Guidelines for Autonomous Shipping

December 2017

Guidance Note
NI 641 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/

GUIDANCE NOTE NI 641

Guidelines for Autonomous Shipping

December 2017

Section 1 General

Section 2 Risk and Technology Assessment

Section 3 Guidelines for Functionality of Autonomous Systems

Section 4 Guidelines for Reliability of Autonomous Systems

SECTION 1 GENERAL

1 General

1.1 Context

1.1.1 Compared to conventional shipping, autonomous shipping is a great opportunity for the stakeholders of the maritime sector to improve the safety, the reliability and to reduce the costs.

But while the information and communication technologies enable the autonomy in the shipping industry, those technologies also imply new hazards that are to be identified and new associated risks that are to be mitigated.

1.2 Scope of the guidelines

1.2.1 This Guidance Note sets out the main recommendations for the design or the operation of systems which may be used to enhance the autonomy in the shipping.

1.2.2 This Guidance Note is mainly focused on surface units which may be considered as a ship by the authorities (e.g. Maritime Autonomous Surface Ships of 500 GT or more). This excludes small ships (typically length less than 20 m) and unmanned underwater vehicles.

1.3 Organization of the guidelines

1.3.1 In addition to the current introductive section, this Guidance Note includes 3 sections:

- Sec 2 is about the risk and technology assessment of new technologies used in autonomous shipping
- Sec 3 provides guidelines for ensuring a suitable level of functionality for autonomous systems
- Sec 4 provides guidelines for improving the reliability of autonomous systems.

1.4 Definitions

1.4.1 Terms used in this Guidance Note are defined below:

- Autonomous ship: ship having the same capabilities as those of a smart ship and including autonomous systems capable of making decisions and performing actions with or without human in the loop. An autonomous ship may be manned with a reduced crew or unmanned with or without supervision
- Conventional ship: ship where most essential decisions and actions are performed by the crew aboard. A conventional ship may have automated systems to assist the crew by automatically performing some actions, but those systems are always under the control of human aboard. By definition, a conventional ship is manned
- Cybersecurity: preservation of confidentiality, integrity and availability of information in the Cyberspace (ISO/IEC 27032:2012)
- Cyberspace: complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form (ISO/IEC 27032:2012)
- Ergonomics: applied science that studies, designs and adapts equipment, work and the environment to meet human capabilities and limitations and to enhance safety and comfort (ISO 14105:2011)
- Latency: the time interval between the instant at which an instruction control unit issues a call for data and the instant at which the transfer of data is started (ISO/IEC/IEEE 24765:2010)
- Level of autonomy: degree of decision making (authority) deferred from the human to the system. A global level of autonomy of the ship should be defined according to the main roles between the human and the systems. Descriptions of different levels of autonomy from the conventional ship to the fully autonomous ship are given in Tab 1. A level of autonomy should be defined for every autonomous ship's system prior to any assessment (see Sec 2, [3.4])
- Lookout: activity carried out at all times by sight and hearing as well as by all available means appropriate in the prevailing circumstances and conditions so as to make a full appraisal of the situation and of the risk of collision (ISO 8468:2007)
- Navigation: all tasks relevant for deciding, executing and maintaining course and speed in relation to waters and traffic (IACS Unified Requirements N1)
- Reliability: property of a system and its parts to perform its mission accurately and without failure or significant degradation (ISO/IEC 27036-3:2013)
- Sensor: device that responds to biological, chemical, or physical stimulus (such as heat, light, sound, pressure, magnetism, motion, and gas detection) and provides a measured response of the observed stimulus (ISO/IEC/IEEE 21451-7:2011)
- Smart ship: generic term to define a connected ship, capable of collecting data from sensors and having the capacity to process a large amount of data in order to assist the crew during the decision making process. Compared to a conventional ship, a smart ship may be manned with reduced crew or totally unmanned with a remote control

- System: combination of interacting elements organized to achieve one or more stated purposes (ISO/IEC 15288:2008)
- System element: member of a set of elements that constitutes a system. A system element is a discrete part of a system that can be implemented to fulfil specified requirements. A system element can be hardware, software, data, humans, processes (e.g., processes for providing service to users), procedures (e.g., operator instructions), facilities, materials, and naturally occurring entities (e.g., water, organisms, minerals), or any combination (ISO/IEC 15288:2008)
- System integrity: quality of a data processing system fulfilling its operational purpose while both preventing unauthorized users from making modifications to or use of resources and preventing authorized users from making improper modifications to or improper use of resources (ISO/IEC 2382:2015)
- Unmanned ship: ship that does not physically contain a human and is capable of controlled movement. Unmanned ship may be remotely controlled, supervised or fully autonomous.

1.5 Acronyms

1.5.1 Acronyms used in this Guidance Note are defined below:

AIS : Automatic Identification System
ANS : Autonomous Navigation System
CCTV : Closed Circuit Television
COLREGs: Convention on the International Regulations for Preventing Collisions at Sea
CRC : Cyclic Redundancy Check
GPS : Global Positioning System
IACS : International Association of Classification Societies
IMO : International Maritime Organisation
IT : Information Technology
LIDAR : LIght Detection And Ranging
LOS : Line Of Sight
MARPOL: International Convention for the Prevention of Pollution from Ships
NAVTEX: Navigational Telex
RCM : Risk Control Measure
RCO : Risk Control Options
SCC : Shore Control Centre
SOLAS : International Convention for the Safety of Life at Sea
STCW : International Convention on Standards of Training, Certification and Watchkeeping for Seafarers
VDR : Voyage Data Recorder
VHF : Very High Frequency
VSAT : Very Small Aperture Terminal
VTS : Vessel Traffic Services.

2 Safety and security conditions

2.1 General

2.1.1 To achieve an acceptable level of safety and security the general principles behind the recommendations contained in this Guidance Note are given in [2.2] to [2.7].

2.1.2 The threats for autonomous ships are very similar to those for conventional ships, but in addition new threats may arise from the reduction or absence of crew aboard. They are mainly coming from the environment, other ships in its vicinity and operations of the considered ship.

Compared to conventional ships, the management of the risks is transfered from the crew aboard to the sensors and the software and ultimately to the supervisors onshore.

2.1.3 It is required that autonomous or remotely controlled ships should be at least as safe as a conventional ship having the same purpose or design (e.g. carrying cargo or passengers).

For safe operations, autonomous ships should not be a source of danger to themself, to the other ships around, to the maritime infrastructures and to the marine environment.

Table 1 : Ship categories and level of autonomy

Ship category	Level of autonomy		Manned	Method of control	Authority to make decisions	Actions initiated by
Conventional	0	Human operated	Yes	Automated or manual operations are under human control	Human	Human
Smart	1	Human directed	Yes/No	Decision support Human makes decisions and actions	Human	Human
Autonomous	2	Human delegated	Yes/No	Human must confirm decisions	Human	System
	3	Human supervised	Yes/No	System is not expecting confirmation Human is always informed of the decisions and actions	Software	System
	4	Fully autonomous	No	System is not expecting confirmation Human is informed only in case of emergency	Software	System
Note 1: Definitions of the level of autonomy are given in Sec 2, Tab 16						

2.2 Main ship capabilities

2.2.1 The autonomous ships should be capable of:

- managing a pre-defined voyage plan and updating it in real-time if relevant
- navigating according to the predefined voyage plan and avoid collisions with obstacles coming from the traffic or unexpected objects
- keeping a sufficient level of manoeuvrability and stability in various sea states
- withstanding unauthorized physical or virtual trespassing.

