H : Human factor US : Users								

3.3 Threats likelihood (K)

3.3.1 Objective

The threats revealed in impact study of feared hazards are now evaluated in term of likelihood.

Threats on the process chain are developed in this step.

The objective is to list paths of cyber-attacks on the process chain. Threats may be described in a narrative way or by using a table. Each threat is to be submitted with:

- one or more source of attack
- a level of likelihood.

Sources of attacks are chosen from predefined list here delivered (i.e. slack crew member, malicious remote operator, careless maintenance staff member, common virus, script-kiddies passenger, etc.)

Threats are freely chosen.

3.3.2 Likelihood score

The likelihood describes the odds of being under attack.

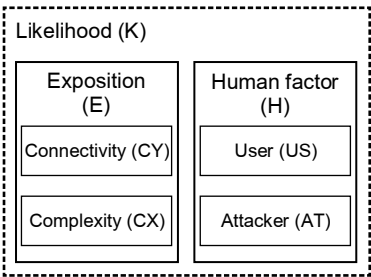
The Likelihood (K) is the result of the addition of Exposition (E) and Human Factor (H).

Likelihood = Exposition + Human Factor

K = E + H

To score the Exposition (E), Connectivity (CX) and Complexity (CX) of the equipment is determined by using [3.4]. To score the Human Factor (H), Users (US) and Attacker (AT) are determined by using [3.5]. See Fig 7.

Figure 7 : Likelihood composition



3.3.3 Example

“PC OT A” is an OT engineering computer used to control PLC of “Some System”:

- CX : System Connectivity [3.4.2]), is 2 because from a logical point of view, the secondary system doesn't connect to the system. All connexions are initiated by the system to the attention of the secondary system
- CY : System Complexity [3.4.3]), is 2 because it is an ICS supervisor
- E : Exposition is 2 as determined in [3.4.4]
- US : Users [3.5.2]), is 1 because crew is trained and events are logged
- AT : Attackers [3.5.3]), is 2, 3 and 4 depending on the 3 Sources (Human Error, Malicious Attack, Targeted Attack)
- H : Human Factor is 1 and 2 as determined in [3.5.4]
- K : Likelihood is, at the end, 3 and 4.

3.3.4 Delivery

Threats are presented in Tab 6 showing, for each of them, sources and likelihood score.

3.4 Exposition (E)

3.4.1 Definition

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

3.4.2 Connectivity (CY)

Connectivity 1:

This grade is only for isolated system. Isolated system means a system without any network interconnection except those dedicated for the system itself (see Fig 8). Usage of a network and a switch without external connexion is accepted for Connectivity 1.

