Cybersecurity Requirements for Products to be Installed On-Board Naval Ships

July 2018

Rule Note
NR 642 DT R00 E

Marine & Offshore
92937 Paris la Défense Cedex – France
Tel: + 33 (0)1 55 24 70 00
Website: http://www.veristar.com
Email: veristarinfo@bureauveritas.com

MARINE & OFFSHORE - GENERAL CONDITIONS

1. INDEPENDENCY 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, 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 Services are carried out by the Society according to the applicable Rules and to the Bureau Veritas' Code of Ethics. 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 the Services' performance and con tract's execution.

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 class certificates, attestations and reports following the Society's intervention. The Certificates are an appraisement 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.

2.2. "**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 class certificate with reference to the Rules.

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 proto cols 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 register published annually by the Society.

2.11. "**Rules**" means the Society's classification rules, guidance notes and other documents. The Rules, procedures and instructions of the Society 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, training activities, all activities and duties incidental thereto such as documentation on any supporting means, software, instrumentation, measurements, tests and trials on board.

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 the 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. 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.

3.2. Subject to the Services performance 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 enters the Unit's class in the Society's Register;
- survey the Unit periodically in service to note that 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.

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 after surveys; (iii) present the Unit for surveys; and (iv) inform the Society in due course of any circumstances that may affect the given appraisement of the Unit or cause to modify the scope of the Services.

4.2. Certificates referring to the Society's Rules 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.

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, drawings, 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. 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 save, indemnify, defend and hold harmless the Society from the Client's own consequential loss regardless of cause.

7.2. In any case, 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 performance of the Services. This limit applies regardless of fault by the Society, including 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 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 agrees to release, 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 except for those claims caused solely and completely by the 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 class 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.

10. FORCE MAJEURE

10.1. Neither Party shall be responsible 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 already known by the receiving Party from another source and is properly and lawfully in the possession of the receiving Party prior to the date that it is disclosed;
- is already in possession of the public or has entered the public domain, otherwise than through a breach of this obligation;
- is acquired 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 Society and the Client 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. 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 for the performance of the Services including, but not limited to drawings, calculations, and reports shall remain 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 a 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. The Conditions shall be construed and governed by the laws of England and Wales.

15.2. The Society and the Client 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 by arbitration under the LCIA rules, 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 London (UK).

16. PROFESSIONNAL ETHICS

16.1. Each Party shall conduct all activities in compliance with all laws, statutes, rules, 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. 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 Society's Code of Ethics of Bureau Veritas. http://www.bureauveritas.com/home/about-us/ethics+and+compliance/

RULE NOTE NR 642

NR 642

Cybersecurity Requirements for Products to be Installed On-Board Naval Ships

July 2018

Section 1 General

Section 2 Principles of Cybersecurity Verification

Section 3 Manufacturer Survey

Section 4 Product Survey

Appendix 1 Products Requirements

Appendix 2 Template for Survey Report

SECTION 1 GENERAL

1 General

1.1 Goal

1.1.1 The Goal of this Rule Note is to define a process in order to assess that:

- a Manufacturer has set in place procedures in order to deliver products following requirements regarding cybersecurity
- a Product delivered by a Manufacturer fulfills requirements regarding cybersecurity

1.2 Application

1.2.1 This Rule Note applies to ships covered by NR483 Rules for Naval Vessels. It can be applied on request to other kind of ships.

1.2.2 Any equipment containing any logical code or addressable memory should be considered in the scope of this Rule Note.

1.3 Principles

1.3.1 Requirements contained in this Rule Note are dedicated to Manufacturers and their Products. The agreement between the Society and the Manufacturer does not need to be linked to a specific Ship Classification.

1.3.2 Upon satisfactory completion by the Society of security verification and surveys, the Society delivers to the Manufacturer survey certificates in accordance with Sec 3 and Sec 4.

2 Definitions and references

2.1 Definitions

2.1.1 ACL (access control list)

On some types of proprietary computer-hardware (in particular routers and switches), an access control list provides rules that are applied to port numbers or IP addresses

2.1.2 Administrator

A system administrator is a person who is responsible for the upkeep, configuration, and reliable operation of computer systems.

2.1.3 COTS

Commercial-off-the-shelf (COTS) software and services are built and delivered usually from a third party vendor. COTS can be purchased, leased or even licensed to the general public

2.1.4 CPU

Central processing unit: the key component of a computer system, which contains the circuitry necessary to interpret and execute program instructions.

2.1.5 Firewall

A firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules.

2.1.6 HMI

The user interface or human–machine interface is the part of the machine that handles the human–machine interaction.

2.1.7 MAC address

A media access control address (MAC address) of a computer is a unique identifier assigned to network interfaces for communications at the data link layer of a network segment.

2.1.8 Hash function

A hash function is any function that can be used to map data of arbitrary size to data of fixed size.

2.1.9 Navy

Navy means the Governmental Body to whom the State or the Defence Department of the State has delegated responsibility for ownership of naval ships. The Navy is responsible for the requirement, procurement and through life support and maintenance of the naval ship

2.1.10 OSI

The Open Systems Interconnection model (OSI model) is a conceptual model that characterizes and standardizes the communication functions of a telecommunication or computing system without regard to their underlying internal structure and technology.

2.1.11 QoS

In the field of computer networking and other packet-switched telecommunication networks, quality of service refers to traffic prioritization and resource reservation control mechanisms rather than the achieved service quality. Quality of service is the ability to provide different priority to different applications, users, or data flows, or to guarantee a certain level of performance to a data flow.

2.1.12 Router

A router is a networking device that forwards data packets between computer networks.

2.1.13 Sensitive data

Data are considered as sensitive when declared as so by the Manufacturer or by other criteria promoted by an organization like a governmental organization. In order to handle

them or store sensitive data, specific methods shall be used, proposed by the Manufacturer or determined by an external organization

2.1.14 Standard operating systems

Operating system software implemented on widely commercialized computerized systems, including non-industrial systems.

2.1.15 Switch

A network switch is a multiport network bridge that uses hardware addresses to process and forward data at the data link layer (layer 2) of the OSI model. Some switches can also process data at the network layer (layer 3) by additionally incorporating routing functionality that most commonly uses IP addresses to perform packet forwarding; such switches are commonly known as layer-3 switches or multilayer switches.

2.1.16 USB

USB (Universal Serial Bus), is an industry standard that defines cables, connectors and communications protocols for connection, communication, and power supply between computers and devices.

2.1.17 VLAN

A virtual LAN (VLAN) is any broadcast domain that is partitioned and isolated in a computer network at the data link layer (OSI layer 2).

2.1.18 Virtual machine

A virtual machine (VM) is an emulation of a computer system. Virtual machines are based on computer architectures and provide functionality of a physical computer.

