

Guidelines for Autonomous Shipping

October 2019

Guidance Note NI 641 DT R01 E

Marine & Offshore 8 Cours du Triangle - CS 50101 92937 Paris La Defense Cedex - France Tel: + 33 (0)1 55 24 70 00 https://marine-offshore.bureauveritas.com/bv-rules © 2019 Bureau Veritas – All rights reserved



GENERAL CONDITIONS

INDEPENDENCE OF THE SOCIETY AND APPLICABLE TERMS

1.1 The Society shall remain at all times an independent contractor and neither the Society nor any of its officers, employees, servants, agents or subcontractors shall be or act as an employee, servant or agent of any other party hereto in the performance of the Services.

The operations of the Society in providing its Services are exclusively conducted by way of random inspections 1.2 and do not, in any circumstances, involve monitoring or exhaustive verification.

1.3 The Society acts as a services provider. This cannot be construed as an obligation bearing on the Society to obtain a result or as a warranty. The Society is not and may not be considered as an underwriter, broker in Unit's sale or chartering, expert in Unit's valuation, consulting engineer, controller, naval architect, designer, manufacturer, shipbuilder, repair or conversion vard, 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.

The Society only is qualified to apply and interpret its Rules 1.4

The Client acknowledges the latest versions of the Conditions and of the applicable Rules applying to the 1.5 Services' performance.

1.6 Unless an express written agreement is made between the Parties on the applicable Rules, the applicable Rules shall be the Rules applicable at the time of entering into the relevant contract for the performance of the Services

1.7 The Services' performance is solely based on the Conditions. No other terms shall apply whether express or implied.

2 DEFINITIONS

"Certificate(s)" means classification or statutory certificates, attestations and reports following the Society's 2.1 intervention

"Certification" means the activity of certification in application of national and international regulations or 2.2 standards, in particular by delegation from different governments that can result in the issuance of a Certificate.

"Classification" means the classification of a Unit that can result or not in the issuance of a classification 2.3 Certificate with reference to the Rules. Classification is 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.

2.4 "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.

"Industry Practice" means international maritime and/or offshore industry practices. 2.6

"Intellectual Property" means all patents, rights to inventions, utility models, copyright and related rights, 2.7 trade marks, logos, service marks, trade dress, business and domain names, rights in trade dress or get-up, rights in goodwill or to sue for passing off, unfair competition rights, rights in designs, rights in computer software, database rights, topography rights, moral rights, rights in confidential information (including know-how and trade secrets), methods and protocols for Services, and any other intellectual property rights, in each case whether capable of registration, registered or unregistered and including all applications for and renewals, reversions or extensions of such rights, and all similar or equivalent rights or forms of protection in any part of the world.

"Parties" means the Society and Client together. 2.8

"Party" means the Society or the Client. 2.9

2.10 "Register" means the public electronic register of ships updated regularly by the Society.

2.11 "Rules" means the Society's classification rules and other documents. The Society's Rules take into account at the date of their preparation the state of currently available and proven technical minimum requirements but are not a standard or a code of construction neither a guide for maintenance, a safety handbook or a guide of professional practices, all of which are assumed to be known in detail and carefully followed at all times by the Client. 2.12 "Services" means the services set out in clauses 2.2 and 2.3 but also other services related to Classification

and Certification such as, but not limited to: ship and company safety management certification, ship and port security certification, maritime labour certification, training activities, all activities and duties incidental thereto such as documentation on any supporting means, software, instrumentation, measurements, tests and trials on board. The Services are carried out by the Society according to the applicable referential and to the Bureau Veritas' Code of Ethics. The Society shall perform the Services according to the applicable national and international standards and Industry Practice and always on the assumption that the Client is aware of such standards and Industry Practice.

"Society" means the classification society 'Bureau Veritas Marine & Offshore SAS', a company organized 2.13 and existing under the laws of France, registered in Nanterre under number 821 131 844, or any other legal entity of Bureau Veritas Group as may be specified in the relevant contract, and whose main activities are Classification and Certification of ships or offshore units.

2.14 "Unit" means any ship or vessel or offshore unit or structure of any type or part of it or system whether linked to shore, river bed or sea bed or not, whether operated or located at sea or in inland waters or partly on land, including submarines, hovercrafts, drilling rigs, offshore installations of any type and of any purpose, their related and ancillary equipment, subsea or not, such as well head and pipelines, mooring legs and mooring points or otherwise as decided by the Society.

3. SCOPE AND PERFORMANCE

Subject to the Services requested and always by reference to the Rules, the Society shall: 31

review the construction arrangements of the Unit as shown on the documents provided by the Client;

conduct the Unit surveys at the place of the Unit construction;

class the Unit and enter the Unit's class in the Society's Register;

survey the Unit periodically in service to note whether the requirements for the maintenance of class are met. The Client shall inform the Society without delay of any circumstances which may cause any changes on the conducted surveys or Services.

The Society will not: 3.2

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.

RESERVATION CLAUSE 4.

The Client shall always: (i) maintain the Unit in good condition after surveys; (ii) present the Unit for surveys; 4.1 and (iii) inform the Society in due time of any circumstances that may affect the given appraisement of the Unit or cause to modify the scope of the Services.

Certificates are only valid if issued by the Society. 4.2

The Society has entire control over the Certificates issued and may at any time withdraw a Certificate at its 4.3 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.

The Society may at times and at its sole discretion give an opinion on a design or any technical element that would 'in principle' be acceptable to the Society. This opinion shall not presume on the final issuance of any Certificate or on its content in the event of the actual issuance of a Certificate. This opinion shall only be an appraisal made by the Society which shall not be held liable for it.

ACCESS AND SAFETY 5.

The Client shall give to the Society all access and information necessary for the efficient performance of the requested Services. The Client shall be the sole responsible for the conditions of presentation of the Unit for tests, trials and surveys and the conditions under which tests and trials are carried out. Any information, drawing, etc. required for the performance of the Services must be made available in due time.

5.2 The Client shall notify the Society of any relevant safety issue and shall take all necessary safety-related measures to ensure a safe work environment for the Society or any of its officers, employees, servants, agents or subcontractors and shall comply with all applicable safety regulations.

PAYMENT OF INVOICES 6.

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.

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

LIABILITY

7.1 The Society bears no liability for consequential loss. For the purpose of this clause consequential loss shall include, without limitation: Indirect or consequential loss:

Any loss and/or deferral of production, loss of product, loss of use, loss of bargain, loss of revenue, loss of profit or anticipated profit, loss of business and business interruption, in each case whether direct or indirect.

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

7.2 Except in case of wilful misconduct of the Society, death or bodily injury caused by the Society's negligence and any other liability that could not be, by law, limited, the Society's maximum liability towards the Client is limited to one hundred and fifty per-cents (150%) of the price paid by the Client to the Society for the Services having caused the damage. This limit applies to any liability of whatsoever nature and howsoever arising, including fault by the Society, breach of contract, breach of warranty, tort, strict liability, breach of statute,

7.3 All claims shall be presented to the Society in writing within three (3) months of the completion of Services' performance or (if later) the date when the events which are relied on were first discovered by the Client. Any claim not so presented as defined above shall be deemed waived and absolutely time barred

INDEMNITY CLAUSE

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

TERMINATION 9.