Figure 8 : Connectivity 1 example

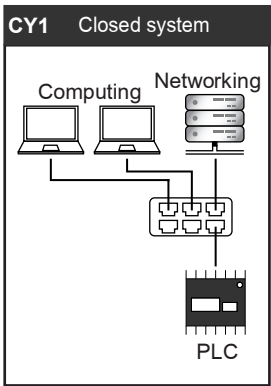


Figure 9 : Connectivity 2 example

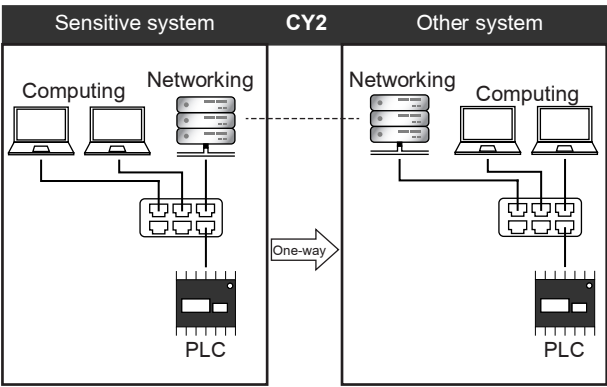


Figure 10 : VPN IPsec

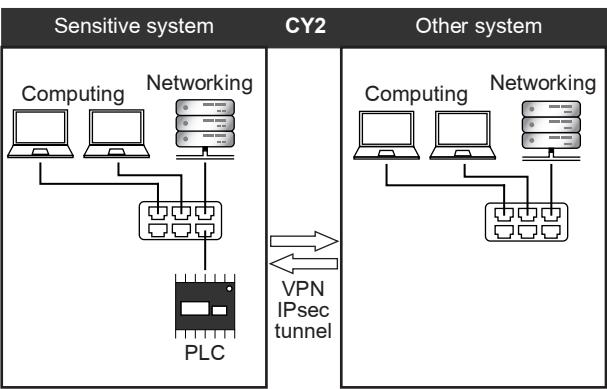


Figure 11 : Connectivity 3 example

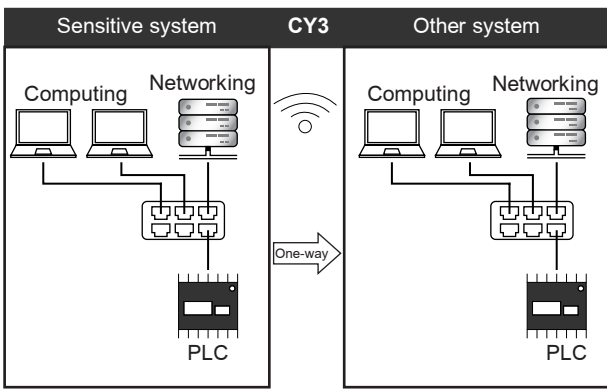
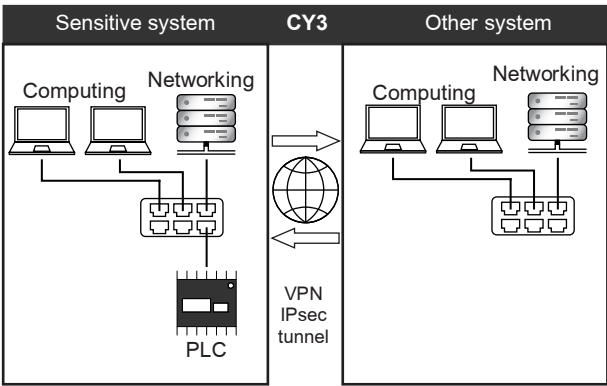


Figure 12 : VPN IPsec public network



Connectivity 2:

- System is interconnected to another system. Interconnection means network connexion to another system. But, from a logical point of view, the secondary system doesn't connect to the system. All connexions are initiated by the system to the attention of the secondary system (see Fig 9). Connexions are managed inside an encrypted tunnel like VPN SSL. Only connexions from the inside to the outside are authorized. This is typically DMZ configuration.
- System is interconnected to another system. Interconnection means network connexion to another system. There is no restriction regarding way of connexion. But the traffic is fully encrypted at client level in a Layer 3 tunnel (IPsec fully tunnelled).

Connectivity 3:

- Applicable to Connectivity 1 and 2 systems which employ and use wireless connexions (see Fig 11).
- System interconnected to another system by employing VPN IPsec communication through public network (see Fig 12) in order to trust source.
- System is interconnected to another system. Interconnection means network connexion to another system. There is no restriction regarding way of connexion. But the traffic is encrypted in a VPN SSL and there is no other traffic than the one transported through the VPN SSL (see Fig 13).

Connectivity 4:

- System host one or more services which can be accessed, operated or used from a secondary system through a distant link - like a Local Area Network (LAN). Connexions are done by using a private network which is neither managed nor mastered by one of the two systems (see Fig 14). This could be, for example:
 - network services (e.g. data, printing sharing...),
 - web services (e.g. web, file transfer server...),
 - administration services (e.g. remote administration...),
 - maintenance services (e.g. remote engine manufacturers).

- System is interconnected to another system. Interconnection means network connexion to another system. There is no restriction regarding way of connexion. But the traffic is encrypted in a VPN SSL (clientless encryption). Systems are connected to a public network (i.e. Internet) with a traffic disruption (i.e. DMZ or Bastion) see Fig 15.

Connectivity 5:

System deliver services for public access. Clients from public network can connect to the onboard system (see Fig 16). The public network may be Internet. For example: a Supplier using Internet to directly connect to a vessel system, through tunnel VPN SSL.