2.2.2 The autonomous ships should be designed to authorize a human to come aboard for controlling the ship, for example when a critical situation arises (e.g. fire, flooding, loss of propulsion etc).

During the sea trials or for survey in service, the autonomous ships should be designed to accept the presence of a human aboard or in their vicinity.

Regardless of the possibility of a remote control, the autonomous ships should be designed to be controlled aboard by either a portable device (e.g. laptop) or by a built-in control system.

The possibility for a human to take the control aboard should be granted only to the authorized personnel, in particular when the autonomous ships carry passengers.

A passenger of autonomous ships should have the possibility to activate an emergency push button in case of critical situation (e.g. passenger overboard, obstacle during docking).

2.3 Infrastructure

2.3.1 Shore Control Centre

The Shore Control Centre (SCC) should be considered as an extension of the ship. To prevent that unexpected events on the SCC could have consequences on the ship (e.g. fire, earthquake), mitigation measures should be integrated in the design and operations of the SCC.

Those measures should not interfere with land-based regulations (e.g. lockdown during manoeuvre and procedure for fire escape) which may differ from one country to the other depending on where the SCC is located.

The SCC, including facility and manning, should be qualified with regard to each ship it is supervising. When the SCC is used for an additional ship, a new qualification should be obtained by the SCC for this ship.

When the ship operates near restricted area (e.g. military fleet), it should be necessary to have more stringent measures for the protection of the SCC (e.g. to avoid terrorist attack).

2.3.2 Interaction with the maritime infrastructure

Interaction with other autonomous or conventional ships should be taken into consideration during the design and the operation. The autonomous ships should not interfere with the communications between other ships operating in their vicinity. However, the autonomous ships should be able to respond at any usual request (e.g. identification, position) from other ships by means of radio communications or visual signals.

Port and coastal authorities should be able to communicate with autonomous ships in order to be informed about the planned manoeuvres and to be able to regulate the traffic.

2.4 Reliability

2.4.1 Compared to a conventional ship, the autonomous ships may have less or even no crew aboard to rely on for maintenance operations and corrective tasks due to system failure. Consequently, the systems should be designed to be resilient to failure (e.g. fault tolerant) and to have extended maintenance intervals (see Sec 4).

2.4.2 Highest reliability should be achieved by introducing efficient diagnostics and predictive algorithms for controlling the risk of failures and pre-scheduling maintenance operations that should be performed in harbour (e.g. by using a condition-based maintenance).

2.4.3 The usage of an intensive remote monitoring and control of the status of the equipment should be considered in order to prevent failures.

2.4.4 A partial or full redundancy are some solutions to improve the availability for critical systems such as communication infrastructure or machinery.

2.4.5 Redundancy is easiest to achieve for ships with electrical propulsion. Generators producing electricity for recharging batteries or additional emergency batteries should be considered as a simple and cost-effective way to improve the propulsion and steering reliability.

2.5 Human factors

2.5.1 The multiple sensors used for the monitoring increase a lot the amount of information provided to an operator. In order to avoid the risk of overload of information that may reduce the accuracy of the actual ship situation, a fusion of the data collected by the sensors should be proposed to the operator.

2.5.2 The ergonomics of monitoring systems should take into account the human vigilance that could be reduced during extended periods of remote control or when several ships which are in different situations are managed by only one operator.

2.5.3 The remote operator should be aware of the latency due to the communication that cause a delay between his/her action and the actual ship reaction. The latency should be continuously displayed during the operations (e.g. manoeuvring) and a warning should be issued when the latency is over pre-defined limits.

2.6 Cybersecurity

2.6.1 The usage of information and communication technologies makes possible virtual unauthorized or malicious actions to autonomous ships (e.g. virus infection). Data communication between ship and shore or GPS signal could be intentionally disturbed or changed in order to hijack the ship or cause severe damages.

2.6.2 Amongst the best practices for the usage of information and communication technologies, measures should be adopted to provide the highest level of confidence for data (e.g. protection, encryption) and for user access (e.g. password authentication).

2.7 Cargo

2.7.1 Likewise for all conventional ships, the cargo on autonomous ships should be carefully loaded and monitored because the consequences for the ship could be from a simple shifting to fire or flooding.

2.7.2 The correct stowage of cargo aboard should rely on port operators, since the autonomous ships have few means (less or no crew and equipment) for ensuring a proper cargo securing at sea.

3 Regulations

3.1 General

3.1.1 Autonomous ships should be compliant with all relevant regulations from international conventions adopted by IMO or from local legislation. If necessary, exemptions or equivalent solutions should be explicitly approved by the Administration.

3.2 SOLAS

3.2.1 The following regulations from Chapter V (Safety of navigation) should have a special interest for autonomous ships:

- Reg.14: Ships' manning
- Reg.15: Principles relating to bridge design, design and arrangement of navigational systems and equipment and bridge procedures
- Reg.22: Navigation bridge visibility
- Reg.24: Use of heading and/or track control systems
- Reg.33: Distress situations: obligations and procedures
- Reg.34: Safe navigation and avoidance of dangerous situations.

The Reg. 12 from Chapter IV (Radio-communications) relative to the continuous watches should also be considered.

3.2.2 Regarding the obligation of assistance in distress situations, autonomous ships should be able to, at least, ensure that distress signals are received and relayed to the relevant search and rescue authorities.

3.3 MARPOL

3.3.1 Provisions for prevention of pollution should not have any onerous consequences in the design and operation for autonomous ships. However, attention should be paid to the regulations about prevention of pollution by oil, in particular to enable a full automatic control of operations of oil discharges. In a similar way, it should be always possible to automatically control the air emissions from autonomous ships.

3.3.2 All record books to report operations as required by the MARPOL should be maintained in an electronic format.

3.4 COLREGs

3.4.1 To prevent collision at sea, the two main tasks that should be handle by autonomous ships are:

- the look-out:

  to ensure that ships are always monitored by using appropriate information to have a full appraisal of the situation and the risk of collision
- the operational decisions:

  obligation for ships to take avoidance decisions.

3.4.2 Autonomous ships should be able to inform other ships about its status and intentions, by giving a specific light signal or communication message (e.g. AIS). The autonomous ships should be able to communicate with other ships to determine if the intentions have been understood and if it is necessary to provide recommendations such as to change the route because of a risk of a collision.

This signalling should be resilient to any communication failure, and for this particular case, the status should be "not under command".

3.5 STCW

3.5.1 The requirements of STCW should be used as a basis for the qualification and the definition of duties for the personnel operating ships. In particular, the responsibilities of the watchkeeping should be adjusted taking into account that the officers could be shore-based or the crew reduced.

SECTION 2 RISK AND TECHNOLOGY ASSESSMENT

1 General

1.1 Purpose and approach

1.1.1 The risk and technology assessment are two qualitative assessments which are the most appropriate for dealing with novel technology that may be used for autonomous ships.

1.1.2 The purpose of those assessments is to identify and to reduce as low as reasonably practical the risks due to hazards that may threaten autonomous ships.

1.1.3 The risk-based approach considers autonomous ships as a model of several different interconnected systems aboard and onshore.

1.1.4 The measures to mitigate the risks should be founded on prescriptive requirements already existing in the Rules or in other standards or guidance notes from the industry or regulatory bodies.

2 Risk assessment

2.1 Methodology

2.1.1 References

The process for the risk assessment should be based on the techniques available in the following documents:

- IMO MSC-MEPC.2/Circ.12 Revised Guidelines for Formal Safety Assessment (FSA)
- ISO/IEC 31010:2009 Risk management - Risk assessment techniques
- ISO/IEC 27005:2011 Information technology — Security techniques — Information security risk management.