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

ā2 In such a case, the Classification granted to the concerned Unit and the previously issued Certificates shall remain valid until the date of effect of the termination notice issued, subject to compliance with clause 4.1 and 6 above.

9.3 In the event where, in the reasonable opinion of the Society, the Client is in breach, or is suspected to be in breach of clause 16 of the Conditions, the Society shall have the right to terminate the Services (and the relevant contracts associated) with immediate effect.

10. FORCE MAJEURE

10.1 Neither Party shall be responsible or liable for any failure to fulfil any term or provision of the Conditions if and to the extent that fulfilment has been delayed or temporarily prevented by a force majeure occurrence without the fault or negligence of the Party affected and which, by the exercise of reasonable diligence, the said Party is unable to provide against.

10.2 For the purpose of this clause, force majeure shall mean any circumstance not being within a Party's reasonable control including, but not limited to: acts of God, natural disasters, epidemics or pandemics, wars, terrorist attacks, riots, sabotages, impositions of sanctions, embargoes, nuclear, chemical or biological contaminations, laws or action taken by a government or public authority, quotas or prohibition, expropriations, destructions of the worksite, explosions, fires, accidents, any labour or trade disputes, strikes or lockouts.

CONFIDENTIALITY

11.1 The documents and data provided to or prepared by the Society in performing the Services, and the information made available to the Society, are treated as confidential except where the information:

is properly and lawfully in the possession of the Society;

is already in possession of the public or has entered the public domain, otherwise than through a breach of this obligation:

is acquired or received independently from a third party that has the right to disseminate such information;

is required to be disclosed under applicable law or by a governmental order, decree, regulation or rule or by a stock exchange authority (provided that the receiving Party shall make all reasonable efforts to give prompt written notice to the disclosing Party prior to such disclosure

11.2 The Parties shall use the confidential information exclusively within the framework of their activity underlying these Conditions.

11.3 Confidential information shall only be provided to third parties with the prior written consent of the other Party. However, such prior consent shall not be required when the Society provides the confidential information to a subsidiary

11.4 Without prejudice to sub-clause 11.1, the Society shall have the right to disclose the confidential information if required to do so under regulations of the International Association of Classifications Societies (IACS) or any statutory obligations.

INTELLECTUAL PROPERTY

12.1 Each Party exclusively owns all rights to its Intellectual Property created before or after the commencement date of the Conditions and whether or not associated with any contract between the Parties.

12.2 The Intellectual Property developed by the Society for the performance of the Services including, but not limited to drawings, calculations, and reports shall remain the exclusive property of the Society

ASSIGNMENT

13.1 The contract resulting from to these Conditions cannot be assigned or transferred by any means by a Party to any third party without the prior written consent of the other Party.

13.2 The Society shall however have the right to assign or transfer by any means the said contract to a subsidiary of the Bureau Veritas Group

SEVERABII ITY 14.

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.

GOVERNING LAW AND DISPUTE RESOLUTION 15.

These Conditions shall be construed and governed by the laws of England and Wales. 15.2 The Parties shall make every effort to settle any dispute amicably and in good faith by way of negotiation within thirty (30) days from the date of receipt by either one of the Parties of a written notice of such a dispute.

15.3 Failing that, the dispute shall finally be settled under the Rules of Arbitration of the Maritime Arbitration Chamber of Paris ("CAMP"), which rules are deemed to be incorporated by reference into this clause. The number of arbitrators shall be three (3). The place of arbitration shall be Paris (France). The Parties agree to keep the arbitration proceedings confidential

16. PROFESSIONAL ETHICS

16.1 Each Party shall conduct all activities in compliance with all laws, statutes, rules, economic and trade sanctions (including but not limited to US sanctions and EU sanctions) and regulations applicable to such Party including but not limited to: child labour, forced labour, collective bargaining, discrimination, abuse, working hours and minimum wages, anti-bribery, anti-corruption, copyright and trademark protection, personal data protection (https://personaldataprotection.bureauveritas.com/privacypolicy).

Each of the Parties warrants that neither it, nor its affiliates, has made or will make. with respect to the matters provided for hereunder, any offer, payment, gift or authorization of the payment of any money directly or indirectly, to or for the use or benefit of any official or employee of the government, political party, official, or candidate. 16.2 In addition, the Client shall act consistently with the Bureau Veritas' Code of Ethics. https://group.bureauveritas.com/group/corporate-social-responsibility



GUIDANCE NOTE NI 641

Guidelines for Autonomous Shipping

SECTION 1GENERALSECTION 2RISK AND TECHNOLOGY ASSESSMENTSECTION 3FUNCTIONALITY OF AUTOMATION SYSTEMSSECTION 4RELIABILITY OF AUTOMATION SYSTEMS

Section 1 General

1	General	7
	 1.1 Context 1.2 Scope 1.3 Applicability 1.4 Wording 1.5 Definitions 1.6 Acronyms 1.7 Navigation notation 1.8 Degrees of automation 1.9 Degrees of control 1.10 Characterisation 1.11 Documents to be submitted 	
2	Safety and security conditions	12
	 2.1 General 2.2 Main ship capabilities 2.3 Operational limitations 2.4 Identification 2.5 Interactions 2.6 Responsibilities 2.7 Remote control 2.8 Direct control 2.9 Reliability 2.10 Human factors 2.11 Cybersecurity 2.12 Cargo 	
3	Rules and Regulations	15
	 3.1 General 3.2 Society Rules 3.3 IMO 3.4 SOLAS convention 3.5 MARPOL convention 3.6 COLREG convention 3.7 ISM code 3.8 ISPS code 3.9 STCW convention 3.10 Maritime Labour Convention (MLC) 3.11 EU Ship Recycling Regulation (EU SRR) 	

Section 2 Risk and Technology Assessment

1	General	18	
	1.1 Purpose and approach		
2	Risk assessment	18	
	 2.1 Methodology 2.2 Ship model 2.3 Hazard identification 2.4 Risk index calculation 2.5 Risk evaluation 		
	2.6 Risk Control Options		

3 Technology assessment

- 3.1 Reference
- 3.2 General

Section 3 Functionality of Automation Systems

1	General	24
	1.1 Scope	
2	Navigation system	24
	 2.1 Goal 2.2 Functional requirements 2.3 References 2.4 Voyage planning 2.5 Navigation 2.6 Docking and undocking 2.7 Lookout 2.8 Weather routing 2.9 Ship status and dynamics 2.10 Voyage recording 2.11 Collision avoidance 2.12 Situational awareness 	
3	Communication network and system	26
	 3.1 Goal 3.2 Functional requirements 3.3 References 3.4 Type of communication system 3.5 Performance 	
4	Machinery system	27
	 4.1 Goal 4.2 Functional requirements 4.3 References 4.4 Monitoring 4.5 Maintenance 4.6 Emergency management 	
5	Cargo management system	28
	 5.1 Goal 5.2 Functional requirements 5.3 References 5.4 Monitoring 5.5 Control 5.6 Loading and unloading 	
6	Passenger management system	28
	 6.1 Goal 6.2 Functional requirements 6.3 References 6.4 Overload prevention 6.5 Life saving 	