Figure 13 : VPN SSL

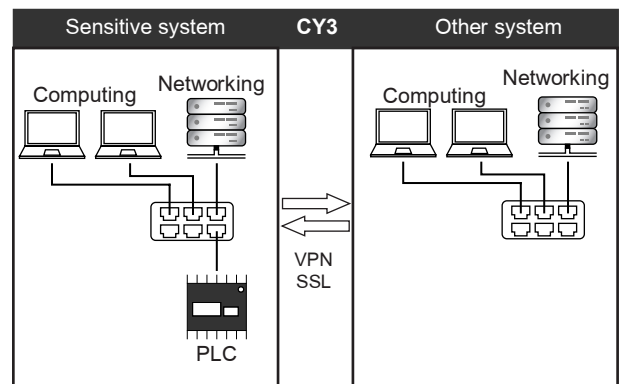


Figure 14 : Connectivity 4 example

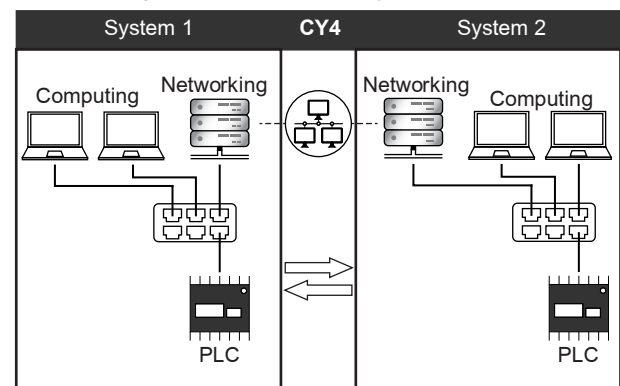


Figure 15 : SSL and disruption

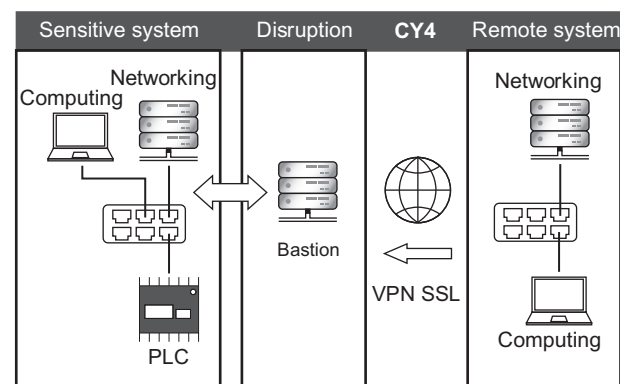
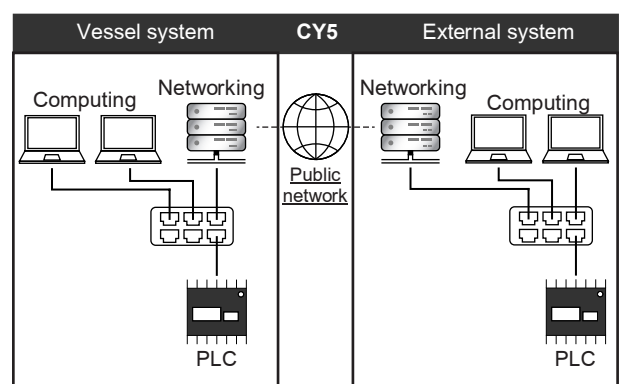


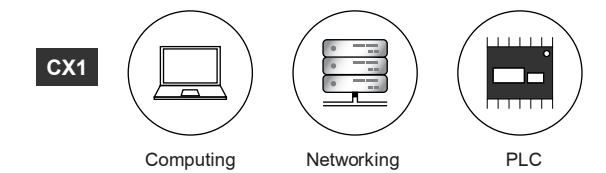
Figure 16 : Connectivity 5 example



3.4.3 Complexity (CX)

Complexity 1: OT/IT systems have workstations and light servers (see Fig 17). Restoration procedures of those systems are easy to apply. Administration level is standard. OT systems are made of sensors, controllers, consoles and control commands.

Figure 17 : Complexity 1 areas



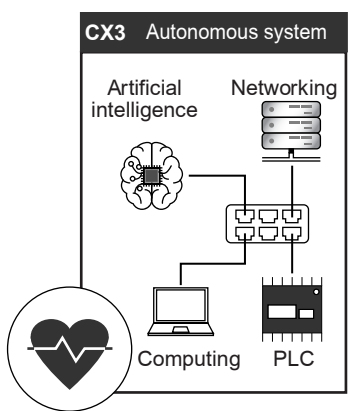
Complexity 2: IT systems which host authentication servers, databases servers, calculator or any server sized to answer to reliability purposes (see Fig 18). Administration requires dedicated skills. OT systems contain supervision or programming workstations. For example, this grade applies to maintenance systems, critical systems or autonomous systems.