2.2 References

2.2.1 For guidance, reference is made the requirements of:

ISO/IEC 27002-2013 Information technology -- Security techniques -- Code of practice for information security controls

SECTION 2 PRINCIPLES OF CYBERSECURITY VERIFICATION

1 General

1.1 Global context

1.1.1 Cybersecurity measures on board a ship

This Rule Note is assuming the following hypothesis:

- a risk analysis has been undertaken regarding the ship cyber systems on the specific scope of cybersecurity. This analysis shall provide for each system a ranking regarding cybersecurity related to the risk and/or the impact of a cyber attack. The achievement of this analysis is not in the scope of this Rule Note; for a better understanding of this global context, ISO/IEC 27005:2013 might be refered to.
- an organization is set in place at the level of the ship and of the Navy in order to handle the cybersecurity. This may lead for instance to the setting up of centralised system in order to monitor cyber events and control the cybersecurity measures aboard the ship.
- Requirements mentioned in this Rule Note are generic. For a specific project, additional requirements might be asked by another Party than the Society. In case these specific requirements and the generic requirements described in this Rule Note enter into conflict, the Society should be made aware of this situation.

1.1.2 The different cybersecurity levels:

The systems can be classed into three levels regarding cybersecurity:

- Level 1: The risks or the consequences of a cyber attack are low for these systems and those connected systems. These systems should not carry or store sensitive data.
- Level 2: The risks or the consequences of a successful cyber attack are significant. These systems do not require a State control but the Authority in charge of the operation of these systems shall be able to provide the proofs that an adequate policy has been set up in case of control or cyber event.
- Level 3: The risks or the consequences of a cyber attack are critical. These systems may be submitted to State controls or checked by accredited organizations.

The requirements regarding products delivered by Manufacturer listed in this Rule Note may be modulated according to the capacity of the Product to be part of system granted with a specific cyber security level. This capacity of a Product will be for easier convenience mentioned the same way as the cyber security level for the system, ie Level "X".

The implications for a system being interconnected with other systems regarding its cybersecurity level are not addressed by this Rule Note and shall be considered in the design phase mentionned in [1.1.1].

1.2 Manufacturer duties

1.2.1 The Manufacturer shall provide documentation and prepare the checking phases as required by this Rule Note.

1.2.2 The Manufacturer shall make the Society aware of the circumstances that might render the previously undertaken surveys not valid anymore.

2 Verification process

2.1 Manufacturer survey

2.1.1 Content of survey

Manufacturer policies regarding

- Human resource,
- Operations all over the life cycle of the product,
- Manufacturer systems acquisition, development and maintenance,
- Supplier relationships

shall be evaluated thanks to document review and on-site inspection. The requirements related to these topics are described in Sec 3.

2.1.2 Validity of survey

Once completed, the survey Manufacturer remains valid for four years except if:

- a new Product is delivered.
- production sites are relocated or created and/or perimeter of the information systems used for the elaboration of the products has changed
- the highest cybersecurity level granted among the products delivered by this Manufacturer has been modified
- significant changes in the existing process have been implemented. Installation of a security patch, unless if considered requiring major maintenance on the software, does not normally jeopardize the validity of the survey.
- On-site scheduled surveys have not been undertaken or successful.

After this four year period, the survey shall be renewed, focusing on the modifications of the Manufacturer's organization and process.

2.1.3 Document produced and other Manufacturer's surveys

Details for organization and document production for Manufacturers' surveys are provided in Sec 3.

2.2 Product survey

2.2.1 Categories of products

The requirements for Products may differ according to the category of products considered. Several categories of products shall be considered for the purpose of this Rule Note:

a) CAT A

Basic equipment

b) CAT B

Equipment dedicated to network and security

c) CAT C

Programmable Logic Controller

d) CAT D

Electronic configurable equipment not included in other categories

The content of the categories is detailed in Sec 4, [2]

The Product delivered by the Manufacturer may fall under several of the categories described, in this case, the corresponding requirements shall be applied accordingly.

2.2.2 Content of initial survey

The requirements shall be checked for each Product through:

- review of the documentation submitted by the Manufacturer regarding the Product
- on-site testing and checking of the Product when required

2.2.3 Validity of initial survey

Once completed, the initial survey for a Product remains valid for five years except if:

- the cybersecurity level of the Product is upgraded
- the Product is modified. The installation of patches is normally not altering the validity of the survey.
- the production site of the Product is changed or the perimeter of the information systems used for the elaboration of the Product has been changed
- the Product suffers obsolescence and needs modification related to it (e.g. evolution of a communication protocol widely spread, evolution of a supplier technology)

2.2.4 Documents produced and other Products surveys

Details for organization and document production for Products Surveys are provided in Sec 4.

SECTION 3 MANUFACTURER SURVEY

1 Phases of survey

1.1 Review of documentation provided by Manufacturer

1.1.1 Documentation about human resource security

Procedures shall be implemented at the different steps of relationships between the employees and the Manufacturer.

a) Prior to employment

1) Screening

Background verification checks on all candidates for employment should be carried out in accordance with relevant laws, regulations and ethics and should be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.

2) Terms and conditions of employment

The contractual agreements with employees and contractors should state their and the organization's responsibilities for information security.

b) During employment

1) Management responsibilities

Management should require all employees and contractors to apply information security in accordance with the established policies and procedures of the organization.

2) Information security awareness, education and training

All employees of the organization and, where relevant, contractors should receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function.

3) Disciplinary process

There should be a formal and communicated disciplinary process in place to take action against employees who have committed an information security breach.

c) Termination and change of employment

Information security responsibilities and duties that remain valid after termination or change of employment should be defined, communicated to the employee or contractor and enforced.

ISO 27002:2013 §7 shall be referred to for guidance.

1.1.2 Documentation about operations security

Procedures shall be implemented regarding security of operations in the Manufacturer's premises, dealing with items mentioned below:

a) Operational procedures and responsibilities

1) Documented operating procedures

Operating procedures should be documented and made available to all users who need them.

2) Change management

Changes to the organization, business processes, information processing facilities and systems that affect information security should be controlled.

3) Capacity management

The use of resources should be monitored, tuned and projections made of future capacity requirements to ensure the required system performance.

4) Separation of development, testing and operational environments

Development, testing, and operational environments should be separated to reduce the risks of unauthorized access or changes to the operational environment.

5) Integrity of software produced during the process

A procedure shall be set in place in order to keep the integrity of software during its production process.

b) Protection from malware

Detection, prevention and recovery controls to protect against malware should be implemented, combined with appropriate user awareness and taking into account updates of the threats.

c) Backup

Backup copies of information, software and system images should be taken and tested regularly in accordance with an agreed backup policy.

d) Logging and monitoring

1) Event logging

Event logs recording user activities, exceptions, faults and information security events should be produced, kept and regularly reviewed.

2) Protection of log information

Logging facilities and log information should be protected against tampering and unauthorized access.

3) Administrator and operator logs

System administrator and system operator activities should be logged and the logs protected and regularly reviewed.

4) Clock synchronisation

The clocks of all relevant information processing systems within an organization or security domain should be synchronised to a single reference time source.

5) A process should be set in place in order to detect and alert in case of abnormal activity.

e) Installation of software on operational systems

Procedures should be implemented to control the installation of software on operational systems. In particular process shall be defined in order to have the last security patch installed on software before delivery.

f) Technical vulnerability management

1) Management of technical vulnerabilities

Information about technical vulnerabilities of information systems being used should be obtained in a timely fashion, on a permanent basis, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk. A management of the patches installation shall be set in place.

2) Restrictions on software installation

Rules governing the installation of software by users should be established and implemented.