22

7	Remote Control Centre	
	 7.1 Goal 7.2 Functional requirements 7.3 References 7.4 Means of communication 7.5 Monitoring and control 7.6 Manning 	
8	Failures or malfunctions	30
	8.1 Fail-safe sequences8.2 Minimum communication link8.3 Degraded modes	

Section 4 Reliability of Automation Systems

1	General	31
	1.1 Scope	
2	General system design	31
	 2.1 References 2.2 Risk-based design 2.3 Component failure 2.4 Network failure 2.5 Power failure 	
3	Human machine interface	31
	 3.1 References 3.2 Design 3.3 Information display 3.4 Controls and indicators 3.5 User training 	
4	Network and communication	32
	 4.1 References 4.2 Design 4.3 Performance 4.4 Redundancy 	
5	Software quality assurance	33
	5.1 References5.2 Quality plan5.3 Testing5.4 Configuration management	
6	Data quality assurance	33
	 6.1 References 6.2 Data quality assessment 6.3 Data acquisition 6.4 Data storage 6.5 Data authentication 6.6 Data integrity 6.7 Data confidentiality 	
7	Cyber security	34

7.1 References

8	Testing	
	0.1	C (1

8.3

SECTION 1

GENERAL

1 General

1.1 Context

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

But while the information and communication technologies enable the automation 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

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 automation in shipping.

1.2.2 The recommendations of this Guidance Note are related to the design and operations of ships equipped with automation systems capable, to varying degrees, of making decisions and performing actions with or without human interaction, and their associated remote control centres if any.

1.2.3 This Guidance Note could be applied to a specific automation system, such as for example a navigating automation system or a remote engine control system, or to a ship as a whole.

1.2.4 This Guidance Note is mainly focused on surface propelled units. This excludes underwater vehicles and non-manoeuvring units, such as drifting buoys used for scientific research.

1.2.5 This Guidance Note provides also recommendations on the statutory requirements deemed applicable for ships covered by this Guidance Note, see in particular [3].

These recommendations are intended as a reference for designers, shipyards, manufacturers, shipowners and Administrations in order to help in the definition of the statutory framework applicable to these ships.

The application of this Guidance Note does not relieve the Interested Party from compliance with any requirements issued by Administrations.

1.3 Applicability

1.3.1 In addition to this first general section, this Guidance Note includes three specific sections:

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

1.3.2 The recommendations of this Guidance Note may be adjusted according to the results of the risk and technology assessment, the degree of automation, the degrees of direct control and remote control, the navigation notation, the national regulations of the Administration, the operational limitations, the possibility of external rescue, etc.

1.3.3 Likewise, the recommendations of this Guidance Note may be adjusted for small units that cannot embark humans on board at any time during operations.

1.3.4 In particular, the applicable requirements related to the assignment of the additional class notations as recommended in Sec 3 and Sec 4, and more generally the requirements of the Rules & Regulations as mentioned in [3], may be adjusted accordingly, to the satisfaction of the Society and the Administration.

1.4 Wording

1.4.1 Following the recommendations on deprecated terms from paragraph 7 of the document SAE J3016 SEP2016 - Surface Vehicle Recommended Practice - Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles, this Guidance Note avoids the use of the term "autonomy" to describe the degrees of automation systems.

1.4.2 Unless otherwise specified, the term "ship" in this Guidance Note refers to a ship equipped with automation systems capable, to varying degrees, of making decisions and performing actions with or without human interaction.

1.4.3 The use of the term "autonomous" should be limited to the highest degree of automation (degree A4, see [1.8]) and avoided for the other degrees of automation.

1.5 Definitions

1.5.1 Terms used in this Guidance Note are defined below:

- Administration: Government of the State whose flag the ship is entitled to fly or the State under whose authority the ship is operating in the specific case
- Automation system: system based on one or more devices whose implementation can be adjusted in advance, including, where appropriate, devices whose behaviour depends on unforeseeable factors. An automation system can be composed of various types of devices: mechanical, electrical, digital, electronic, magnetic, hydraulic or other. An automation system may be used, for example, for control, protection, lookout, recording or monitoring functions.
- Control: controlling a ship consists in operating devices related to its navigation or its operations. Ships may be controlled either by the crew, or remotely by operators, or by automation systems with or without human interaction.
- Control station: single or multiple position including all equipment such as computers and communication terminals and furniture at which control and monitoring functions are conducted (ISO 11064-3).
- Conventional ship: ship where most decisions and actions are performed by the crew aboard. A conventional ship may have automation systems to assist the crew by automatically performing some actions, but those systems are always under the control of human aboard.
- Crew: all persons carried aboard the ship to provide navigation and maintenance of the ship, its machinery, systems and arrangements essential for propulsion and safe navigation or to provide services for other persons aboard (IMO Resolution MSC.266(84)).
- Cybersecurity: preservation of confidentiality, integrity and availability of information in the Cyberspace (ISO/IEC 27032).
- 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).
- Essential service: service necessary for a ship to proceed at sea, be steered or manoeuvred, or undertake activities connected with its operation, and for the safety of life, as far as class is concerned.
- 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).
- Hazard: any source of potential damage or casualty, or any situation with potential to cause it.
- 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).

- 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).
- Navigation: all tasks relevant for deciding, executing and maintaining course and speed in relation to waters and traffic (IACS Unified Requirements N1).
- Monitoring: act of periodically checking equipment and environment in order to detect any changes (ISO 8468)
- Operators: all persons in the remote control centre to provide remotely navigation and maintenance of the ship, its machinery, systems and arrangements essential for propulsion and safe navigation or to provide remotely services for other persons aboard.
- Reliability: property of a system and its parts to perform its mission accurately and without failure or significant degradation (ISO/IEC 27036-3).
- Remote Control: control of an operation at a point distant from the controlled device, using the transmission of information by telecommunications techniques.
- Remote Control Centre: area located onshore or on another ship (conventional ships included) or on an off-shore unit from which the monitoring and control the ship is exercised.
- Remote Control station: control station located in a Remote Control Centre.
- Risk: concept quantifying a hazard, consisting in a combination of probability or frequency and consequence of the related hazard.
- Risk analysis: structured method involving:
 - identification of hazards related to the unit, installation or equipment
 - estimation of hazard probabilities or frequencies
 - estimation of hazard consequences.
- Risk assessment: systematic analysis of risks including risk analysis, review of risk acceptability by comparison with agreed criteria and identification of risk reduction measures, when relevant.
- 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).
- Society: Bureau Veritas Marine & Offshore classification society.
- System: combination of interacting elements organized to achieve one or more stated purposes (ISO/IEC 15288).
- 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., operators instructions), facilities, materials, and naturally occurring entities (e.g., water, organisms, minerals), or any combination (ISO/IEC 15288).

- 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).
- Technical personnel: persons temporarily embarked aboard a ship equipped with automation systems for the purpose of its maintenance or time-limited technical intervention.
- Unmanned ship: ship having no crew to operate ship systems. An unmanned ship may be remotely controlled or supervised by operators or with full automation. It may have passengers, special personnel according to SPS Code MSC.266(84) or temporarily technical personnel aboard an unmanned ship.