Figure 18 : Complexity 2 areas



Complexity 3: IT and OT systems whose efficiency requires systems dispatched through remote or distributed architecture (see Fig 19). This grade typically applies to unmanned systems, swarm connexions or any systems whose availability is linked to a high density of system exchange.

Figure 19 : Complexity 3 example



3.4.4 Exposition score

The exposition score is the combination of Complexity (CX) and Connectivity (CY) as defined in Fig 20.

- for Complexity 1, the Exposition Score equals the Connectivity Level
- for Complexity 2, the Exposition Score equals the Connectivity Level, without being taken less than 2
- for Complexity 3, the Exposition Score is 3 for Connectivity 1–2, 4 for Connectivity 3–4 and 5 for Connectivity 5.

3.5 Human factor (H)

3.5.1 Definition

Human Factor (H) is the conjunction of users' level of maturity and attackers motivation (see Fig 20). In one hand, users training and activity recording is taken into account. In another hand, attackers' level is evaluated.

Figure 20 : Exposition score (E)

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

3.5.2 Users index (US)

- Users index is 1 (US1) when users are authorized, trained and actions are logged.
- Users index is 2 (US2) when users are authorized but not trained. Actions are partially logged.
- Users index is 3 (US3) when users are not trained and actions are not logged.
- Users index is 4 (US4) when users are unknown.

(See Fig 21).

Figure 21 : User level (US)

	 Authorized users	 Actions recording	 Trained users
H1	✓	✓	✓
H2	✓	✓	
H3	✓		

3.5.3 Attackers index (AT)

The Attack index AT is ranging from 1 to 5, depending on the level of complexity and skill of the attacker. 1 corresponding to the lowest level and 5 to the most advanced attacks. The level is freely selected in accordance with the target of evaluation.

- Attackers' index is 1 (AT1) when attackers are considered users having unintentionally and accidentally introduced common, untargeted virus and malwares.
- Attackers' index is 2 (AT2) when attackers are users trying to bypass system security without malicious intention.
- Attackers' index is 3 (AT3) for malicious attackers (at sea or on shore employee, sub-contractor) using hacking tools and technics.

- Attackers' index is 4 (AT4) when attackers are using organisation means (criminal organisation, competitor) to construct scenarios of attacks.
- Attackers' index is 5 (AT5) when attackers are considered using governmental attacks.

3.5.4 Human factor score

The Human Factor score H is calculated from Users index (US) and Attackers index (AT) according to Fig 22.

Figure 22 : Human factor score (H)

HUMAN FACTOR	H =	USERS			
		US1	US2	US3	US4
	AT1	H0	H1	H1	H2
	AT2	H1	H1	H2	H2
	AT3	H1	H2	H2	H3
	AT4	H2	H2	H3	H3
	AT5	H2	H3	H3	H4

3.6 Level (L)

3.6.1 Objective

The Level contributes to determine Rules which will be later considered during the application of the Rules and survey operations.

To avoid rules limitation regarding the final Level (1, 2 or 3), vessel integrator may consider to adapt design of the vessel for systems having a high impact regarding the following graduation. Such systems may be limited in term of equipment (cost reduction) but also limited in term of connectivity or complexity (exposition and thus likelihood reduction).

3.6.2 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 23

Figure 23 : Level (of equipment) score table

IMPACT (P)	LIKELIHOOD (K)						
	K1	K2	K3	K4	K5	K6	K7+
	p1	LEVEL 1					
	p2						
	p3		LEVEL 2				
	p4				LEVEL 3		
	p5						

Table 7 : Equipment level delivery example

System/equipment	K	P	L
Some system			
PC OT	4	5	3

3.6.3 Delivery

To conclude, an intermediate table with Likelihood (K) and Impact (P) indicators for systems and equipment involved is to be provided (see Tab 7). At the end, Level is determined thanks to the Level Score Table (see Fig 23).

3.6.4 Example

K and P are taken from Tab 6 and Tab 5. Maximum Likelihood and Impact scores are used. As a conclusion, PC Engineering used in "Some System" is Level 3.

3.7 Risk calculation

3.7.1 objective

Risk calculation is the final operation of the risk assessment. The Cyber Risk Analysis is a dynamic process, an intellectual 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 study case by case.