2.1.2 Stages

The risk assessment should be performed according to the following stages:

a) model of the autonomous ship's systems (see [2.2])

b) in case the system is not based on a qualified technology, a technology assessment should be carried (see [3])

c) hazards identification (see [2.3])

d) risk analysis and associated outcome (see [2.4])

e) risk control options to eliminate intolerable risks (see [2.5]).

2.2 Model of autonomous ship

2.2.1 At the first stage of the risk assessment, the systems of the autonomous ship, including maritime infrastructure (SCC), should be split into several groups of functions covering all aspects of the operations.

As a guidance, the following groups of functions should be considered and some are detailed in [2.3.2] to [2.3.9]:

- voyage
- navigation
- detection of navigational and environmental conditions
- safety and emergency
- security
- ship strength and stability
- passenger management
- cargo management
- technical infrastructure.

2.3 Hazards identification

2.3.1 Principles

The hazards identification should cover all possible sources of hazards potentially contributing to undesirable events or accidents.

The consideration of a functional failure associated with the consequence of an accident scenario should be governing the process of identification.

As a guidance, for some group of functions, a list of typical hazards for autonomous ships are given in [2.3.2] to [2.3.9].

2.3.2 Voyage

The hazards that should be considered for voyage purpose are summarized in Tab 1.

2.3.3 Navigation

The hazards that should be considered for navigation purpose are summarized in Tab 2.

2.3.4 Detection of navigational or environmental conditions

The hazards that should be considered for detection purpose are summarized in Tab 3.

2.3.5 Safety and emergency

The hazards that should be considered for safety and emergency purpose are summarized in Tab 4.

Table 1 : Hazards for the voyage

Hazard	Consequence
Failure of ship-shore connection	Loss Collision Sinking
Failure of update (e.g. of nautical publications, weather forecasts)	Grounding Sinking
Human error in input of voyage plan	Loss
Human error in remote monitoring and control (e.g. through situation unawareness, data misinterpretation, SCC capacity overload)	Collision
Human error in remote maintenance	Loss Sinking

Table 2 : Hazards for the navigation

Hazard	Consequence
Heavy traffic	Collision
Heavy weather	Sinking
Low visibility	Collision
Propulsion failure	Collision Grounding
Sensor failure	Collision
Marine wildlife (e.g. whales, squids, carcasses)	Collision
Floating objects	Collision
Offshore installations	Collision

Table 3 : Hazards for the detection

Hazard	Consequence
Failure in detection of small objects (wreckage)	Collision
Failure in detection of collision targets	Collision
Failure in detection of navigational marks	Grounding
Failure in detection of ship lights and shapes	Collision
Failure in detection of semi-submerged towed or floating devices (e.g. seismic gauges, fishing trawls)	Collision
Detection of unforeseeable events (e.g. freak wave)	Sinking
Detection of considerable data discrepancy between charted water depth and sounded water depth - grounding objects	Grounding
Detection of considerable data discrepancy between weather forecast and actual weather situation	Sinking

Table 4 : Hazards for the safety and emergency

Hazard	Consequence
Failure in position fixing (due to e.g. GPS selective availability)	Collision
Communication failure in case of other ship in distress (e.g. message reception, relay, acknowledgment)	Loss of other ship
Communication failure in case of own ship in distress (e.g. with SCC, relevant authorities, ships in vicinity)	Loss
Fire	Loss
Water flooding - sudden hull damage	Loss

2.3.6 Security

The hazards that should be considered for security purpose are summarized in Tab 5.

2.3.7 Ship strength and stability

The hazards that should be considered for ship strength and stability purpose are summarized in Tab 6.

2.3.8 Passenger management

The hazards that should be considered in case of a ship carrying passengers are summarized in Tab 7.

2.3.9 Technical infrastructure

The hazards that should be considered for the technical infrastructure are summarized in Tab 8.

Table 5 : Hazards for the security

Hazard	Consequence
Willful damage to ship structures by others (e.g. pirates, terrorists)	Sinking
Attempt of unauthorised ship boarding (e.g. pirates, terrorists, stowaways, smugglers)	Illegal actions Hijack Loss
Failure of ship's IT systems (e.g. due to bugs)	Loss
Jamming or spoofing of AIS or GPS signals	Collision
Jamming or spoofing of communications, hacker attack, also on SCC (e.g. in case of pirate or terrorist attack)	Collision Grounding

Table 6 : Hazards for the ship strength and stability

Hazard	Consequence
Loss of intact stability due to structural damage	Sinking
Loss of intact stability due to unfavorable ship responses (e.g. to waves)	
Loss of intact stability due to shift and/or liquefaction of cargo	
Loss of intact stability due to icing	

Table 7 : Hazards for the passengers

Hazard	Consequence
Too many passenger onboard (overload)	Sinking
Passenger overboard	Human injury or fatality
Passenger unwellness	Human injury
Passenger injured during arrival or departure	
Passenger interfering in an onboard system (deliberately or not)	Illegal actions Hijack Loss

Table 8 : Hazards for the technical infrastructure

Hazard	Consequence
Sensor / Actuator failure	Loss of control
Sensor / Actuator failure due to ship icing	Loss of observation
Temporary loss of electricity (e.g. due to black-out)	Loss of control
Permanent loss of electricity	Loss of control Grounding
Failure of ship's IT infrastructure (e.g. due to fire in the server room)	Loss of control
Part failure or total loss of propulsion system	Loss of control
Part failure or total loss of rudder function	Loss of control
Failure to drop anchor when drifting	Grounding
Unavailability of SCC (fire, environmental phenomenon...) or of operator (faintness, emergency situation, etc.)	Loss of control

Table 9 : Frequency index

Index	Definition	Definition	Per ship year
7	Frequent	Likely to occur once per month on one ship	10
6	Common	Likely to occur once per year on one ship	1
5	Reasonably	Likely to occur once per year in a fleet of 10 ships, i.e. likely to occur a few times during the ship's life	0,1
4	Possible	Likely to occur once per year in a fleet of 100 ships	10^{-2}
3	Remote	Likely to occur once per year in a fleet of 1000 ships, i.e. likely to occur in the total life of several similar ships	10^{-3}
2	Unlikely	Likely to occur once in the lifetime (20 years) of a fleet of 500 ships	10^{-4}
1	Extremely unlikely	Likely to occur once in the lifetime (20 years) of a world fleet of 5000 ships	10^{-5}

2.4 Risk analysis

2.4.1 Principles

The purpose of the risk analysis is to investigate the causes and the consequences of the most important accident scenario revealed by the hazards identification. The risk for a given accident scenario due to an hazard is estimated with a risk index as a combination of the frequency of the cause and the severity of the consequence.

2.4.2 Frequency

The frequency is estimated by the probability of an event to occur once per year in a fleet of several ships having the same operating mode. The frequency indexes based on a logarithmic scale are summarized in Tab 9.

2.4.3 Severity

The severity is estimated according to the impact on the human, the ship or the environment. The severity indexes based on a logarithmic scale are summarized in Tab 10 to Tab 12.

2.4.4 Risk index

The risk index is calculated before any mitigation measure and is obtained on a logarithmic scale by adding the frequency and the severity indexes defined in [2.4.2] and [2.4.3]:

Risk index = Frequency index + Severity index

Finally a risk matrix should be derived to obtain the final risk index.