1.6 Acronyms

1.6.1 Acronyms used in this Guidance Note are defined below:

AIS : Automatic identification system ALARP : As low as reasonably practicable Degree of automation of a system (x from 0 to Ax 4), see [1.8] CCTV Closed circuit television : COLREG: IMO Convention on the international regulations for preventing collisions at sea CRC : Cyclic redundancy check DCy : Degree of direct control of a system (y from 0 to 3), see [1.9] EU SRR : European ship recycling regulation GAx : Global degree of automation of a ship (x from 0 to 4), see [1.8] GDCy : Global degree of direct control of a ship (y from 0 to 3), see [1.9] GNSS : Global navigation satellite system GPS : Global positioning system Global degree of remote control of a ship (z GRCz : from 0 to 3), see [1.9] IACS International association of classification societies : ILO : International labour organisation International maritime organisation IMO : ISM IMO International safety management code : ISPS : IMO International ship and port facility security code IT Information technology : LIDAR : Light detection and ranging LOS : Line of sight MARPOL: IMO International convention for the prevention of pollution from ships MASS Maritime autonomous surface ship : MLC : ILO Maritime labour convention Navigating automation system NAS : NAVTEX: Navigational telex RCC Remote control centre : RCO : Risk control options

- RCz : Degree of remote control of a system (z from 0 to 3), see [1.9]
- RSE : Regulatory scoping exercise
- SOLAS : IMO International convention for the safety of life at sea
- SMS : Safety management system
- SPS : IMO Special purpose ships code
- STCW : IMO 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.

1.7 Navigation notation

1.7.1 Any ship covered by the present Guidance Note should be assigned a navigation notation or a range of navigation character in accordance with Society classification Rules listed in [3.2.1], as applicable.

Note 1: e.g. ships complying with NR467 Rules for the classification of steel ships are to be assigned one of the navigation notation:

- unrestricted navigation
- summer zone
- tropical zone
- coastal area
- sheltered area

as defined in Society Rules for Steel Ships NR467, Pt A, Ch 1, Sec 2, [5.2].

1.7.2 In specific cases, the designation of the geographical area and/or the most unfavourable sea conditions considered may be added to the navigation notation.

1.7.3 The assigned navigation notation should be taken into account in the risk assessment process as described in Sec 2, including the consideration of potential specific arrangements for restricted navigation notations.

1.7.4 The assignment of a navigation notation does not absolve the Interested Party from compliance with any international and national regulations established by the Administrations for a ship operating in national waters, or a specific area, or a navigation zone.

1.8 Degrees of automation

1.8.1 The degree of automation represents the degree of decision making (authority) deferred from the human to the system.

1.8.2 The degree of automation 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 function:

- a) information acquisition
- b) information analysis

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 degree of automation the impact of a system error will be predominant, whereas for a low degree of automation, the impact of an human error will be predominant.

1.8.3 A degree of automation Ax (x from 0 to 4) should be defined for each automation system.

1.8.4 Several different degrees of automation could be considered for the duration of a single voyage.

1.8.5 Degrees of automation Ax (x from 0 to 4) considered in this Guidance Note are described below and in Tab 1:

- Degree A0 Human operated:
 - The system or ship can perform information acquisition, but cannot analyse information, take decisions and execute operations on behalf of human.
 - Human makes all decisions and controls all functions.Human is located aboard (crew).
- Degree A1 Human directed:
 - The system or ship can perform information acquisition, information analysis and suggest actions but cannot take decisions and execute operations on behalf of human.
 - Human makes decisions and actions.
 - Human can be located aboard (crew) or remotely outside the ship in a remote control centre (operators).
- Degree A2 Human delegated:
 - The system or ship can perform information acquisition, information analysis, take decisions and initiate

actions, but requests human confirmation. System invokes functions waiting for human confirmation.

- Human can reject decisions.
- Human can be located aboard (crew) or remotely outside the ship in a remote control centre (operators).
- Degree A3 Human supervised:
 - The system or ship can perform information acquisition, information analysis, take decisions and execute operations under human supervision. System invokes functions without expecting human confirmation.
 - Human is always informed of the decisions and actions, and can always take control.
 - Human can be located aboard (crew) or remotely outside the ship in a remote control centre (operators).
- Degree A4 Full automation:
 - Self-operating system or ship at defined conditions and in specific circumstances.
 - The system or ship can perform information acquisition & analysis, take decisions and executes operations without the need of human intervention or supervision. System invokes functions without informing the human, except in case of emergency.
 - Human can always take control.
 - The supervision can be done aboard (crew) or remotely, outside the ship from a remote control centre (operators).

1.8.6 A global degree of automation GAx (x from 0 to 4) of a ship should be defined considering the lowest degree of automation of main systems covering essential services (see Sec 2, [2.2.1] and Sec 3).

Table 1 : Degrees of automation

Degree of automation		Manned	Definition	Information Acquisition	Information Analysis	Authority to make decisions	Action initiated by
A0	Human operated	Yes	Automated or manual operations are under human control. Human makes all decisions and controls all functions.	System Human	Human	Human	Human
A1	Human directed	Yes/No	Decision support: system suggests actions. Human makes decisions and actions.	System	System Human	Human	Human
A2	Human delegated	Yes/No	System invokes functions. Human must confirm decisions. Human can reject decisions.	System	System	Human	System
A3	Human supervised	Yes/No	System invokes functions without waiting for human reaction. System is not expecting confirmation. Human is always informed of the decisions and actions.	System	System	System	System
A4	Full automation	Yes/No	System invokes functions without informing the human, except in case of emergency. System is not expecting confirmation. Human is informed only in case of emergency	System	System	System	System

1.9 Degrees of control

1.9.1 The degree of control represents the degree of availability of human operating the ship aboard (crew) or remotely outside the ship from a remote control centre (operators).

1.9.2 A degree of direct control DCy (y from 0 to 3) and remote control RCz (z from 0 to 3) should be defined for each automation system.

1.9.3 Several different degrees of control could be considered for the duration of a single voyage.

1.9.4 Degrees of direct control DCy (y from 0 to 3) and remote control RCz (z from 0 to 3) considered in this Guidance Note are described below and in Tab 2:

Degree DC0 - No direct control

There are no crew to monitor and control the system or ship, nor to take control in case of warning or alert from the system.

• Degree DC1 - Available direct control

The crew is available aboard, ready to take control in case of warning or alert from the system, but they may be not at the control station (e.g. periodically unmanned bridge).

• Degree DC2 - Discontinuous direct control

The system or ship is monitored and controlled by the crew from the control station aboard (bridge or engine control room). But monitoring and control may be discontinuous during a short period. The crew is always available at the control station aboard, ready to take control in case of warning or alert from the system. • Degree DC3 - Full direct control

The system or ship is actively monitored and controlled at any time by the crew from the control station aboard (bridge or engine control room).

• Degree RC0 - No remote control

There are no operator in a remote control centre outside the ship to monitor and control the system or ship, nor to take control in case of warning or alert from the system.

• Degree RC1 - Available remote control

Operators are available in a remote control centre outside the ship, ready to take control in case of warning or alert from the system, but they may be not at the control station (e.g. periodically unmanned remote control station).

• Degree RC2 - Discontinuous remote control

The system or ship is monitored and controlled by operators from a remote control station outside the ship. But monitoring and control may be discontinuous during a short period. Operators are always available at the remote control station, ready to take control in case of warning or alert from the system.