That is the reason why Cyber Risk Analysis is required. Nevertheless, in order to easily integrate the set of rules applicable according to the requested classification notation, a quick and easy way to consider and to calculate risk is proposed in [3.7.2] to [3.7.5] hereafter.

3.7.2 Security measures

- Security measures are:
- applicable requirements depending of the selected classification notation)
 - architecture principles (i.e. DMZ, etc.)
 - physical protection (i.e. locked room, optical fibre, etc.)
 - specific capabilities of the equipment
 - certifications for the equipment
 - vessel's infrastructure architecture
 - special usage of security solutions
 - etc.

From this point, the requirements applicable to the selected classification notation are developed and taken into account in the proposed risk process. It is up to the Shipowner to add its own specific and special security measures and to write a rationale regarding the risk.

3.7.3 Risk metrics

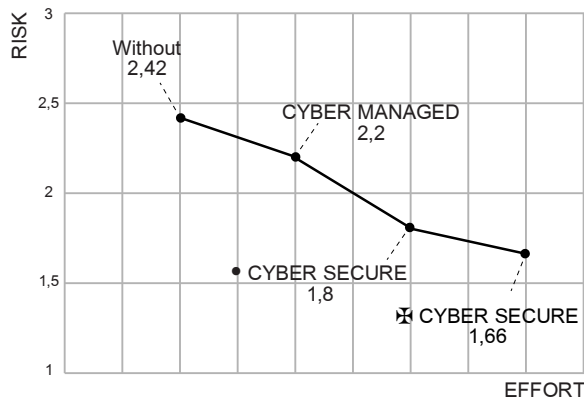
- Three degrees of risk are used: negligible, significant and unacceptable:
- Negligible (R1) are risks that are covered by the security measures. Of course, the risk still exist.
 - Significant (R2) is a degree for risks covered by the security measures but which still need to be regularly tracked and presented at board level. Risk treatment may be introduced to reduce the risk
 - Unacceptable (R3) are risks that are partially covered by the security measures, but those risks need a dedicated treatment in order to reinforce the security and to reduce the risk to a significant (R2) score.

Thanks to the counter-measures that the class notation will introduce to identified systems, the average score of risk will decrease depending of the selected classification notation.

To figure out this, let’s build a diagram with risk measure on ordinate axis and on abscissa axis. The score has been calculated from different combinations of impacts regarding trained users versus motivated attackers.

In this example (Fig 24), without notation, a score of 2,42 on 3 is reached. Compliance with **CYBER MANAGED** notation decreases the risk to 2,2. Note that the average is still above the significant (R2) level of risk because **CYBER MANAGED** relies on human factor and does not require changes on infrastructure. In those conditions, with **CYBER SECURE** notation, the score drops to 1,8 on 3 which is an important gap. Considering **CYBER SECURE** notation, the score reaches 1,66, a good median on the scale of our risk metrics.

Figure 24 : Average class notation impact on the risk



Two degrees of risks are established for each feared hazards:

- The first one is the degree of risk without security measures (“before” application of the classification notation requirements and relevant actions). It is called Original Risk (OR) and is detailed in [3.7.4].
- The second one is the residual degree of risk (on which risk treatment will work on to decide, for example, to apply mitigation measures). It is simply called risk (R) and detailed in [3.7.5].

3.7.4 Original Risk (OR)

The first degree of risk is easy to retrieve: the Level of equipment (L) calculated in [3.6.2] is directly reported as a degree of Risk:

- Level 3 equipment, means an unacceptable risk (R3)
- Level 2 equipment, means an significant risk (R2)
- Level 1 equipment, means an negligible risk (R1).

Original risk may be reported and evaluated in an intermediate table (see Tab 8). The original risk may be reconsidered and revaluated with a justification. Shipowner may decide a risk as overrated or under rated.

Table 8 : Original risk from equipment level

System/equipment	Original risk
Some system	
PC OT	Unacceptable

3.7.5 Risk (R)

The second degree of risk takes into account the security measures, thus the application of the requirements from the applicable classification notation, as described in [3.7.2].

As for original risk, the present risk may be reconsidered and revaluated with a justification even after application of classification notation bonuses described hereafter. Shipowner may decide a risk as overrated or under rated. Special and dedicated security measures may enter in this judgement.