2.4.5 Risk analysis outcome

For each hazard, the risk index should be evaluated in order to identify the highest risks by considering separately the impact on human, ship and environment. Example of risk analysis outcome is given in Tab 13.

Threshold for risk tolerance may be estimated for example with regard to economic parameters.

Table 10 : Severity index for the human

Index	Definition	Human	Equivalent fatalities
1	Minor	Single or minor injuries	0,01
2	Significant	Multiple or severe injuries	0,1
3	Severe	Single fatality or multiple severe injuries	1
4	Catastrophic	Multiple fatalities	10

Table 11 : Severity index for the ship

Index	Definition	Ship	Equivalent damage
1	Minor	Local equipment damage	0,01
2	Significant	Non-severe ship damage	0,1
3	Severe	Severe damage	1
4	Catastrophic	Total loss	10

Table 12 : Severity index for the environment

Index	Definition	Environment	Equivalent oil or chemical substance spill
1	Minor	Local spill	< 1 t
2	Significant	Significant local spill	1 - 100
3	Severe	Severe large spill	100 - 10 000 t
4	Catastrophic	Very large spill	> 10 000 t

Table 13 : Risk analysis outcome

Hazard	Consequence	Frequency index	Severity index			Risk index		
			Human	Ship	Environment	Human	Ship	Environment
Failure of ship's IT systems (e.g. due to bugs)	Loss	3	1	4	1	4	7	4
Failure in position fixing (due to e.g. GPS selective availability)	Collision	4	2	2	1	6	6	5
Low visibility	Collision	7	2	2	1	9	9	8
Fire	Loss	4	1	4	2	5	8	6

Table 14 : Risk Control Options

Category	Risk Control Option
Unmanned ship and Ship Control Centre	Design of SCC for a proper control and monitor. Suitable SCC manning as well as training of personnel.
	Absence of human is required on unmanned ship.
	Ship should be directly controlled in heavy or complex traffic.
	A ship without accommodation section is much easier to secure against stowaways in enclosed spaces.
Unmanned maintenance and technical operations	Design of aboard systems for easy maintenance and accurate monitoring of maintenance state. Must also be fast to repair.
	Need redundant power generation, distribution, propulsion and steering.
	Automated fire extinguishing systems are required in all relevant areas. Note that no crew makes this simpler as areas are smaller and that CO^2 can be used more safely.
	Improved cargo monitoring and planning is required.
Heavy weather	Software are to be able to avoid heavy or otherwise dangerous weather – use of weather routing.
Sensors systems	Need good sensor and avoidance systems. Selected systems must also be redundant so that a single failure does not disable critical functions identified during the risk assessment.
Cybersecurity	Cybersecurity measures are important, including alternative position estimation based on non-GPS systems. The SCC may be particularly vulnerable. Data communication links must also have sufficient redundancy.

2.5 Risk Control Options

2.5.1 Principles

The Risk Control Options (RCO) should be determined to prevent the occurrence or to mitigate the consequences of an accident scenario.

2.5.2 Risk Control Measures

The RCOs are constituted by a collection of Risk Control Measure (RCM). Each potential RCM should be select100

ed by considering one or more, but not limited to, the following attributes:

- preventive:

  when reducing the probability of the event
- mitigate:

  when reducing the severity of the outcome of the event
- engineering:

  where safety features (either built in or added on) are within the design
- inherent:

  where choices are made in the design concept that restrict the level of potential risk
- procedural:

  when operators control the risk by behaving in accordance with defined procedures.

Typical Risk Control Options for autonomous ships are given as a guidance in Tab 14.

3 Technology assessment

3.1 Reference

3.1.1 When the design and the reliability of a ship's system are not covered by any existing standard, a technology assessment should be carried out.

The technology assessment should be based on the following methodologies:

- Risk Based Qualification of New Technology - Methodological Guidelines in the latest revision of the Bureau Veritas Guidance Note NI 525 and summarized in [3.3]
- Independent Safety Assessment (ISA)
- Goal Structuring Notation (GSN).

3.2 General

3.2.1 The risk assessment described in [2] is influenced by the level of confidence and the degree of autonomy existing for the technologies used in systems for autonomous ships.

The purpose of the technology assessment is to evaluate a level of confidence having an influence on the probability of failure (impact on the frequency) and/or on the consequences of this failure (impact on the severity).

To increase or decrease the induced risk by a novel technology, the level of confidence in this technology should be rated according to [3.3].

To estimate the impact of an autonomous system failure using a novel technology, the level of autonomy should be defined according to [3.4].

3.3 Technology rating

3.3.1 The novelty of the technology is rated taking into account both the level of maturity and the proposed conditions of operation (see Tab 15).

3.4 Level of autonomy

3.4.1 The level of autonomy should be defined to make a distinction between the role of the human and the role of the system among the various functions of the system. These functions are based on a four-stage model of human information processing and can be translated into equivalent system functions (see Tab 16):

a) information acquisition

b) information analysisML

c) decision and action selection

d) action implementation.

The four functions can provide an initial categorisation for types of tasks in which automation can support the human.

For a high level of autonomy the impact of a system error will be predominant, whereas for a low level of autonomy, the impact of an human error will be predominant.

Table 15 : Technology rating

Technology maturity	Application conditions	
	Similar	Different
Proven	0	1
Limited references	1	2
Extrapolated from proven	2	3
New	3	3

Table 16 : Level of autonomy

Level of autonomy		Definition	Acquisition	Analysis	Decision	Action
0	Human operated	Human makes all decisions and controls all functions	System Human	Human	Human	Human
1	Human directed	System suggests actions Human makes decisions and actions	System	System Human	Human	Human
2	Human delegated	System invokes functions Human can reject decisions during a certain time	System	System	System Human	Human
3	Human supervised	System invokes functions without waiting for human reaction	System	System	System	System Human
4	Fully autonomous	System invokes functions without informing the human, except in case of emergency	System	System	System	System

SECTION 3 GUIDELINES FOR FUNCTIONALITY OF AUTONOMOUS SYSTEMS

1 General

1.1 Scope

1.1.1 This Section provides guidelines for ensuring a suitable level of functionality of systems associated with essential services involved in the operations of autonomous ships.

For each autonomous system, a goal-based approach has been used to set a minimum level of functionality and associated recommendations for the system design.

2 Navigation system

2.1 Goal

2.1.1 The goal of the Autonomous Navigation System (ANS) is to be able to navigate a ship safely and efficiently along a predefined voyage plan taking into account of traffic and weather conditions.

2.2 Functional requirements

2.2.1 The Autonomous Navigation System should be responsible for all navigation-related matters with respect to the legal framework.

2.2.2 The ANS should include SCC communication capabilities for remotely controlled or remotely supervised voyage planning and navigation.

2.2.3 The ANS should be aware of traffic and weather conditions and should be able to make a modification of the navigation path accordingly while keeping the ship on the pre-defined voyage plan.

2.2.4 The mooring and unmooring operations, as well as the harbour navigation or port approach should be remotely supervised or controlled in case the level of autonomy doesn't allow a full autonomy for these operations.

2.2.5 In case of problems of connectivity, a fail-safe sequence should be defined to put the ship in a safe situation in accordance with the operating mode and the level of autonomy (e.g. manoeuvring in harbor or at sea).

2.3 References

2.3.1 The navigation system should be compliant with the applicable requirements and regulations related to the assignment of the following additional class notation from NR467 Rules for Steel Ships:

- for integrated bridge system (**SYS-IBS**, see NR467 Pt F, Ch 4, Sec 2)
- for dynamic positioning with redundancy (**DYNAPOS AM/AT R**, see NR467 Pt F, Ch 11, Sec 6).