• Degree RC3 - Full remote control

The system or ship is actively monitored and controlled at any time by operators from a remote control station outside the ship.

1.9.5 A global degree of direct control GDCy (y from 0 to 3) and remote control GRCz (z from 0 to 3) of a ship should be defined according to the lowest degrees of direct control and remote control of main functions covering essential services (see Sec 2, [2.2.1] and Sec 3).

Degree of control		e of control	Human presence	Location of control station	
Direct control	DC0	No direct control No crew available to monitor and control the system, nor to take control in case of warning or alert.		(1)	
	DC1	Available direct control	Crew available aboard, ready to take control in case of warning or alert But they may be not at the control station		
	DC2	2Discontinuous direct controlMonitoring and control may be discontinuous during a short period Crew always available at the control station, ready to take control		Aboard	
	DC3	Full direct control	System is actively monitored and controlled at any time	Aboard	
	RC0	No remote control	No operator available to monitor and control remotely the system, nor to take control in case of warning or alert.	(1)	
Remote control	RC1	Available remote control	Operators available in the RCC, ready to take control in case of warning or alert But they may be not at the remote control station	RCC	
	RC2	Discontinuous remote control	Remote monitoring and control may be discontinuous during a short period Operators always available at the remote control station, ready to take control	RCC	
	RC3	Full remote control	System is actively monitored and controlled remotely at any time	RCC	
(1) See also [2.8.3]: there may not be any integrated control station					

Table 2 : Degrees of control

1.10 Characterisation

1.10.1 Any system covered by the present Guidance Note should be characterised by:

• a degree of automation Ax

(x from 0 to 4), see [1.8]

• a degree of direct control DCy

(y from 0 to 3), see [1.9]

• a degree of remote control RCz

(z from 0 to 3), see [1.9]

1.10.2 For example, a "human supervised" Navigating Automation System (see [1.8.5]) with available direct control and no remote control (see [1.9.4]) would be characterized by the following terminology:

A3 DC1 RC0

1.10.3 Any ship covered by the present Guidance Note should be characterised by:

• a global degree of automation GAx

(x from 0 to 4), see [1.8]

- a global degree of direct control GDCy
- (y from 0 to 3), see [1.9]
- a global degree of remote control GRCz
 - (z from 0 to 3), see [1.9]
- a navigation notation, see [1.7]

1.10.4 For example, a "human delegated" unmanned ship (see [1.8.5]) with no direct control and discontinuous remote control (see [1.9.4]) and intended to operate in any area and any period of the year would be characterized by the following terminology:

GA2 GDC0 GRC2 unrestricted navigation

1.11 Documents to be submitted

1.11.1 At the request of the designer, shipyard, manufacturer and/or owner, the Society may review the design of a ship according to the content of this Guidance Note.

1.11.2 For this purpose, the documents that should be submitted in the scope of this review are listed in Tab 3.

2 Safety and security conditions

2.1 General

2.1.1 Any ship covered by this Guidance Note should provide at least the same degree of safety, security and protection of the environment as provided by a conventional ship having the same purpose or design.

2.1.2 To achieve this minimum degree of safety, security and protection of the environment, the general principles behind the recommendations contained in this Guidance Note are given in [2.2] to [2.12].

2.1.3 During operations, a ship should not be a source of danger to itself, to the other ships around (conventional ships included), to the maritime infrastructures and to the marine environment.

2.1.4 New threats may arise from the reduction or absence of crew and from the use of remote control.

2.1.5 The risk management is transferred from the crew to sensors and software, and to operators in the remote control centre if any.

2.2 Main ship capabilities

2.2.1 Guidelines for ensuring a suitable level of functionality of systems associated with essential services of a ship are provided in Sec 3.

2.2.2 In particular, any ship covered by this Guidance Note should be capable of:

- managing a predefined 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
- complying with all relevant international and local regulations

2.2.3 The possibility for the crew or remote operators to regain control of a ship in case of emergency or system failure should always be possible.

2.2.4 The possibility to activate an automation system or regain control should be granted to authorized and qualified personnels only (crew or operators). Specific attention should be paid in particular aboard ships carrying passengers.

2.2.5 When a ship is operated remotely, the crew should always be able to regain control of the ship in priority to the remote operator.

2.3 Operational limitations

2.3.1 The operational limitations of a ship are parameters to which the crew or operators must refer for the monitoring and control of the ship.

2.3.2 It is the designer, shipyard, manufacturer and/or shipowner responsibility to specify these limitations in order to define the conditions under which the ship is to be operated.

Table 3 : Documents to be submitted

Торіс	Plans and documents to be submitted		
Classification	Plans and documents to be submitted according to Society Rules in the scope of the classification of the ship and relevant to the service notation applied for		
Additional class notations	Plans and documents to be submitted according to Society Rules in the scope of the additional class nota- tions as specified in this Guidance Note, see Sec 3, [2.3.1], Sec 3, [4.3.1], Sec 3, [5.3.1] and Sec 4, [7.1.1]		
Operational limitations	Details of parameters to which the crew or operators must refer for the control of the ship, see [2.3]		
Identification	Details of provisions for identification, see [2.4]		
Interactions	Details of provisions for interactions, see [2.5]		
Automation systems	 Detailed specification of all automation systems, including: Specification of the Navigation system, see Sec 3, [2] Specification of the Communication network and system, see Sec 3, [3] Specification of the Machinery system, see Sec 3, [4] Specification of the Cargo management system, see Sec 3, [5] Specification of the Passenger management system, see Sec 3, [6] Specification of the Remote Control Centre, see Sec 3, [7] These specifications should clearly specify for each function the distribution of roles and responsibilities between the human and the system, see [2.6] and [1.8.2] 		
Risk assessment	Detailed risk assessment report including:		
	 Groups of functions considered, see Sec 2, [2.2] List of hazards considered, see Sec 2, [2.3] Risk analysis outcome, see Sec 2, [2.4] Risk Control Options considered, see Sec 2, [2.6] 		
Technology assessment	Detailed technology assessment report, if applicable, see Sec 2, [3]		
Reliability	 Details of provisions for improving the reliability of systems including: General system design, see Sec 4, [2] Human machine interface, see Sec 4, [3] Network and communication, see Sec 4, [4] Software quality assurance, see Sec 4, [5] Data quality assurance, see Sec 4, [6] Cybersecurity, see Sec 4, [7] 		
Testing	 Detailed tests specifications and reports, including: Software tests, see Sec 4, [8.1] Simulation tests, see Sec 4, [8.2] Full scale tests, see Sec 4, [8.3] All tests reports should include the targeted objective, the followed procedure, the expected results and the outcome achieved 		

2.3.3 The operational limitations should at least refer to the following parameters:

- degree of automation
- degree of control
- navigation notation
- Administration's national regulations, if any
- local legislation, if any
- traffic conditions, if any
- deadweight and assigned freeboard
- minimum ballast draught
- maximum service speed
- design loads on decks, hatch covers and double bottom
- density of cargoes
- situational awareness system characteristics
- navigation system characteristics
- communication system characteristics
- machinery system characteristics

- cargo management system characteristics
- passenger management system characteristics
- distributions of roles and responsibilities.