3) Cyberevents occurrence and evidence they have been solved shall be registered

g) Information systems audit considerations

Audit requirements and activities involving verification of operational systems should be carefully planned and agreed to minimize disruptions to business processes.

ISO 27002:2013 §12 shall be referred to for guidance.

1.1.3 Documentation about system development and maintenance

Procedures shall be implemented regarding development and maintenance of products, dealing with items mentioned below.

a) Security requirements of information systems

1) Information security requirements analysis and specification

The information security related requirements should be included in the requirements for new information systems or enhancements to existing information systems.

2) Securing application services on public networks

Information involved in application services passing over public networks should be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification.

3) Protecting application services transactions

Information involved in application service transactions should be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.

b) Security in development and support processes

1) Secure development policy

Rules for the development of software and systems should be established and applied to developments within the organization.

2) System change control procedures

Changes to systems within the development lifecycle should be controlled by the use of formal change control procedures.

3) Technical review of applications after operating platform changes

When operating platforms are changed, business critical applications should be reviewed and tested to ensure there is no adverse impact on organizational operations or security.

4) Restrictions on changes to software packages

Modifications to software packages should be discouraged, limited to necessary changes and all changes should be strictly controlled.

5) Secure system engineering principles

Principles for engineering secure systems should be established, documented, maintained and applied to any information system implementation efforts.

6) Secure development environment

Organizations should establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle.

7) Outsourced development

The organization should supervise and monitor the activity of outsourced system development.

8) System security testing

Testing of security functionality should be carried out during development.

9) System acceptance testing

Acceptance testing programs and related criteria should be established for new information systems, upgrades and new versions.

c) Test data

Test data should be selected carefully, protected and controlled.

ISO 27002:2013 §14 shall be referred to for guidance.

1.1.4 Supplier relationships

Procedure shall be implemented regarding relationships between the manufacturer and its suppliers, dealing with items mentioned below.

a) Information security in supplier relationships

1) Information security policy for supplier relationships

Information security requirements for mitigating the risks associated with supplier's access to the organization's assets should be agreed with the supplier and documented.

2) Addressing security within supplier agreements

All relevant information security requirements should be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organization's information.

3) Information and communication technology supply chain

Agreements with suppliers should include requirements to address the information security risks associated with information and communications technology services and product supply chain.

b) Supplier service delivery management

1) Monitoring and review of supplier services

Organizations should regularly monitor, review and audit supplier service delivery.

2) Managing changes to supplier services

Changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, should be managed, taking account of the criticality of business information, systems and processes involved and re-assessment of risks.

ISO 27002:2013 §15 shall be referred to for guidance.

1.1.5 Risk Management process

A Risk management process should be in place.

ISO 27005:2013 §15 shall be referred to for guidance.

1.2 Survey in the Manufacturer premises

1.2.1 Intervention of the Surveyor

The Surveyor shall be able to check the requirements mentioned in [1.1] through:

- consultation of documentation on-site, including the list of the cyberevents that took place since the last survey.
- interviews of Manufacturer's employees. Employees taking part into pure support activities as commercial or accounting activities should not be impacted by these surveys.

1.3 Type of survey in the Manufacturer premises

1.3.1 Scheduled surveys

After initial survey, a schedule for regular intermediate surveys shall be established between the Manufacturer and the Society. Annual intermediate surveys should normally be planned. Deviations from the situation stated during the last survey should be traced during these events, including a status of the products approved or under approval according to these Rules.

1.3.2 Renewal surveys

Renewal surveys shall be scheduled taking into account the circumstances described in Sec 2, [2.1.2]. A global evaluation regarding requirements mentioned in [1.1] shall be undertaken.

2 Documents

2.1 List of documents required from the Manufacturer

2.1.1 The Manufacturer shall provide documents listed in Tab 1 in order to check requirements mentioned in [1.1]

2.2 Model of document issued by the Society after survey completion for a Manufacturer

2.2.1 Information mentioned in Tab 2 should be listed in the document produced after the manufacturer Survey

Table 1 : List of documents required from the Manufacturer

N°	Title
1	Procedures related to the relationships between the employees and the Manufacturer regarding security
2	Procedures related to the security of operations in the Manufacturer's premises
3	Procedures related to the development and maintenance of products
4	Procedure related to the relationships between the manufacturer and its suppliers
5	Manufacturer's organisation chart describing chain of responsibilities at the Manufacturer's regarding security
6	Any attestation showing accreditation by a National Authority to handle confidential data by the Manufacturer's staff and the list of this accredited staff **(1)**
7	Any attestation of a national accreditation Authority dealing with cybersecurity **(1)**
8	Documentation related to Risk Management process
9	List of the cyberevents that took place since the last survey
(1) When available. If not, this should be mentioned in the document issued by the Society.	

Table 2 : Model of document issued by the Society after survey completion for a Manufacturer

MANUFACTURER's NAME: xxx

Manufacturer Main address: xxx

Manufacturer premises involved in the Products making and corresponding addresses:
XXXXXX XXXXXXX
XXXXX XXXXXXXXXXX

List of Products surveyed within the scope of NR 642
(Name of Product / Level of product / Categorie(s) involved/ name of the information system involved if relevant)
XXXXXXXXX / xxxx / xxxxxxx / xxxxx
XXXXXXX / xxxx / xxxxxx / xxxxx

Type of Survey (Inital/Intermediate/Renewal): xxxxxxxxxxxxxx

Date of Survey Completion: xxxxxxxx

Surveyor's Name and Signature: xxxxxxxxxxxxxx

BV Stamp

SECTION 4 PRODUCT SURVEY

1 Phases of survey

1.1 Review of documentation provided by the Manufacturer regarding initial Product Survey

1.1.1 Review of documentation submitted shall enable to check the requirements mentioned in App 1, Tab 1 for the Product regarding its cybersecurity level as defined in Sec 2, [1.1.2] and its category as defined in Sec 2, [2.2.1]. This review shall be undertaken for each new product and does not need to be repeated except during the renewal of this initial survey.

1.2 Initial Product Survey in the Manufacturer premises

1.2.1 When a check in the premises of the Manufacturer is required in list included in App 1, Tab 1, the Surveyor shall be able to perform the checking on the Manufacturer premises for any new product.

1.3 Product Survey during each Product delivery

1.3.1 Each time a product is delivered, the conformity of the delivered product shall be checked according to the requirements used at the initial survey, at the satisfaction of the Surveyor regarding the provisions involving checkings on-site. The Surveyor shall also be able to trace the parameters that are changed (eg MAC addresses, software versions) compared to the inital survey of the Product.

2 Requirements for a product

2.1 Initial Product survey

2.1.1 List of components

In the scope of the initial survey, a list of the components included in the Product shall be provided showing at least:

- a description of each component
- for each component, the version of the pieces of software installed (including OS and installed packages, libraries of other COTS)

2.1.2 Architecture of product

The arrangement of the components inside the product shall be detailed

2.1.3 Documents required

The documents provided by the Manufacturer shall be sufficient to check the requirements selected for a Product as mentioned in App 1, Tab 1.

2.2 Product delivery survey

2.2.1 A document tracing the discrepancies between Product considered during the initial survey and the Product delivered shall be provided to the surveyor. This document shall also mention the Ship where this Product will be finally installed.