2.4 Voyage planning

2.4.1 The voyage plan describing the full voyage from departure to arrival and taking into account the charts and weather forecasts should be defined and updated at any time by a shore-based operator.

2.4.2 The voyage plan should be established by defining waypoints, headings, turning angles and safe speeds the ship must follow during its voyage.

2.4.3 Depending on the level of autonomy, the ANS should be able to notify the SCC each time the ship is deviating from the planned course and should send an alarm when the deviation is out of specified margins. The tolerance in the deviation should be set in accordance with the context (e.g. in heavy traffic or open sea) in order to avoid overload of information for the supervisor.

2.4.4 In case the connection between ship and shore is unavailable for a period of time, to be defined depending on the level of autonomy, the ship is to enter into a fail-safe sequence.

The purpose of this specific fail-safe sequence is to recover a safe situation for the ship and may include the following stages to be considered with regard to the risk assessment:

a) operator attempts to take a manual control

b) ship slows down to the next waypoint

c) ship stops and stays at the current position

d) ship sails back to the previous waypoint.

2.5 Navigation

2.5.1 The data from various ship's sensors should be gathered and evaluated in order to thoroughly determine the location and heading of the ship. Redundant sensors and positioning by multiple sources should ensure a high degree of data accuracy. The current speed and water depth should be monitored as well.

2.5.2 The data for navigational and weather forecast should be retrieved from combined external sources such as the SCC, AIS transceivers or data providers (Navigational Telex NAVTEX, SafetyNET).

2.5.3 The ANS should identify the COLREG obligation of the ship towards all objects in the vicinity and calculate COLREG-compliant deviation measures for a given traffic conditions.

For path planning, solutions like sampling-based algorithms should be used. For collision avoidance, algorithms like velocity obstacles should be used.

2.5.4 When the level of autonomy requests supervision during operations in harbour (e.g. docking and undocking) or heavy traffic conditions near shore, land-based communication networks should be used to provide a maximum availability and a minimum latency.

2.6 Ship status and dynamics

2.6.1 The ship status data should include position with displacement, draft, trim, ship motions within 6 degrees of freedom and information about propulsion and steering systems. Cargo monitoring should also be part of the ship status.

2.6.2 The dynamics of the ship (velocities and acceleration) should be predicted within a short time frame (less than 5 minutes) based on own ship's characteristics as well as environmental conditions (e.g. wind, wave headings and frequencies).

2.6.3 The weight distribution aboard the ship should be calculated to determine the ship's buoyancy and to control the stability.

2.7 Lookout

2.7.1 The ship should independently gather weather data from its own sensors. The accumulated data like wind speed, wave frequencies, should be used for subsequent weather routing and should be also stored and provided to the SCC.

2.7.2 Navigational sensors aboard the ship should continuously gather data to generate a complete traffic picture of the vicinity of the ship. Objects should be detected, identified and tracked. This traffic assessment should be supported by at least one CCTV system.

2.8 Weather routing

2.8.1 The weather data which have been gathered by the ship should be evaluated in comparison with weather forecasts which have been received from shore via the SCC.

2.8.2 With this data combination a valid estimation of current and upcoming weather conditions along the navigational and voyage plan of the ship should be made.

2.8.3 Combined with predefined parameters and taking into account stability and maneuverability conditions a route optimization should be conducted under weather routing criteria.

2.9 Collision avoidance

2.9.1 To navigate the ship safely and to be COLREG-compliant a continuous monitoring of the current traffic situation should be performed.

2.9.2 All traffic-related data should be combined and assessed and possible future scenarios predicted.

2.9.3 As soon as a potential close quarters situation is identified, appropriate measures should be taken, such as:

- reduce speed
- predict and anticipate the obstacle's motions
- deviate from the initial ship's path.

2.10 Voyage recording

2.10.1 Data from essential ship processes (e.g. navigation, machinery, propulsion or any significant process identified during the risk assessment) should be received and stored in the log book. Situational data are similar to what is recorded by a VDR and should be complemented with expected or unexpected events or decisions.

2.10.2 Data type regularly submitted to the SCC and their associated intervals and amount should depend on the current ship control mode (e.g. remote or fully autonomous).

2.10.3 All log book data should be able to be retrieved directly by the SCC at any time.

2.11 Emergencies and alarm

2.11.1 Situations which are potentially threatening the safety of the ship should be managed with permanent and reliable means to inform the SCC and other ship's processes (e.g. fire alarms).

2.12 Devices used for situational awareness

2.12.1 Relevant input parameters for the process of autonomous navigation should be provided by devices (e.g. sensors) to have an accurate situational awareness, which provides the ANS with a perception of the vicinity of the ship, including environmental conditions as well as with target data for detected objects.

This perception should be done for example by using a sensor fusion-based approach where raw sensor data from existing navigational sensors (e.g. data provided by LIDARs, cameras, radars and GNSS) are gathered, processed and correlated among themselves to map a realistic representation of the ship's environment.

2.12.2 Special attention should be paid to the limitations due to technical reasons and legal reasons (COLREGs). The sensors should be able to detect floating or partly submerged object of standard container size (typically several meters) in a mid-range distance (typically less than one kilometer).

2.12.3 The sensors should be also capable of detection of a life raft or a person in the water in a short range distance (typically several hectometers).

2.12.4 The sensors should be able to detect any limitation in the operating range such as a reduced visibility (e.g. use of Circular Error Probability to detect uncertainties of object position).

3 Communication network and system

3.1 Goal

3.1.1 The goal of the communication network and system is to be available to transfer data externally (ship to shore, ship to ship) and internally, without compromising their integrity.

3.2 Functional requirements

3.2.1 Land-based and space-based communication system should be used for the ship to shore communications. For ship to ship communications, a line of sight (LOS) communication system should be used.

3.2.2 The ship should include an efficient and secure network for communication between systems internally and externally.

3.2.3 The communication system should be designed to operate with different level of communication quality and should be resilient to a signal degradation.

3.3 References

3.3.1 The communication network and system should be compliant with the applicable requirements from IEC 61850-90-4 Network Engineering.

3.4 Type of communication system

3.4.1 For external communication, in order to maintain a correct level of availability in case of failure, backup arrangement is to be provided for the transmission of critical data. In the event of a failure, an automatic transition between the main and the backup solution should be provided, and an alarm should be triggered. A solution should be to use two independent communication systems, for example the Iridium system and a VSAT system operating outside the L-band.

3.4.2 Different frequency bands should be used in order to minimize the risks of disturbance of signals due to atmospheric effects (e.g. fading due to heavy rain).

3.4.3 Line of sight communication systems should be mainly based on AIS or digital VHF systems with a range of at least two kilometers.

3.5 Performance

3.5.1 Remotely controlled ship should require more communication bandwidth for operation than a conventional ship and should need several communication channels.

3.5.2 Bandwidth and latency of the communication network and system should be adequate for the traffic that is mainly oriented from ship to shore due to the amount of data transmitted by the autonomous systems.

3.5.3 The minimum bandwidth and latency for various types of data streaming are given as a guidance in Tab 1.

3.5.4 Methods for reducing the amount of data to only what is needed for human perception should be considered. Such methods should be the reduction of the frame-rate, the image resolution or an efficient image compression.