2.4 Identification

2.4.1 The identification of a ship should be based on the following standards and regulations:

- IMO A.1117(30) IMO Ship Identification Number Scheme
- ISO 10087 Small craft Craft identification Coding system.
- Administration's national regulations, if any
- Local legislation, if any

2.4.2 Any ship covered by this Guidance Note should be marked by explicit distinguishing marks in order to be easily identified, in particular for ships with high degrees of automation (e.g. degree A3 or A4).

The size of the marking must be adapted to the size of the ship so that it can be easily read by an external observer.

For the same purpose, these ships should be painted with light colours (e.g. yellow or orange), in order to be as visible as possible from afar on the sea and recognizable by other ships (conventional ships included) operating in their vicinity.

2.4.3 Any ship should be equipped with an Automatic Identification System (AIS), encoded as far as possible according to the local regulations of the waters in which they are intended to operate.

For example, according to the U.S. Coast Guard Navigation Center (NAVCEN) Guidance Note "Automatic Identification System Encoding Guide" v.2012-01-12, code 29 should be used for AIS ship type to represent autonomous or remotelyoperated ships when operating in U.S. waters.

It is recommended to use this AIS ship type code 29 by default in the absence of any contrary regulation.

2.5 Interactions

2.5.1 Interactions with other ships (conventional ships included) should be taken into consideration during the design and the operation.

2.5.2 Any ship covered by this Guidance Note should not interfere with other ships (conventional ships included) operating in their vicinity.

2.5.3 Any ship covered by this Guidance Note should be able to respond at any usual request (e.g. identification, position) from other ships (conventional ships included) by means of radio communications or visual signals

2.5.4 Port and coastal authorities should be able to communicate with any ship covered by this Guidance Note in order to be informed about the voyage plan and to be able to regulate the traffic.

Specific communication protocol should be established if necessary.

2.5.5 Specific attention should be paid to the protection of third parties who could be confronted with any ship covered by this Guidance Note in the event of grounding or collision, in particular in the case of an unmanned ship.

For example, it is recommended to protect all moving parts and to provide automatic power breakers.

An appropriate marking indicating the level of danger incurred in the event of attempted disassembly (degassing, overpressure, electrical voltage, etc.) and the contact details of the operators is also recommended.

2.6 Responsibilities

2.6.1 There should be a responsible party defined at all times and in all circumstances for all operations of any ship covered by this Guidance Note, even if that person is not aboard.

2.6.2 The following distributions of roles and responsibilities should be clearly defined and described in the operational limitations:

- aboard, between automation systems and the crew
- at the remote control center, between automation systems and remote operators
- between the crew and remote operators.

2.7 Remote control

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

2.7.2 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 RCC is located.

2.7.3 The RCC, including facility and manning, should be designed with regard to each ship it supervises. When the RCC is used for an additional ship, this design should be reassessed and potentially upgraded accordingly.

2.7.4 When a ship operates in sensitive or restricted area (e.g. military fleet), and depending on its degree of automation, it could be necessary to have more stringent measures for the protection of the RCC (e.g. to avoid terrorist attack).

2.7.5 Before taking control of a ship from the RCC, remote operators should first ensure that they have an accurate situational awareness and that all devices to control the ship remotely are available and operational.

2.7.6 Refer also to Sec 3, [7] providing guidelines for ensuring a suitable level of functionality for RCC.

2.8 Direct control

2.8.1 All operations for which a ship has to be directly controlled or may be remotely operated should be clearly defined within the operational limitations, according to the results of the risk and technology assessment, the degree of automation, the degrees of direct control and remote control, the navigation notation, and depending on local regulations and traffic.

2.8.2 Regardless of the possibility of a remote control, a ship should be designed to authorize a human to come aboard or in their vicinity for controlling the ship, for example when a critical situation arises (e.g. fire, flooding, loss of propulsion).

2.8.3 Any ship covered by this Guidance Note should be designed to be controlled aboard by an integrated control station, or at least by a portable device (e.g. laptop) for small units.

2.8.4 For sea trials, surveys in service, flag or port state control inspections and technical personnel intervention, any ship should be designed to accept the presence of a human aboard (or at least in their vicinity for small units).

2.8.5 Due to size or design, a ship may not have the capacity to carry a human aboard and may only be controlled remotely or by automation systems.

In this case, the recommendations of this Guidance Note may be adjusted: for example, the provisions relating to the life-saving appliances (e.g. presence of lifejackets or lifeboats) may be simplified.

These specific arrangements should be considered on a case-by-case basis by the Society and approved by the Administration.

2.9 Reliability

2.9.1 Compared to a conventional ship, a ship covered by this Guidance Note may have less or even no crew to rely on for maintenance operations and corrective tasks due to system failure. Consequently, the systems should be designed to be as resilient as possible to failure (e.g. fault tolerant) and to have extended maintenance intervals (see Sec 4).

2.9.2 Highest reliability should be achieved by introducing for example 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).

2.9.3 The usage of intensive remote monitoring and control of the status of equipments should be considered in order to prevent failures.

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

2.9.5 Redundancy is easiest to achieve 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.

2.10 Human factors

2.10.1 The multiple sensors used for monitoring and control increase a lot the amount of information provided to crew and operators. 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 crew and operators.

2.10.2 The ergonomics of monitoring and control 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.

2.10.3 The remote operators 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.

2.11 Cybersecurity

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

2.11.2 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).

2.11.3 For cybersecurity reference is made to Sec 4, [7].

2.12 Cargo

2.12.1 Cargo on any ship covered by this Guidance Note should be carefully loaded, stowed and monitored at all times and for all operations.

2.12.2 The stowage of cargo aboard should be ensured at port, since the ship could have few means (less or no crew and equipment) for ensuring a proper cargo securing at sea.

2.12.3 For cargo management system reference is made to Sec 3, [5].

3 Rules and Regulations

3.1 General

3.1.1 Any ship covered by this Guidance Note should be compliant with Society Rules as defined in [3.2.1] and all relevant regulations from applicable international conventions, Administration's national regulations or local legislation if any.

3.1.2 Where appropriate, exemptions or equivalent solutions should be explicitly approved by the Administration.

3.2 Society Rules

3.2.1 The following classification Rules should be applied as far as practicable, depending on the type and the service of the ship:

- NR467 : Rules for the classification of steel ships
- NR216 : Rules on materials and welding for the classification of marine units
- NR600 : Hull structure and arrangement for the classification of cargo ships less than 65 m and non cargo ships less than 90 m
- NR566 : Hull arrangement, stability and systems for ships less than 500 GT
- NR483 : Rules for the classification of naval ships

- NR500 : Rules for the classification and the certification of yachts
- NR217 : Rules for the classification of inland navigation vessels
- NR659 : Rules on cyber security for the classification of marine units.

3.3 IMO

3.3.1 Regulatory Scoping Exercise

The IMO Maritime Safety Committee 98 (06/2017) agreed to include in its 2018-2019 biennial agenda an output on a "Regulatory Scoping Exercise" (RSE) for the use of "Maritime Autonomous Surface Ships" (MASS), with a target completion year of 2020.

The objective of the RSE on MASS is to assess the degree to which the existing regulatory framework under its purview may be affected in order to address MASS operations.

The RSE is conducted as an exploratory research with focus on the identification of relevant instruments and regulations that are related to MASS and, in particular, those which may have an impact on, or may limit the introduction of MASS.