To recalculate this risk, the following bonuses are considered, depending on the selected notation:

- Complexity index CX: as systems and infrastructure designs are explained in the Cyber Repository and under control of the cyber security responsible, Complexity index CX is reevaluated from **CYBER MANAGED** notation. A reduction of –1 on the initial value is granted for **CYBER MANAGED** and –2 for **CYBER SECURE**.
- Connectivity index CY: connectivity principles are hardened from **CYBER SECURE**. A reduction of –1 on the initial value is granted for this notation and –2 is granted to **CYBER SECURE**.
- Attackers index AT: taking into account equipment monitoring, equipment hardening and equipment certification, the attackers' skills needs to increase. A reduction on the initial value is granted for
 - 1 for **CYBER MANAGED**,
 - 2 for **CYBER SECURE** and
 - 3 for **CYBER SECURE**.

Tab 9 presents those principles.

Threat calculation shall be consolidated by re-using likelihood elements from Tab 6 with new elements as developed in Tab 10 and Tab 11.

Table 9 : Risk reduction bonuses

	CYBER MANAGED	• CYBER SECURE	✕ CYBER SECURE
Complexity (CX)	–1	–2	–2
Connectivity (CY)	0	–1	–2
Attackers (AT)	–1	–2	–3

4 Risk treatment

4.1 Residual risks

4.1.1 Selection

As risk treatment has already been applied through the application of the Rules and survey operations according to the classification notation, the Cyber Risk Analysis directly treat Residual Risks.

Risk at degree 3 (unacceptable) are not accepted and mitigation measures shall be reconsidered in order to reevaluate the risk in an iterative process.

Risk at degree 2 (significant) are considered residual risks.

Risk already, always and still exist. The objective of the Cyber Risk Analysis is no 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.

The residual risk may be reconsidered and reevaluated with a justification. Shipowner may decide a risk as residual or no.

4.1.2 Decision on risks

Decisions about risks identified as residual risks need to be taken. The Shipowner decides about the strategy to employ in order to cover risks.

The following actions may be used:

- Avoid: change the context in order to be disengaged of the risk.
- Reduction: introduce new mitigation measures in order to cut down impact and, or, likelihood. Mitigation measures may be:

- organisational by installing new procedures
- technical by dedicating a cyber security component like i.e. a firewall
- physical by introducing i.e. locks, optical fibres or room controls
- dedicated monitoring: this is of course considered as a security measure
- increased frequency of an already existing monitoring procedure.
- quality driven by using certified equipment
- etc.

- Assume: take the risk without any security measure
- Transfer: use a third-party operator to cover the operation and, thus, the risk.

A rationale, in a table or in plain-text, is to be submitted to explain decisions about risk treatment.

Table 10 : Risk evaluation example

Threats	Source	CYBER MANAGED bonuses							P	R
		CX	CY	E	US	AT	H	K		
Some system PC OT A										
Loss of equipment compliance	Human error	1 (2)	2 (2)	2 (2)	1	1 (2)	0 (1)	2 (3)	4	2 (2)
Encrypted station	Common ransomware	1 (2)	2 (2)	2 (2)	1	2 (3)	1 (2)	3 (4)	4	2 (3)
Pirate remote control	Targeted attack	1 (2)	2 (2)	2 (2)	1	3 (4)	1 (2)	3 (4)	5	3 (3)
Note 1: (Original) Original values are display with parenthesis										
Note 2:										
CY		:	Connectivity	K	:	Likelihood	R	:	Risk	
AT : Attackers		=	E : Exposition	P	:	Impact	US	:	Users	
CX : Complexity		=	H : Human factor							

Table 11 : Example of • CYBER SECURE bonuses

Threats	Source	● CYBER SECURE bonuses							P	R
		CX	CY	E	US	AT	H	K		
Some system PC OT A										
Loss of equipment compliance	Human error	1 (2)	1 (2)	1 (2)	1	1 (2)	0 (1)	1 (3)	4	2 (2)
Encrypted station	Common ransomware	1 (2)	1 (2)	1 (2)	1	1 (3)	0 (2)	1 (4)	4	2 (3)
Pirate remote control	Targeted attack	1 (2)	1 (2)	1 (2)	1	2 (4)	1 (2)	2 (4)	5	2 (3)
Note 1: (Original) Original values are display with parenthesis										
Note 2:										
CY : Connectivity K : Likelihood R : Risk										
AT : Attackers = E : Exposition P : Impact US : Users										
CX : Complexity = H : Human factor										