2.3 Specific requirements for basic equipment CAT A

2.3.1 Type of equipment addressed by these requirements

The specific requirements for CAT A are addressed to the types of equipment mentioned in Tab 1.

2.3.2 List of requirements

Requirements as mentioned in App 1, Tab 1 shall be fulfilled for CAT A equipment.

2.4 Specific requirements for Network and security equipment CAT B

2.4.1 Type of equipment addressed by these requirements

The specific requirements for CAT B are addressed to the types of equipment as mentioned in Tab 2

2.4.2 List of requirements

Requirements as mentioned in App 1, Tab 1 shall be fulfilled for CAT B equipment

2.5 Specific requirements for Programmable logic controller CAT C

2.5.1 Type of equipment addressed by these requirements

The specific requirements for CAT C are addressed to the types of equipment as mentioned in Tab 2

2.5.2 List of requirements

Requirements as mentioned in App 1, Tab 1 shall be fulfilled for CAT C equipment

2.6 Specific requirements for other configurable equipment CAT D

2.6.1 Type of equipment addressed by these requirements

The specific requirements for CAT D are addressed to the types of equipment as mentioned in

2.6.2 List of requirements

Requirements as mentioned in App 1, Tab 1 shall be fulfilled for CAT D equipment

Table 1 : description of basic equipment CAT A

N°	Name	description
1	Server	Equipment operated thanks to a standard operating system. Access to this kind of equipment is limited to maintenance.
2	Calculator	Equipment including one or several CPUs cards. These cards may work thanks to a standard operating system or to an embedded operating system. Access to this kind of equipment is limited to maintenance.
3	Working station, terminal	Equipment working thanks to a standard operating system. Access to this kind of equipment is limited to operators and maintenance.

Table 2 : description of Network and security equipment CAT B

N°	Name	description
1	Switch router	Equipment operated thanks to a firmware, under the form of a specific appliance, module for PLC or card integrated to a CPU. Access to this kind of equipment is limited to maintenance
2	Firewall, probe	

Table 3 : description of Programmable Logic Controller CAT C

N°	Name	description
1	CPU Module	Equipment operated thanks to a firmware and an application (programmable logic). Access to this kind of equipment is limited to maintenance.
2	PLC HMI	Equipment operated thanks to a firmware and an application. Access to this kind of equipment is limited to operation.

Table 4 : description of other configurable equipment CAT D

N°	Name	description
1	configurable electronic equipment	Equipment operated thanks to a firmware and an application (programmable logic). Access to this kind of equipment is limited to maintenance.

2.7 Evaluation of the cyber security level

2.7.1 Request from Manufacturer

The Manufacturer shall mention in Form mentioned in [2.8.1]:

- which cybersecurity level is targeted for the Product under consideration
- those threats against which the Product is providing protection
- the security functionalities included in the Product in order to treat the identified threats.

2.7.2 List of requirements

List of requirements mentioned in App 1 provides criteria in order to grant cybersecurity levels for each of these requirements. This shall be undertaken during the document approval and at the survey in the premises. When it is found that criteria on some specific requirements does not allow to grant the cybersecurity level expected by the Manufacturer for the Product, the Surveyor may consider a derogation to these criteria.

When a requirement is considered as non relevant for the considered product, the surveyor shall trace and detail this statement.

When a requirement is considered as relevant but not able to be fulfilled for cybersecurity level, the word “none” shall be used in the survey report described in [2.8.2]

Considering the amount of cybersecurity levels obtained for each specific requirement, taking into account derogations, the field Surveyor will determine the global cybersecurity level of the Product as the minimum figure found in this list of specific cybersecurity levels.

2.7.3 Rules for derogation

a) As a general Rule, any derogation shall be justified in writing in Form mentioned in [2.8.2]

b) A derogation can only be granted at the level of a requirement, not for the whole product level

c) In order to have a cybersecurity level 1 instead of none, the derogation might be granted by the local surveyor.

d) In order to have a cyberscurity level 2 instead of one, the derogation might be granted by the approval office.

e) In no case a level 3 can be obtained by derogation.

2.8 Model of documents

2.8.1 A model of Request Form to be filled by the Manufacturer is shown in Tab 5.

2.8.2 A Model of document issued by the Society after initial and delivery survey completion for a Product is shown in App 2, Tab 1.

Table 5 : Request Form for a Product

MANUFACTURER's NAME: xxx

Manufacturer Main address: xxx

Manufacturer premises involved in the Products making and corresponding addresses:
XXXXXX XXXXXXX
XXXXX XXXXXXXXXXX

Products (Name of product / Level of product / Categorie(s) involved/ Cybersecurity level targeted /Name of the information system involved if relevant)
XXXXXXXX / xxxx / xxxxxxx / X / xxxxx

Date of request: xxxxxxxx

Is it an initial request?: Y/N

APPENDIX 1 PRODUCTS REQUIREMENTS

1 General

1.1

1.1.1 With reference to Sec 4, [1.1.1] and Sec 4, [2.7.2], the applicable requirements for a Product considering its category and applicable criteria in order to grant cybersecurity levels are detailed in Tab 1.

Table 1 : Cybersecurity requirements

IDENTIFICATION CODE **(1)**	CONTENT	ASSOCIATED TEST **(2)**	LEVEL1 **(3)**	LEVEL 2 **(3)**	LEVEL 3 **(3)**
ARCH 01 A,B,C,D	Existence of roles for users shall be implemented and checked roles including: • identification of functions performed by each role; • responsability sharing for operations undertaken in the scope of a role; • access to the different systems for each role; Implementation of these aspects shall be checked through the kind of user accounts set in place.	Testing on involved devices of the existence of these roles at the Manufacturer's premises	R	M	M
ARCH 02 A,B,C	The system shall include elements enabling to handle remotely following functions : • integrity policy configuration; • triggering of integrity checks; • reporting of results of integrity checks.	Configuration of these functions shall be checked when possible on involved devices thanks to simulating tools if necessary	R	M	M
ARCH 03 A,B,C,D	Administration tools shall be centralised in dedicated working stations.	To be checked at Manufacturer's premises when applicable	R	M	M
ARCH 04 A,B,C,D	The different elements of a sensitive system shall comply with the regulations related to emission security when prescribed	NA	R	M	M
ARCH 05 A,B	Systems shall be fitted with an antivirus solution including following functions, remotely accessible from a supervision tool : • updating of databases; • configuration of antivirus policy; • reporting of cyber events	To be checked at Manufacturer's premises	M	M	M
ARCH 06 B	Sensitive data shall be transported through physically separated data flows according to each level of classification	NA	M	M	M

ARCH 07
B
	Following requirements shall be applied when two systems with two different levels of sensitivity need to be connected :
	• agreed methods are used in order to obtain that :
	  • lower level of sensitivity data only can be released by the upper level of sensitivity system to the lower level of sensitivity system;
	  • such releases of data are allowed and controlled by the sender;
	  • such releases are registered in a data log and affected to the sender; OR, alternatively
	• imports from the lower level of sensitivity system are allowed only if they go through a buffer area, part of an approved network architecture handled by the operational authority in charge of the upper level of sensitivity system. These transfers shall be operated thanks to agreed uni-directional means of data transfer. Such transfers shall be registered in a data log.
		Process of registration on data log shall be checked at Manufacturer's premises	M	M	M