It is not intended as a regulatory drafting exercise, which should follow at the next stage.

3.3.2 Preliminary definitions

For the purpose of this Regulatory Scoping Exercise and only for that, the following preliminary definition of MASS and degrees of autonomy are considered:

• Maritime Autonomous Surface Ship (MASS):

Ship which, to a varying degree, can operate independent of human interaction.

• IMO MASS Degree 1:

Ship with automated processes and decision support.

Seafarers are on board to operate and control shipboard systems and functions. Some operations may be automated and at times be unsupervised but with seafarers on board ready to take control.

• IMO MASS Degree 2:

Remotely controlled ship with seafarers on board.

The ship is controlled and operated from another location. Seafarers are available on board to take control and to operate the shipboard systems and functions.

• IMO MASS Degree 3:

Remotely controlled ship without seafarers on board.

The ship is controlled and operated from another location. There are no seafarers on board.

IMO MASS Degree 4:

Fully autonomous ship.

The operating system of the ship is able to make decisions and determine actions by itself.

3.3.3 Interim Guidelines for MASS trials

The IMO Maritime Safety Committee 101 (06/2019) approved the "Interim Guidelines for MASS trials" MSC.1/Circ.1604, with the aim of assisting relevant authori-

ties and relevant stakeholders with ensuring that the trials of Maritime Autonomous Surface Ships (MASS) related systems and infrastructure are conducted safely, securely, and with due regard for protection of the environment.

3.4 SOLAS convention

3.4.1 In addition to [3.1], the following regulations from Chapter V (Safety of navigation) as amended should be given special attention and should be applied as far as practicable:

- 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.

3.4.2 With regard to the obligation of assistance (Reg. 33), any ship covered by this Guidance Note should be able to provide assistance at least as effective as a conventional ship having the same purpose or design.

These obligations may be adjusted for an unmanned ship taking into account all the means at its disposal.

However, at a minimum, it should be ensured that distress signals are received and relayed to the relevant search and rescue authorities.

3.5 MARPOL convention

3.5.1 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.

3.5.2 In a similar way, it should be always possible to automatically control the air emissions from ships

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

3.6 COLREG convention

3.6.1 To prevent collision at sea, the two main tasks that should be handle by any ship covered by this Guidance Note are:

• the lookout:

to ensure that the ship is always monitored by using appropriate information to have a full appraisal of the situation and the risk of collision

• the operational decisions:

obligation for a ship to take avoidance decisions.

3.6.2 The following regulations from COLREG as amended should be applied as far as practicable:

- Part B Steering and sailing Rules 4 to 19
- Part C Lights and shape Rules 20 to 31
- Part D Sound and light signals Rules 32 to 37.

3.6.3 Any ship should be able to inform other ships (conventional ships included) about its status and intentions, by giving a specific light signal or communication message (e.g. AIS).

Any ship should be able to communicate with other ships (conventional ships included) 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.

3.7 ISM code

3.7.1 The requirements of the ISM code should be considered by the shipowner of any ship covered by this Guidance Note as a basis for developing, implementing and maintaining a proper Safety Management System (SMS), in order to ensure safety at sea, prevention of human injury or loss of life, and avoidance of damage to the environment, in particular, to the marine environment, and to property.

3.8 ISPS code

3.8.1 The requirements of the ISPS code should be considered by the shipowner of any ship covered by this Guidance Note as a basis for detecting security threats and take preventive measures against security incidents.

3.9 STCW convention

3.9.1 The status of crew, remote operators and technical personnel remains the responsibility of the Administration.

3.9.2 The requirements of STCW should be used as a basis for the qualification and the definition of duties for the crew and the remote operators.

3.9.3 These requirements may be adjusted taking into account that the officers could be based in the remote control centre or the crew reduced.

3.9.4 Education and training of the crew and operators should provide adequate skills for the general understanding and control of the system (e.g. software skills) and also for the management of abnormal situations or failures.

3.9.5 In particular, before any operation of a ship covered by this Guidance Note, training and quality procedure should be in place to insure that the crew or remote operators are perfectly aware of:

- the operational limitations of the ship
- the purpose and the different phases of the planned operations
- the degrees of automation and control for each phase
- the outcome of the risk and technology assessment as specified in Sec 2
- the means of control and alert in case of failure or damage
- the available fail-safe sequences.

3.9.6 When a ship is remotely operated, operators should be able to demonstrate appropriate specific trainings for remote control of the ship.

3.9.7 Technical personnel temporarily embarked aboard a ship for the purpose of maintenance or time-limited technical intervention should be trained and equipped for their mission.

3.9.8 Refer also to:

- Remote Control Centre manning, see Sec 3, [7.6]
- Human Machine Interface user training, see Sec 4, [3.5].

3.10 Maritime Labour Convention (MLC)

3.10.1 The requirements of MLC should be used as a basis for the minimum working and living standards for seafarers aboard ships, including, among others, minimum age, employment agreements, hours of work or rest, payment of wages, paid annual leave, repatriation at the end of contract, aboard medical care, the use of licensed private recruitment and placement services, accommodation, food and catering, health and safety protection and accident prevention and seafarers' complaint handling.

3.11 EU Ship Recycling Regulation (EU SRR)

3.11.1 The requirements of EU SRR should be used as a basis for proactive approach to safety and environmental protection in ships recycling, with a major focus on management of hazardous materials.

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 any ship covered by this Guidance Note.

1.1.2 The purpose of those assessments is to identify and to reduce to a level As Low As Reasonably Practicable (ALARP) the risks due to hazards that may threaten the ship within the operational limitations as defined in Sec 1, [2.3].

1.1.3 The risk-based approach considers a ship 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.

1.1.5 The risk and technology assessment should be carried out by persons (ideally an independent and appropriate third party) who have documented knowledge and experience of the relevant methodology used and who have the necessary knowledge of the systems to be assessed. Their role and skills should be documented. The risk and technology assessment report should be submitted to the Society for information.

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:

- ISO/IEC 31010 Risk management Risk assessment techniques
- ISO/IEC 27005 Information technology Security techniques Information security risk management.

2.1.2 Stages

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

- a) ship model formalisation (see [2.2])
- b) hazard identification (see [2.3])
- c) risk index calculation considering frequency and severity of the hazardous event (see [2.4])
- d) risk evaluation considering risk acceptance criteria (see [2.5])
- e) risk control options determination, when relevant (see [2.6]).

In case systems are not based on a qualified technology, a technology assessment should be carried (see [3]).

2.2 Ship model

2.2.1 At the first stage of the risk assessment, all main systems of a ship, including Remote Control Centre (RCC), should be split into several groups of functions covering essential services.

As a guidance, a list of typical groups of functions is given below:

- voyage
- navigation
- detection
- communication
- ship integrity, machinery and systems
- cargo and passenger management
- remote control
- security.

2.3 Hazard identification

2.3.1 Principles

The hazard 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, a list of typical hazards for ships covered by this Guidance Note are given in [2.3.2] to [2.3.9].

2.3.2 Voyage

Typical hazards that should be considered for voyage purpose are given in Tab 1.