Table 1 : Minimum bandwidth and latency

Data streaming	Bandwidth (KBps)	Latency (sec)
Ship to ship	2	0,05
Remote control	2	1
Telemetry	32	1
Radar images	75	1
Video (HD)	3000	2,5

4 Machinery system

4.1 Goal

4.1.1 The goal of the autonomous machinery system is to ensure that safety in all sailing conditions, including manoeuvring is equivalent to that of a ship having machinery spaces manned.

4.2 Functional requirements

4.2.1 The autonomous machinery system should control and monitor the propulsion plant and steering system.

4.2.2 The autonomous machinery system should mitigate the impact of emergency situations such as fire and flooding.

4.2.3 A maintenance plan should be developed for an extensive period of time and should include adequate preventive actions for limiting periodic maintenance tasks.

4.3 References

4.3.1 The machinery system should be compliant with the applicable requirements and regulations related to the assignment of the following additional class notation from NR467 Rules for Steel Ships:

- for integrated machinery spaces (**AUT-IMS** see NR467 Pt F, Ch 3, Sec 4)

- for automated operation in port (**AUT-PORT** see NR467 Pt F, Ch 3, Sec 3)
- for availability of machinery (**AVM-IPS** see NR467 Pt F, Ch 2, Sec 3).

4.4 Monitoring

4.4.1 The machinery system should be able to collect and analyse information about operating condition and health condition from, but not limited to, the main engine, engine for auxiliary systems and shafting. A visual monitoring should be provided by at least one CCTV system.

4.4.2 The data from diagnostics should be transmitted, recorded and documented in a suitable format to be used by the remote controller or the supervisor.

4.5 Maintenance

4.5.1 The machinery system should be designed to allow an extended period of time without any physical interference in the machinery spaces (e.g. 500 hours).

4.5.2 Based on the condition assessment of the machinery, the system should suggest or take corrective actions for the prevention of machinery failure. Instead of a condition-based maintenance, systematic preventive maintenance should also be adopted.

4.5.3 Information on the need for spare parts that enable ordering in advance should be delivered to the operator.

4.6 Emergency management

4.6.1 An alarm system should be provided to allow identification of faults in the machinery and should be able to communicate with a remote SCC.

4.6.2 The alarm system should be triggered by sensors such as IR-cameras, water inrush detectors, gas and fire detectors.

4.6.3 In case of the detection of an emergency situation, the system should be able to automatically activate means to recover a safe situation or at least to mitigate the damages (e.g. automatic change-over).

4.6.4 Fire fighting systems or pumps should be able to start automatically upon the request of the system or the operator. Means should be provided to prevent any inadvertent starting of fire fighting systems.

5 Cargo management system

5.1 Goal

5.1.1 The goal of the autonomous cargo management system is to ensure that cargo does not compromise the safety of the ship or not degrade the environment.

5.2 Functional requirements

5.2.1 The autonomous cargo management system should collect and monitor the main cargo parameters.

5.2.2 The loading and unloading sequences should be properly handled by the autonomous cargo management system.

5.3 References

5.3.1 The cargo management system should be compliant with the applicable requirements and regulations related to the assignment of the following additional class notation:

- for liquid cargo in bulk (**CARGOCONTROL**, see NR467 Pt F, Ch 11, Sec 9)
- for liquid cold cargo (**COLD CARGO**, see NR467 Pt F, Ch 11, Sec 11)
- for refrigerated cargo (**REF-CARGO**, see NR467 Pt F, Ch 7, Sec 2).

5.4 Monitoring

5.4.1 The cargo parameters should be collected and analysed by means of sensors installed in the cargo hold, within the carrying device or directly on the cargo. A visual monitoring should be provided by at least one CCTV system.

5.4.2 The temperature, the pressure, the gas, the water incoming, the cargo shifting, are the main parameters that should be monitored.

5.4.3 An alarm system able to issue warning or alert to the operator should be provided for the detection of abnormal values for each cargo parameter.

5.5 Control

5.5.1 Means should be provided to automatically control the cargo parameters, such as for heating, cooling, ventilating or pumping.

5.6 Loading and unloading

5.6.1 During the loading and unloading sequences, the autonomous cargo management system should monitor the cargo capacity, the ballast water, the ship's structural strength and the stability (loads induced by the cargo).

6 Passenger management system

6.1 Goal

6.1.1 The goal of the passenger management system is to ensure the safety of passengers during a voyage on autonomous ships.

6.2 Functional requirements

6.2.1 The passenger management system should prevent any overload due to an exceedance of the ship's capacity.

6.2.2 During boarding and un-boarding sequences, the passenger management system should prevent any passenger from injury.

6.2.3 In case of a critical incident (e.g. man overboard), the passenger management system should provide means for alerting and rescuing.

6.2.4 All systems onboard should be designed to avoid any deliberate or unwilled interference or obstruction by a passenger.

6.3 References

6.3.1 The passenger management system should be compliant with the applicable requirements and regulations of SOLAS, in particular those from Chapter III about Life-saving appliances and arrangements.

6.4 Overload prevention

6.4.1 In order to prevent the overload, a system should be provided to determine the number of passenger with regard to the capacity of the ship. This system should be arranged prior to the boarding stage of the passengers.

6.4.2 In order to ensure that the ship has sufficient freeboard, an alarm should be installed and triggered when the waterline exceed the load line.

6.4.3 The ship's capacity should be estimated by a maximum number of person and/or approximate weight. This estimation should take into account a safety margin for additional weight per passenger (e.g. due to luggage, bicycle...).

6.5 Boarding sequence

6.5.1 The docking and undocking procedures should be monitored by sensors (e.g. pressure sensors, radar...) to confirm that there are no obstacles for the safe progress.

6.5.2 In case the system is not able to detect a situation of danger, an emergency push button should be accessible to the passengers to stop the sequence.

6.6 Life saving

6.6.1 The life saving appliances should be stowed in order to be accessible for all passengers and should be designed to be simple to use. A convenient solution should be for each passenger to wear a life jacket.

6.6.2 In case of a passenger overboard, an alarm should be accessible to the passengers onboard (emergency push button) and/or should be activated by the passenger in the water (radio or water activated) to maintain the ship near the actual position and to alert the rescue team.

7 Shore control centre

7.1 Goal

7.1.1 The goal of the Shore Control Centre is to be able to continuously control and monitor several autonomous ships of the same or different type.

7.2 Functional requirements

7.2.1 The SCC system should be designed for displaying suitable information, facilitate the decision making process and remote control for the operator.

7.2.2 The SCC system should provide means of communications with the autonomous ships and any other decision centre taking part in the operation of the ship.

7.2.3 The SCC should be designed and operated in accordance with land-based regulations.

7.3 Means of communication

7.3.1 The SCC should be linked to the ship, to the Vessel Traffic Services (VTS), to the port authorities or the shipping company by using communication technologies that are available (e.g. GSM, WiMax, VHF or satellite).

7.4 Control and monitoring

7.4.1 The SCC should be able to plan and to upload voyage data to the ship.

7.4.2 The SCC operator should be able to easily identify operational abnormalities, unexpected threats and errors efficiently in a highly automated context and then communicate this situation to other stakeholders in the SCC.

7.4.3 It is recommended to gather essential information on one dashboard for each ship under control.

7.4.4 In addition to have a clear visibility around the ship as requested by SOLAS Ch V reg 22 (Navigation bridge visibility), the dashboard should also include sea chart, radar screen and weather chart.

7.4.5 The dashboard should display an information panel summarizing the essential systems to have a clear view of the situation of the ship (e.g. navigation, machinery, cargo), with for each of them, a coloured flag indicator:

- green for normal situation
- yellow for warning that require operator attention and verification
- red for alert that require operator's immediate corrective actions.