(1) A,B,C,D: Letters refer to categories described in Sec 2, [2.2.1]. The requirement shall be taken into account for mentioned categories.
(2) NA: Not Applicable
(3) R: Recommended M: Mandatory

IDENTIFICATION CODE **(1)**	CONTENT	ASSOCIATED TEST **(2)**	LEVEL1 **(3)**	LEVEL 2 **(3)**	LEVEL 3 **(3)**
ARCH 08 A,B	Firewalls shall be monitored and controlled remotely through a centralised tool including following functions : • configuration of control policy for data flows • reporting of cyber events	To be checked at Manufacturer's premises when applicable	R	M	M
ARCH 09 A,B	When sensitive data are involved, transfers with entities located outside the ships shall be protected through agreed means of encryption: means of encryption shall be described, protected data flows shall be mentioned and the associated means of protection described. External organizations which may have controlled these protections means shall be declared.	Configuration of means of encryption shall be checked at Manufacturer's premises	M	M	M
ARCH 10 A,B,C,D	Means shall be available to store and restore any information necessary to the proper operation of ship systems (this can be handled through local storage or through a remote access on shore; the circumstances when these means could be used for instance for the configuration of a newly installed spare part) These means shall be protected regarding the level of sensitivity of data stored.	To be checked at Manufacturer's premises	R	R	M
ARCH 11 A,B,C,D	Means shall be available to store logs of cyber events These means shall be protected regarding the level of sensitivity of data stored.	To be checked at Manufacturer's premises	M	M	M
ARCH 12 A,B,C,D	Means for remote maintenance (operated from a location on the ship or outside of the ship) shall be protected at least by the same means of physical/logic protection corresponding to the level of sensitivity of the related systems	To be checked at Manufacturer's premises when remote maintenance is included in the Product	M	M	M
CAC 001 A,B,C,D	Ships systems shall be able to identify and authenticate each user. Unless clearly for identified systems, no interaction between the system and the user shall be possible unless identification and authentication has been run successfully. While this phase has not be completed, the only function accessible shall be the identification/authentication one. Identification by function and not by personal identification is not allowed unless proper operational justification. This requirement also apply when a maintenance /backup device is plugged in the system: the system shall be able to authenticate the users, simple local authentication on the plugged device is not enough	To be checked at Manufacturer's premises	R	M	M
CAC 002 A,B,C,D	Ship systems shall be able to allow Administrators to grant or deny access permanently or temporarily to the other users to the ship systems.	To be checked at Manufacturer's premises	R	M	M
CAC 003 A,B,C	Ship Systems shall allow the Administrators to: • list/create/modify/delete/disable (for a limited period of time) accounts; • list/create/modify/delete groups of accounts; • list/create/modify/delete accounts in groups of accounts Useless and not in use accounts shall be able to be deleted. The created accounts shall follow the principle of the less privilege granted.	To be checked at Manufacturer's premises	R	M	M

(1) A,B,C,D: Letters refer to categories described in Sec 2, [2.2.1]. The requirement shall be taken into account for mentioned categories.

(2) NA: Not Applicable

(3) R: Recommended M: Mandatory

IDENTIFICATION CODE **(1)**	CONTENT	ASSOCIATED TEST **(2)**	LEVEL1 **(3)**	LEVEL 2 **(3)**	LEVEL 3 **(3)**
CAC 004 A,B,C	Secret authentication information (like passwords) shall not be able to transit on networks unless protected through cryptographic methods providing confidentiality and integrity.	NA	R	M	M
CAC 005 A,B,C,D	Ship systems shall allow any user to renew his password on its own request. Providing the current password shall be mandatory for this operation.	To be checked at Manufacturer's premises	R	M	M
CAC 006 A,B,C,D	Ship systems shall enable Administrators to: • reinitialise the password of another user; • to compel another user to modify his password at the next authentication opportunity.	To be checked at Manufacturer's premises	R	M	M
CAC 007 A,B	Each piece of equipment shall be fitted with an automatic locking or closing of the user session after a predetermined delay of inactivity of the user. This inactivity delay threshold is per default 10 minutes, it can be adjusted according to operational strains of each system (ie equipment requiring a 24/7 watch shall experience locking/closing of session). Administrators shall be able to change the inactivity delay threshold before locking or closing of the session. The unlocking of the session shall be possible after a successful authentication of the user or potentially of an Administrator. The locking and/or closing of the session shall be able to hide or erase the image displayed on the working station screen, unless some operational strains prevent to do so, and to deactivate the input devices.	To be checked at Manufacturer's premises	R	M	M
CAC 008 A,B,C	The applications shall not need to use Administrator rights or system privileges. If for functional reasons, some applications need such rights or privileges, they should be listed	To be checked at Manufacturer's premises	R	M	M
CAC 009 A,B,C,D	All folders shall be fitted with access rights at the lowest possible level needed (reading (R), writing (W), execution (E).	To be checked at Manufacturer's premises	R	M	M
CAC 010 A,B	Ship systems shall deliver to unidentified users following messages through the Human machine interface: • a warning mentioning that only authorized users shall access the system; • a warning mentioning that a surveillance might be set in place in order to track unauthorized use of the system. Two fields shall be reserved in order to indicate on the Human Machine Interface • a warning mentioning penalties and pursuits applicable in case of unauthorized access; • the level of sensitivity of the system. These messages shall be visible from any interface with user, whenever access is remote or local.	To be checked at Manufacturer's premises	R	M	M
CAC 011 A,B,C,D	Oustide maintenance and restore operations, ship systems shall allow the starting up of equipment only on controlled external devices.	To be checked at Manufacturer's premises	R	M	M

(1) A,B,C,D: Letters refer to categories described in Sec 2, [2.2.1]. The requirement shall be taken into account for mentioned categories.