7.5 Manning

7.5.1 The SCC should be manned for uninterrupted supervision during operations of autonomous ships.

A chain of SCCs around the world could alternate in controlling a ship always making sure the center in control have daylight hours, to avoid night shifts with increased risk of accidents.

7.5.2 Manning of shore control centre should include properly qualified personnel such as operators, supervisors, ship engineers and captains.

Personnel should have sufficient sea-going or in service experiences related to an equivalent ship under control. Simulator training should be used for practicing of operators and supervisors.

Taking into account the fatigue due to the large time spent on computer's screen, the proportion between rest and duty periods should be arranged to ensure the efficiency of the watchkeeping.

SECTION 4 GUIDELINES FOR RELIABILITY OF AUTONOMOUS SYSTEMS

1 General

1.1 Scope

1.1.1 This Section provides guidelines for improving the reliability of systems associated with essential services involved in the operations of autonomous ships.

2 General system design

2.1 References

2.1.1 The computerized based system lifecycle should be based on the following international standards:

- ISO/IEC 15288:2015 Systems and Software Engineering - System Lifecycle Processes
- ISO/IEC 12207:2008 Systems and Software Engineering - Software Lifecycle Processes
- ISO/IEC 61508:2010 (all parts) Functional safety of electrical/electronic/programmable electronic safety-related systems.

2.2 Risk-based design

2.2.1 A risk-based design approach (failure analysis) should be adopted to identify, evaluate and mitigate the effects of a system failure. The methodology should be based on a Failure Mode Effects and Criticality Analysis (FMECA).

2.2.2 The boundaries of the system should be clearly identified with all critical components that may affect the safety of operations.

2.3 Component failure

2.3.1 The system should be designed in such a way that a failure of one component should not affect the functionality of other components except for those functions directly dependent upon the information from the defective component.

2.3.2 System and software should be fault tolerant and providing an acceptable level of resilience against unexpected failure.

2.3.3 This resiliency should be achieved by using an appropriate redundancy on the system's critical components (e.g. power supply, communication equipment).

2.4 Network failure

2.4.1 When the systems are interconnected through a network, failure of the network should not prevent individual system from performing its functions.

2.5 Power failure

2.5.1 The system should be arranged with an automatic change-over to a continuously available stand-by power supply in case of loss of normal power source.

2.5.2 The capacity of the stand-by power supply should be sufficient to allow the normal operation of the system for at least half an hour.

3 Human machine interface

3.1 References

3.1.1 The ergonomics, the layout and interfaces of the system should be based on the following international standards:

- ISO 9241-210:2010 Ergonomics of human-system interaction - Part 210: Human-centred design for interactive systems
- ISO 8468:2007 Ships and marine technology - Ship's bridge layout and associated equipment - Requirements and guidelines
- ISO 2412:1982 Shipbuilding - Colours of indicator lights
- IMO A.1021(26) Code on alerts and indicators.

3.2 Design

3.2.1 The human machine interface should be designed to be easily understood in a consistent style. Particular consideration should be given to:

- symbols
- colours
- controls
- information priorities
- layout.

3.2.2 System's controls and indicators should be designed with due regard to the human operator. Controls and indicators are to be so constructed that they can be efficiently operated by suitably qualified personnel.

3.3 Information display

3.3.1 Continuously displayed information should be reduced to the minimum necessary for safe operation. Supplementary information should be readily accessible.

3.3.2 Operational information should be presented in a readily understandable format without the need to transpose, compute or translate.

3.3.3 Displays and indicators should present the simplest information consistent with their function.

3.3.4 All information required by the user to perform an operation should be available on the current display.

3.3.5 The human machine interface should use marine terminology.

3.4 Controls and indicators

3.4.1 The number of operational controls, their design manner of function, location, arrangement and size should be provided for a simple, quick and effective operation.

3.4.2 All operational controls should permit normal adjustments to be easily performed and should be arranged in a manner which minimises the possibility of inadvertent operation. Controls not required for normal operation should not be readily accessible.

3.4.3 Feedback timing should be consistent with the task requirements. There should be clear feedback from any action within a short time. When a perceptible delay in response occurs taking into consideration the communication latency, visible indication should be provided.

3.4.4 Warning and alarm indicators should be designed to show no light in normal position that is an indication of a safe situation. Colour coding of functions and signals should be in accordance with international standards.

3.4.5 Indications, which may be accompanied by a short low intensity acoustic signal, should occur on the user display when an attempt is made to execute an invalid function or use an invalid information.

3.4.6 In case of an input error, the system is to require the operator to correct the error immediately.

3.4.7 The system should indicate default values when applicable.

3.5 User training

3.5.1 Training should be provided to the personnel and should be carried using suitable material and methods to cover the following topics:

- general understanding and operation of the system
- mastering of uncommon conditions in the system.

4 Network and communication

4.1 References

4.1.1 The network components and communication equipment should be designed in accordance with the following standards:

- IEC 61162:(all parts) Maritime navigation and radiocommunication equipment and systems - Digital interfaces
- IMO MSC.252(83) Performance Standards for Integrated Navigation Systems (INS).

4.2 Design

4.2.1 Permanent and reversible communication system between ship and shore should be available. The network should be designed to enable a permanent collection of data aboard and its availability for subsequent transmission.

4.2.2 The network components and communication equipment should be type approved products.

4.2.3 Transmission protocol should be in accordance with a recognised international standard. Satellite communication provider should be recognized by International Maritime Satellite Organisation (IMSO).

4.2.4 The network should have the capacity to transmit the required amount of data with a margin for overload without compromising the data integrity.

4.2.5 Wireless data communication should employ recognised international wireless communication system that incorporate the following features:

a) message integrity:

   fault prevention, detection, diagnosis, and correction so that the received message is not corrupted or altered when compared to the transmitted message

b) configuration and device authentication:

   shall only permit connection of devices that are included in the system design

c) message encryption:

   protection of the confidentiality and or criticality the data content

d) security management:

   protection of network assets, prevention of unauthorised access to network assets.

4.2.6 The network is to be self-checking, detecting failures on the link itself and data communication failures on nodes connected to the link. Detected failures are to initiate an alarm.

4.2.7 The network devices should be automatically started when power is turned on, or restarted after loss of power.

4.3 Performance

4.3.1 A means of transmission control should be provided and designed so as to verify the completion of the data transmitted (CRC or equivalent acceptable method). When corrupted data is detected, the number of retries should be limited so as to keep an acceptable global response time.

4.3.2 All data should be identified with a priority level. The transmission software should be designed so as to take into consideration the priority of data.

4.3.3 Missing or corrupted data transmitted through the network should not affect functions which are not dependent on this data.

4.3.4 When a hardware or software transmission failure occurs, it should be detected by the transmitter and the recipient which should activate an alarm.

4.3.5 A means should be provided to verify the activity of transmission and its proper function (positive information).

4.4 Redundancy

4.4.1 Except if the availability of the connection can be demonstrated in the event of a failure, all transmission equipment should be duplicated or have a secondary means which is capable of the same transmission capacity, with an automatic commutation from one to the other.

4.4.2 Functions that are required to operate continuously to provide essential services dependent on wireless data communication links should have an alternative means of control that can be brought in action within an acceptable period of time.

5 Software quality assurance

5.1 References

5.1.1 The software quality assurance should be based on the following international standards or industry guidelines:

- IMO MSC.1-CIRC.1512 Guidelines on Software Quality Assurance and Human-Centred Design for E-Navigation
- ISO 10007:2003 Quality management systems - Guidelines for Configuration Management
- ISO/IEC 90003:2014 Software engineering - Guidelines for the application of ISO 9001:2008 to computer software
- Bureau Veritas BV SW100 - Software development and assessment guidelines.

5.1.2 The software quality assurance is to comply with the requirements of NR467 Pt C, Ch 3, Sec 3.

5.2 Quality plan

5.2.1 The software development should be carried out according to a quality plan defined by the software provider and records are to be kept.

5.2.2 The quality plan should include the test procedure for software and the results of tests should be documented.

5.3 Testing

5.3.1 Software should be tested in association with hardware and evidences of testing should be produced according to the quality plan.

5.3.2 The software modules of the application software should be tested individually and subsequently subjected to an integration test. It should be checked that:

- the development work has been carried out in accordance with the quality plan
- the documentation includes the method of testing, the test programs producing, the simulation, the acceptance criteria and the results.

5.3.3 Software module tests should provide evidence that each module performs its intended function and does not perform unintended functions.

5.3.4 The behaviour of a machine-learning system is dependent on the training set used during the learning phase of the system. It is recommended to use an extensive training set in order to cover a maximum number of potential situations.

The consistency of the behaviour of a machine-learning system should be tested (repeatability). In particular to be sure that after a long period, the behaviour of the system is not modified and is always responding in the same way.

When testing a machine-learning system, the test data should include some exceptional conditions, in order to validate the behaviour of the system and to detect any deviation from the expected behaviour.

5.3.5 System or subsystem testing should verify that modules interact correctly to perform the functions in accordance with specified requirements and do not perform unintended functions.

5.3.6 Repetition tests should be required to verify the consistency of test results.

5.3.7 Faults should be simulated as realistically as possible to demonstrate appropriate software fault detection and software response.

5.4 Configuration management

5.4.1 A software maintenance should be in place to manage failure due to software change and in case of wrong interaction with existing software from other systems.

5.4.2 Software change should be the responsibility of qualified and authorised member (e.g. chief engineer).

6 Data quality assurance

6.1 References

6.1.1 The data quality assurance should be based on the following international standards:

- ISO 8000: Data quality
- ISO/IEC 10181: Information technology - Open Systems Interconnection - Security frameworks for open systems.

6.2 Data quality assessment

6.2.1 The data quality assessment should be carried on the following measurements:

- completeness:
  all necessary data are recorded
- uniqueness:
  no data will be recorded more than once
- timeliness:
  the degree to which data represent reality from the required point in time
- validity:
  data are valid if it conforms to the syntax (format, type, range) of its definition
- accuracy:
  the degree to which data correctly describes the «real world» object or event being described
- consistency:
  the absence of difference, when comparing two or more representations of a data item against its definition. It is possible to have consistency without validity or accuracy.

6.3 Data acquisition

6.3.1 For the data acquisition, the location and the selection of the sensors should be done so as to measure the actual value of the parameters. Temperature, vibration and electromagnetic interference levels should be taken into account. The sensors should be designed to withstand the local environment.

6.3.2 Means should be provided for testing, calibration and replacement of sensors. Such means should be designed, as far as practicable, so as to avoid perturbation of the normal operation of the system.

6.3.3 Low level signal sensors should be avoided. When installed they should be located as close as possible to amplifiers, so as to avoid external influences.

6.4 Data storage

6.4.1 The data storage should be suitable for the amount of collected data. In case of overcapacity, a mechanism should be provided to remove unnecessary or obsolete data and to recover to a normal situation.

6.4.2 When the data storage is based on a network or distributed system (e.g. storage in the cloud), consequences of the outage of the provider should be considered.

6.4.3 The data storage should have a backup feature (e.g. automatic duplication) and should be fault-tolerant (e.g. due to power failure).

6.5 Data authentication

6.5.1 The authentication of data should be possible each time it is requested by the system, by using a mechanism such as a digital signature or a secure protocol.

6.6 Data integrity

6.6.1 Data integrity (unaltered data) should be preserved by providing means of protection from unauthorised access, the data should carry an internal data checksum against deliberate or unintentional modifications.

6.7 Data confidentiality

6.7.1 Data confidentiality should be maintained by using means of encryption and an adequate level of authorisation for access in consultation of the data storage.

7 Cybersecurity

7.1 References

7.1.1 The cybersecurity should be managed by using the following international standards or industry guidelines:

- ISO/IEC 15408:2009 Information technology -Security techniques - Evaluation criteria for IT security
- ISO/IEC 27001:2013 Information technology -Security techniques - Information Security Management Systems
- IMO MSC.CIRC.1526 Interim Guidelines on Maritime Cyber Risk Management
- National Institute of Standards and Technology (NIST) Framework for Cybersecurity (2014)
- ANSSI Best Practices for CyberSecurity On-board Ships
- Bureau Veritas - BV SW 200 - Cybersecurity Guidelines for Software Development & Assessment.

In addition, the requirements for the cybersecurity from the additional class notation **SYS-COM** (see NR467, Pt F, Ch 4, Sec 3) should be considered.

7.2 Cyber protection

7.2.1 The following functions should be in place to organize the cyber protection:

- identify:
  define personnel roles and responsibilities for cyber risk management and identify the systems, assets, data and capabilities that, when disrupted, pose risks to ship operations,
- protect:
  implement risk control processes and measures, and contingency planning to protect against a cyberevent and ensure continuity of shipping operations,

- detect:

  develop and implement activities necessary to detect a cyber event in a timely manner,

- respond:

  develop and implement activities and plans to provide resilience and to restore systems necessary for shipping operations or services impaired due to a cyberevent,

- recover:

  identify measures to back-up and restore cyber systems necessary for shipping operations impacted by a cyber-event.

7.3 Identification

7.3.1 An accurate map of the IT installations should be established and should be regularly updated.

7.3.2 This map should describe the network architecture and include a list of equipment (identified by a model number) and software (identified by a version number).

7.3.3 An inventory of all users accounts with the associated privileges should reflect the actual level of authorization given to each user.

7.4 Protection

7.4.1 User access management should be based on a secure authentication protocol including best practises such as avoidance of generic or anonymous accounts, a regular password change with a required high level of complexity.

7.4.2 Procedures for arrival and departure of users (management of accounts, access to SCC or sensitive documentation) should be created and followed.

7.4.3 Software updates should be performed regularly following an update policy. This policy should include:

- the list of components (machine and software) to be updated
- the responsibilities of the various actors in the updating process
- the means used to obtain and assess updates
- a verification of the updates prior to the installation
- a procedure to recover previous configuration in case of update failure.

7.4.4 In case of an automatic download and installation from internet or e-mail, the software patches should be retrieved from trusted sources (preferably from genuine software provider).

7.4.5 The network and especially wireless network should be protected by using secure protocols such as encrypted transmissions.

7.4.6 The internet connection should be secured by a gateway enabling compartmentalisation between internet access and the internal network.

7.5 Detection

7.5.1 Monitoring should be in place to detect abnormal events or intrusion such as massive data transfers (depending on usual operating modes), several log-in failures to an active or inactive account.

7.6 Response and recovery

7.6.1 In the event of an incident, a contingency plan should be defined for working in downgraded mode. The first measure should be to isolate all infected machines from the network. For each incident, a feedback should be capitalised in order to be more effective in dealing with a similar event in the future.

7.6.2 Essential information and software backup facilities should be available for recovering to a clean system.