(2) NA: Not Applicable

(3) R: Recommended M: Mandatory

IDENTIFICATION CODE **(1)**	CONTENT	ASSOCIATED TEST **(2)**	LEVEL1 **(3)**	LEVEL 2 **(3)**	LEVEL 3 **(3)**
CAC 012 A,B,C,D	Per default, unused external communication interface (Ethernet, USB, ...) shall be deactivated on ship equipment (physical and/or logic locks). Activation and deactivation shall be achievable only by Administrators. Physical interfaces used for equipment maintenance shall be able to be activated/deactivated by Administrators outside the maintenance periods.	To be checked at Manufacturer's premises	R	M	M
CAC 013 A	Unless virtual machines are installed, only one operating system shall be installed per equipment	To be checked at Manufacturer's premises	M	M	M
CAC 014 A,B,C	Outside maintenance operation, ship systems shall not allow the ability for a user to access simultaneously administration and application functions.	To be checked at Manufacturer's premises	M	M	M
CAC 015 A,B,C,D	For accounts dedicated to the use of the Administrators ship systems shall use passwords with a minimum level of complexity, at including at least 14 digits with a minimum of three of following character categories: • alpha numeric character, arabic figure (0 to 9); • special character (,;:!?./§%µ? ...) • mix of lowercase and lowercase characters no easily guessable elements should be used in these passwords (part of identification, name of the company or equipment, ...)	To be checked at Manufacturer's premises	M	M	M
CAC 016 A,B,C	Ship systems shall protect passwords as long as they are stored locally on the systems. At least, a protection on a condensed non-reversible shape produced thanks to a hash function (SHA 256 minimum) shall be preferably picked up.	To be checked at Manufacturer's premises	R	M	M
CAC 017 A,B	After (N) authentication attempts consecutively failed, ship systems shall emit an alarm and: • lock the corresponding user account; or • add a (X) seconds delay in order to be able to re-authenticate on this account (N) and (X) should be coherent with the operation of the system involved. It shall be possible to adjust these parameter for an Administrator.This mechanism might be inhibited on specific situations.	To be checked at Manufacturer's premises	R	M	M
CAC 018 A,B,C,D	The booting process of a ship system shall not be able to be modified except by an Administrator. Access to the booting process shall be protected by a password.	To be checked at Manufacturer's premises	M	M	M
CAC 019 A,B,C	Non-deactivated USB interfaces shall control and restrict access to explicitly authorized devices only. Systems booting through removable external devices shall be deactivated	To be checked at Manufacturer's premises	M	M	M
CAC 020 A,B,C	Responsible Administrators shall be able de define criteria of length and complexity for secret information (eg: passwords) on ship systems. Default values if specified should be used.	To be checked at Manufacturer's premises	M	M	M

(1) A,B,C,D: Letters refer to categories described in Sec 2, [2.2.1]. The requirement shall be taken into account for mentioned categories.

(2) NA: Not Applicable

(3) R: Recommended M: Mandatory

IDENTIFICATION CODE **(1)**	CONTENT	ASSOCIATED TEST **(2)**	LEVEL1 **(3)**	LEVEL 2 **(3)**	LEVEL 3 **(3)**
CAC 021 A,B	A time limit for the validity of passwords shall be implemented on ship systems. The value of this time limit shall be able to be set by responsible Administrators.	To be checked at Manufacturer's premises	M	M	M
CAC 022 A,B	A new password shall not be accepted by ship systems unless it differs from the last (N) passwords used. Responsible Administrators shall be able to set this value. Unless otherwise specified, the default value shall be 5 for N.	To be checked at Manufacturer's premises	M	M	M
CAC 023 A	Access to ship systems: • classified; • dedicated to administration (including non classified and remote maintenance systems) shall be undertaken through a strong authentication method, meaning two of the following three aspects: • what I know (eg: password); • what I own (eg: card); • what I am (eg: biometrics)	To be checked at Manufacturer's premises	R	M	M
CAC 024 A,B	Criteria for length and complexity shall be made mandatory for secret information defined by Administrators. Secret information not complying with these criteria shall be rejected by ship systems.	To be checked at Manufacturer's premises	M	M	M
DUR 001 A,B,C	Useless or unjustified software and services shall not be installed on ship systems (eg: development or integration tools, useless network services). Where this is not possible, these software and services shall be deactivated or blocked through filtering rules by Administrators.	NA	M	M	M
DUR 002 A,B,C	Operating systems and COTS software shall be configurated regarding cybersecurity according to specifications if any. Per default cybersecurity tools provided by the installed systems shall be implemented.	To be checked at Manufacturer's premises	M	M	M
DUR 003 A,B,C,D	Each ship system connected to a network shall be able to be synchronised with a common reliable time reference. It shall be impossible to modify time and date for unauthorized users	To be checked at Manufacturer's premises	M	M	M
DUR 004 A,B,C,D	Except when justified performance strains exist, ship systems shall be able to run a battery of autotests during initial starting in order to check the proper working (availability statement and integrity check). This operation shall be able to be achieved at the request of the user during maintenance phases or when preparing an operational deployment of the system.	To be checked at Manufacturer's premises	M	M	M
JOUR 001 A,B,C,D	For ship systems not being able to export data logs to a centralised logging system, cybersecurity events shall be kept during a 45 rolling days without loss on a local storage. A manual export procedure to a centralised system shall be implemented. It shall be possible for Administrators to consult, save and purge the recorded cybersecurity events on the local storage.	To be checked at Manufacturer's premises	M	M	M

(1) A,B,C,D: Letters refer to categories described in Sec 2, [2.2.1]. The requirement shall be taken into account for mentioned categories.

(2) NA: Not Applicable

(3) R: Recommended M: Mandatory

IDENTIFICATION CODE **(1)**	CONTENT	ASSOCIATED TEST **(2)**	LEVEL1 **(3)**	LEVEL 2 **(3)**	LEVEL 3 **(3)**
JOUR 002 A,B,C,D	Cybersecurity events logs produced by ship systems shall be use the SYSLOG format or a compatible format. They should be transferred and registered in real time into a centralised logging system via the SYSLOG protocol, using methods checking the integrity of events.	To be checked at Manufacturer's premises	M	M	M
JOUR 003 A,B,C,D	Each ship system shall be able to generate and store a cyberevents log. Each event shall be connected to the date and time of its occurrence and to the entity that generated it. At least, cyberevents included in following list shall be registered: • connexion/authentication failure events at the operating system and application level; • use of privileges: success, failure (eg use of su function on Linux) • opening, closing of session (operating system and application): success, failure; • error, warnings or information generated by the operating system (stop/ start of machine, stop /start of logging service) • viral alert: detection; • removable devices: successful connexion, connexion failure, import/export of data; • account administration (creation, deletion and modification of accounts and group of accounts): success, failure; • data flow control policy violation (firewall, ACL or MAC filter); • integrity failure; • vulnerabilities abuse (applies to Intrusion Detection System); • deployment of security updates/corrections including for antivirus databases; • adding/removal of software; • operating system parameters modification.	To be checked at Manufacturer's premises for the achievable events	M	M	M
MCS 001 A,B,C,D	Ship systems shall be able to be updated by with security releases published by software editors during the whole life cycle of the systems involved	To be checked at Manufacturer's premises	M	M	M
MCS 002 A,B,C,D	Ship Systems shall be fitted with means to restore them at least into a previously saved state enabling operations.	To be checked at Manufacturer's premises	R	M	M
MCS 003 A,B,C	Ship systems shall use QoS process to guarantee a proper quality of data flows	NA?	R	M	M
MCS 004 A,B,C,D	Ship systems shall be able to be restored by the final client in a fully autonomous way. This involves having an extensive reference configuration available with a guaranteed integrity.	To be checked on-site	R	M	M
MCS 005 A,B,C,D	Ship systems shall be able to return to nominal mode after an operational phase has been experienced in a derated mode or after the replacement of components (eg: new MAC address after a component exchange should be taken into account in order to recover the nominal operation of the system).	To be checked at Manufacturer's premises when applicable	M	M	M

(1) A,B,C,D: Letters refer to categories described in Sec 2, [2.2.1]. The requirement shall be taken into account for mentioned categories.

(2) NA: Not Applicable

(3) R: Recommended M: Mandatory

IDENTIFICATION CODE **(1)**	CONTENT	ASSOCIATED TEST **(2)**	LEVEL1 **(3)**	LEVEL 2 **(3)**	LEVEL 3 **(3)**
PDS 001 A	An antivirus control shall be possible on each ship system. If the system cannot have an antivirus solution embedded, a system scan shall be made possible thanks to an USB connected external device. It shall be able to update the database of the antivirus solution.	To be checked at Manufacturer's premises	R	M	M
PDS 002 A,D	When not foreseen to be stored in spaces granted with the corresponding level of protection, sensitive data shall be stored in a secured way using a cryptography system able to handle the right level of data sensitivity. The type of encryption system chosen shall be mentioned.	NA	R	M	M
PDS 003 A,D	When not foreseen to be stored in spaces granted with the corresponding level of protection, sensitive data shall be stored into a remanent memory extractable device, for the purpose of keeping them inside secure storages when the system is not operated	To be checked at Manufacturer's premises	R	M	M
PDS 004 A	Ship systems shall automatically start a virus scan on any connected external devices before the content of such devices is used. The authenticated user shall be warned in case of virus detection and an alarm shall be triggered to the cybersecurity administration and supervision system.	To be checked at Manufacturer's premises	M	M	M
PDS 005 A,B,C	Ship systems shall allow administrators to check their integrity (files, operating system and applications) et and show the result of such analysis in a standardized format.	To be checked at Manufacturer's premises	M	M	M
PDS 006 A	An antivirus scan shall be undertaken automatically and permanently on the ship systems	To be checked at Manufacturer's premises	M	M	M
PRODEF 001 A,B,C,D	The content of the technical bays shall not be accessible except to the authorized staff. If keys are chosen to achieve this requirement, they should not be easy to copy (eg: a triangle key are not considered as difficult to copy)	To be checked at Manufacturer's premises	R	M	M
PRODEF 002 A,B,C,D	Equipment and non-volatile memory storing or manipulating classified or sensitive data shall be tagged according to the relevant regulations. This tagging shall be also visible on any HMI available on the equipment.	To be checked at Manufacturer's premises	R	M	M
PRODEF 003 A,B,C,D	Technical bays shall be fitted with an opening detector (sound alarm and/or visual alarm and/or alarm sent to a centralised system)	To be checked at Manufacturer's premises	R	M	M
PRODEF 004 A,B	When it is not foreseen technical bays would be installed in secured access rooms, a surveillance (detection of access opening/closing of the bay connected to a remote alarm system) shall be fitted	NA	R	M	M
PTF 001 A,B,C,D	Design of ship data networks shall impose the use of fixed IP and of static routing tables. This involves the use of a fixed IP for each equipment.	To be checked at Manufacturer's premises	R	M	M
PTF 002 A,B,C,D	Ship networks shall be able to identify equipment through MAC addresses filtering before any connexion. This filtering process should be undertaken according to the white list principle (any equipment not included in the list is not allowed to be connected).	To be checked at Manufacturer's premises	R	M	M

(1) A,B,C,D: Letters refer to categories described in Sec 2, [2.2.1]. The requirement shall be taken into account for mentioned categories.

(2) NA: Not Applicable

(3) R: Recommended M: Mandatory

IDENTIFICATION CODE **(1)**	CONTENT	ASSOCIATED TEST **(2)**	LEVEL1 **(3)**	LEVEL 2 **(3)**	LEVEL 3 **(3)**
PTF 003 A,B	Any device on board shall only be able to emit or receive data flows dedicated to its only use through a filtering process included inside the device or an external device. Filtering rules shall involve at least layers OSI2 to OSI4.	To be checked at Manufacturer's premises	R	M	M
PTF 004 A,B,C,D	Data flows dedicated to supervision and administration shall be protected regarding confidentiality and integrity through cryptography mechanisms. It is recommended to use SSHv2, TLS1.2, SNMPv3 protocols.	To be checked at Manufacturer's premises	M	M	M
PTF 005 A,B,C,D	Before any connection to a network, ship devices shall authenticate on network (protocol 802.1x).	To be checked at Manufacturer's premises	M	M	M
SUP 001 A,B,C,D	It shall be possible for Supervision and Administration of cybersecurity functions of ship systems to be controlled locally from the involved system.	To be checked at Manufacturer's premises	M	M	M
SUP 002 A,B,C,D	Ship systems allowing operation of administration and supervision services regarding cybersecurity shall be designed in order to limited the access to these services to Administrators only.	To be checked at Manufacturer's premises	M	M	M
SUP 003 A,B	For each exchange of external data with a ship system, information enabling to determine the sender and the recipient identities and also reference of information exchanged shall be stored.	To be checked at Manufacturer's premises	M	M	M
FOURN 001 A,B,C,D	For each software developed, manufacturer shall indicate which set of rules for good development practices that have been used	NA	M	M	M
FOURN 002 A,B,C,D	A document showing a flow matrix shall be provided showing for each data flow: • Name, MAC address, IP address of the equipment initiating the flow • Name, MAC address, IP address of the equipment receiving the flow • Network protocol (TCP, UDP,…) • Application protocol (FTP, SSH, SNMP, …) and the port number (TCP/UDP) • Identifier of the associated message in the Interface Control Document	To be checked at Manufacturer's premises	M	M	M
FOURN 003 A,B,C,D	A statement from the Manufacturer shall be provided that Products provided are not containing any piece of software used during the development and integration phases and unnecessary to the proper operation of the Product	NA	M	M	M
FOURN 004 A,B,C,D	Security methods implemented shall be described in a specific chapter in the documents dealing with development (specification, conception and testing)	NA	M	M	M
FOURN 005 A,B,C,D	Before the Product is supplied, a list of software and packages including version of those shall be detailed and provided.	NA	M	M	M
FOURN 006 A,B,C,D	The Manufacturer shall provide a statement guaranteeing that the product is not containing any malicious code known at the delivery of the product	NA	M	M	M

(1) A,B,C,D: Letters refer to categories described in Sec 2, [2.2.1]. The requirement shall be taken into account for mentioned categories.

(2) NA: Not Applicable

(3) R: Recommended M: Mandatory

IDENTIFICATION CODE **(1)**	CONTENT	ASSOCIATED TEST **(2)**	LEVEL1 **(3)**	LEVEL 2 **(3)**	LEVEL 3 **(3)**
FOURN 007 A,B,C,D	Procedures set in place in order to handle cyber security (eg: changing passwords, back up) shall be described in the user documentation	NA	M	M	M
FOURN 008 A,B,C,D	Three months before the Product is delivered, the Manufacturer shall list the Common Vulnerabilities and Exposures as published by the MITRE corporation which have not been removed or taken care of.	NA	M	M	M
FOURN 009 A,B,C,D	A list of the files digital fingerprints shall be delivered together with the Product	NA	M	M	M
FOURN 010 A,B,C,D	Operating systems and COTS software shall be fitted with the last security updates three months before the cybersecurity verification.	NA	M	M	M

(1) A,B,C,D: Letters refer to categories described in Sec 2, [2.2.1]. The requirement shall be taken into account for mentioned categories.
(2) NA: Not Applicable
(3) R: Recommended M: Mandatory

APPENDIX 2 TEMPLATE FOR SURVEY REPORT

1 General

1.1

1.1.1 A model of document issued by the Society after initial and delivery survey completion for a product is shown in Tab 1.

Table 1 : Template for survey report

Product Name:			Type of product survey (Initial/Delivery): Date of survey: Name and signature of surveyor: BV Stamp:	
Categor(ies) of Product surveyed within the scope of NR 642:				
IDENTIFICATION CODE **(1)**	Specific Information to be mentioned by Surveyor	Maximum Level reached (none,1, 2 or 3) before any derogation or, non relevant	Maximum Level reached (1, 2 or 3) after derogation if any. If no derogation, put previous figure	Comment (mandatory if derogation is granted or if non relevant)
ARCH 01 A,B,C,D				
ARCH 02 A,B,C				
ARCH 03 A,B,C,D				
ARCH 04 A,B,C,D				
ARCH 05 A,B				
ARCH 06 B				
ARCH 07 B				
ARCH 08 A,B				
ARCH 09 A,B	Means of encryption used: Organization that have controlled means of encryption, if any:			
ARCH 10 A,B,C,D				
ARCH 11 A,B,C,D				
ARCH 12 A,B,C,D				
CAC 001 A,B,C,D				
(1) A,B,C,D: Letters refer to categories described in Sec 2, [2.2.1]. The requirement shall be taken into account for mentioned categories.				

Product Name:			Type of product survey (Initial/Delivery): Date of survey: Name and signature of surveyor: BV Stamp:	
Categor(ies) of Product surveyed within the scope of NR 642:				
IDENTIFICATION CODE **(1)**	Specific Information to be mentioned by Surveyor	Maximum Level reached (none,1, 2 or 3) before any derogation or, non relevant	Maximum Level reached (1, 2 or 3) after derogation if any. If no derogation, put previous figure	Comment (mandatory if derogation is granted or if non relevant)
CAC 002 A,B,C,D				
CAC 003 A,B,C				
CAC 004 A,B,C	Means of encryption used: Organization that have controlled means of encryption, if any:			
CAC 005 A,B,C,D				
CAC 006 A,B,C,D				
CAC 007 A,B				
CAC 008 A,B,C				
CAC 009 A,B,C,D				
CAC 010 A,B				
CAC 011 A,B,C,D				
CAC 012 A,B,C,D				
CAC 013 A				
CAC 014 A,B,C				
CAC 015 A,B,C,D				
(1) A,B,C,D: Letters refer to categories described in Sec 2, [2.2.1]. The requirement shall be taken into account for mentioned categories.				

Product Name:			Type of product survey (Initial/Delivery): Date of survey: Name and signature of surveyor: BV Stamp:	
Categor(ies) of Product surveyed within the scope of NR 642:				
IDENTIFICATION CODE **(1)**	Specific Information to be mentioned by Surveyor	Maximum Level reached (none,1, 2 or 3) before any derogation or, non relevant	Maximum Level reached (1, 2 or 3) after derogation if any. If no derogation, put previous figure	Comment (mandatory if derogation is granted or if non relevant)
CAC 016 A,B,C	Description of means of protection:			
CAC 017 A,B				
CAC 018 A,B,C,D				
CAC 019 A,B,C				
CAC 020 A,B,C				
CAC 021 A,B				
CAC 022 A,B				
CAC 023 A				
CAC 024 A,B				
DUR 001 A,B,C				
DUR 002 A,B,C	Main configuration parameters for cybersecurity tools:			
DUR 003 A,B,C,D				
DUR 004 A,B,C,D				
JOUR 001 A,B,C,D				
JOUR 002 A,B,C,D				
(1) A,B,C,D: Letters refer to categories described in Sec 2, [2.2.1]. The requirement shall be taken into account for mentioned categories.				

Product Name:			Type of product survey (Initial/Delivery): Date of survey: Name and signature of surveyor: BV Stamp:	
Categor(ies) of Product surveyed within the scope of NR 642:				
IDENTIFICATION CODE **(1)**	Specific Information to be mentioned by Surveyor	Maximum Level reached (none,1, 2 or 3) before any derogation or, non relevant	Maximum Level reached (1, 2 or 3) after derogation if any. If no derogation, put previous figure	Comment (mandatory if derogation is granted or if non relevant)
JOUR 003 A,B,C,D				
MCS 001 A,B,C,D				
MCS 002 A,B,C,D				
MCS 003 A,B,C				
MCS 004 A,B,C,D				
MCS 005 A,B,C,D				
PDS 001 A				
PDS 002 A,D	Means of encryption used: Organization that have controlled means of encryption, if any:			
PDS 003 A,D				
PDS 004 A				
PDS 005 A,B,C				
PDS 006 A				
PRODEF 001 A,B,C,D				
PRODEF 002 A,B,C,D				
(1) A,B,C,D: Letters refer to categories described in Sec 2, [2.2.1]. The requirement shall be taken into account for mentioned categories.				

Product Name:			Type of product survey (Initial/Delivery): Date of survey: Name and signature of surveyor: BV Stamp:	
Categor(ies) of Product surveyed within the scope of NR 642:				
IDENTIFICATION CODE **(1)**	Specific Information to be mentioned by Surveyor	Maximum Level reached (none,1, 2 or 3) before any derogation or, non relevant	Maximum Level reached (1, 2 or 3) after derogation if any. If no derogation, put previous figure	Comment (mandatory if derogation is granted or if non relevant)
PRODEF 003 A,B,C,D				
PRODEF 004 A,B				
PTF 001 A,B,C,D				
PTF 002 A,B,C,D				
PTF 003 A,B				
PTF 004 A,B,C,D	Means of encryption used: Organization that have controlled means of encryption, if any:			
PTF 005 A,B,C,D				
SUP 001 A,B,C,D				
SUP 002 A,B,C,D				
SUP 003 A,B				
FOURN 001 A,B,C,D				
FOURN 002 A,B,C,D				
FOURN 003 A,B,C,D				
FOURN 004 A,B,C,D				
(1) A,B,C,D: Letters refer to categories described in Sec 2, [2.2.1]. The requirement shall be taken into account for mentioned categories.				

Product Name:			Type of product survey (Initial/Delivery): Date of survey: Name and signature of surveyor: BV Stamp:	
Categor(ies) of Product surveyed within the scope of NR 642:				
IDENTIFICATION CODE **(1)**	Specific Information to be mentioned by Surveyor	Maximum Level reached (none,1, 2 or 3) before any derogation or, non relevant	Maximum Level reached (1, 2 or 3) after derogation if any. If no derogation, put previous figure	Comment (mandatory if derogation is granted or if non relevant)
FOURN 005 A,B,C,D				
FOURN 006 A,B,C,D				
FOURN 007 A,B,C,D				
FOURN 008 A,B,C,D				
FOURN 009 A,B,C,D				
FOURN 010 A,B,C,D				
GLOBAL LEVEL FOR PRODUCT (Minimum of last column figures):				
(1) A,B,C,D: Letters refer to categories described in Sec 2, [2.2.1]. The requirement shall be taken into account for mentioned categories.				

Move Forward with Confidence

Marine & Offshore
92937 Paris La Defense Cedex - France
Tel: + 33 (0)1 55 24 70 00
Website: http//www.veristar.com
Email: veristarinfo@bureauveritas.com