Table 1 : Hazards for the voyage

Hazard	Consequence
Human error in input of voyage plan	Collision Grounding Sinking
Failure of update (e.g. of nautical publications, weather forecasts)	Loss of localisation Collision Grounding Sinking
Failure in position fixing (due to e.g. GPS selective availability)	Loss of localisation Collision Grounding Sinking

2.3.3 Navigation

Typical hazards that should be considered for navigation purpose are given in Tab 2.

2.3.4 Detection

Typical hazards that should be considered for detection purpose are given in Tab 3.

Table 2 : Hazards for the navigation

Hazard	Consequence		
Heavy traffic	Collision Sinking		
Heavy weather or unforeseeable events (e.g. freak wave)	Grounding Sinking		
Low visibility	Collision Grounding Sinking		
Collision with other ships or offshore infrastructures	Collision Sinking		
Collision with floating objects	Collision Sinking		
Collision with marine wildlife (e.g. whales, squids, carcasses)	Collision Sinking		
Collision with onshore infrastructures or failure in mooring process	Collision Grounding Sinking		
Loss of intact stability due to unfavor- able ship responses (e.g. to waves)	Sinking		
Loss of intact stability due to icing	Sinking		

Table 3 : Hazards for the detection

Hazard	Consequence
Failure in detection of small objects (wreckage)	Collision Sinking
Failure in detection of collision targets	Collision Sinking
Failure in detection of navigational marks	Loss of localisation Collision Grounding Sinking
Failure in detection of ship lights, sounds or shapes	Collision Grounding Sinking
Failure in detection of semi-sub- merged towed or floating devices (e.g. seismic gauges, fishing trawls)	Collision Sinking
Failure in detection of discrepancy between charted and sounded water depth (e.g. wreckage)	Grounding Sinking
Failure in detection of discrep- ancy between weather forecast and actual weather situation	Grounding Sinking
Failure in detection of slamming or high vibration	Hull or machinery damage Sinking

2.3.5 Communication

Typical hazards that should be considered for communication purpose are given in Tab 4.

2.3.6 Ship integrity, machinery and systems

Typical hazards that should be considered for ship integrity, machinery and systems purpose are given in Tab 5.

Table 4 : Hazards for the communication

Hazard	Consequence
Reduction of communication performance (e.g. insufficient bandwidth)	Loss of localisation Collision Grounding Sinking
Communication failure (e.g. with RCC, with relevant authorities, with ships in vicinity)	Loss of localisation Collision Grounding Sinking
Communication failure with an other ship in distress (e.g. message recep- tion, relay, acknowledgment)	Loss of localisation Sinking of the ship in distress
Failure in data integrity (e.g. error in data transmission)	Loss of localisation Collision Grounding Sinking

Table 5 : Hazards for the ship integrity, machinery and systems

Hazard	Consequence	
Water flooding due to structural dam- age or watertightness device failure	Sinking	
Fire	Sinking	
Sensor or actuator failure	Loss of localisation Collision Grounding Sinking	
Temporary or permanent loss of electricity (e.g. due to black-out)	Loss of localisation Collision Grounding Sinking	
Propulsion or steering failure	Collision Grounding Sinking	
Failure of ship's IT systems (e.g. due to bugs)	Loss of localisation Collision Grounding Sinking	
Failure of ship's IT infrastructure (e.g. due to fire in the server room)	Loss of localisation Collision Grounding Sinking	
Failure of anchoring devices when drifting	Collision Grounding Sinking	

2.3.7 Cargo and passenger management

Typical hazards that should be considered for cargo and passenger management are given in Tab 6.

2.3.8 Remote control

Typical hazards that should be considered for remote control purpose are given in Tab 7.

2.3.9 Security

Typical hazards that should be considered for security purpose are given in Tab 8.

2.4 Risk index calculation

2.4.1 Principles

The risk for a given accident scenario due to a 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 index

The frequency is estimated by the number of occurrences of an event to occur per ship year, in a fleet of several ships having the same operating mode.

Examples of frequency index (F) are given in Tab 9.

2.4.3 Severity index

The severity is estimated according to the impact on human, ship and environment.

Examples of severity index (S) are given in Tab 10 to Tab 12.

2.4.4 Risk index

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

Risk index (R) = Frequency index (F) + Severity index (S)

A risk index matrix may be formalised.

2.4.5 Risk index calculation

For each hazard, the risk index should be calculated in order to rank the risks by considering separately the impact on human, ship and environment.

Example of risk index calculation is given in Tab 13.

2.5 Risk evaluation

2.5.1 Principles

The acceptability of the risks identified by the risk index calculation should be reviewed in comparison with agreed risk acceptance criteria.

Table 6 : Hazards for the cargo and passenger management

Hazard	Consequence
Too much cargo or too many passengers aboard (overload)	Sinking
Loss of intact stability due to shift and/or liquefaction of cargo or due to cargo overboard	Sinking
Passenger overboard	Human injury or fatality
Passenger illness	Human injury
Passenger injured during arrival or departure	Human injury or fatality
Passenger interfering in an aboard sys- tem	Loss of localisation Collision Grounding Sinking

Table 7 : Hazards for the remote control

Hazard	Consequence
Unavailability of RCC (fire, environmen- tal phenomenon) or of operators (faint- ness, emergency situation, etc.)	Loss of localisation Collision Grounding Sinking
Human error in remote monitoring and control (e.g. through situation unaware- ness, data misinterpretation, RCC capac- ity overload)	Collision Grounding Sinking
Human error in remote maintenance	Loss of localisation Collision Grounding Sinking

Table 8 : 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, smug- glers)	Illegal actions Hijack Loss of localisation
Jamming or spoofing of AIS or GPS sig- nals	Loss of localisation Collision Grounding Sinking
Jamming or spoofing of communica- tions, hacker attack, also on RCC (e.g. in case of pirate or terrorist attack)	Loss of localisation Collision Grounding Sinking
Failure in data confidentiality (e.g. data interception by unauthorized 3rd party)	Illegal actions
Cyber virus spread from port facilities	Illegal actions Hijack Collision Grounding Sinking

Table 9 : Frequency index (F)

F	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

Table 10 : Severity index (S) for human

S	Definition	Human	Equivalent fatalities
1	Negligible	No damage to human	0,001
2	Minor	Light injuries to human	0,01
3	Severe	Serious injuries to human	0,1
4	Critical	One fatality, or less than 10 on-site permanent disabling injuries	1
5	Catastrophic	Multiple fatalities, and/or 10 or more on-site permanent disabling injuries also out- side the event area	10

Table 11 : Severity index (S) for ship

S	Definition	Ship	Equivalent damage
1	Negligible No damage: safety functions fully available		0,001
2	Minor	Local equipment damage: local damage to safety functions	0,01
3	Severe	Severe equipment damage: large local damages to safety functions	0,1
4	Critical	Critical damage: impairment of safety functions	1
5	Catastrophic	Total loss: total impairment of safety functions	10

Table 12 : Severity index (S) for environment

S	Definition	Environment	Equivalent oil or chemical substance spill
1	Negligible	Non significant spill, minor environment impact No off-site impact/damage	< 0,1 t
2	Minor	A few barrels of pollution to sea. Moderate environment impact Minor off-site impact	0,1 - 1 t
3	Severe	A few tonnes of pollution to sea. Significant environmental impact, situation manage- able Moderate off-site impact limited to property damage or minor health effects	1 - 100 t
4	Critical	Serious environment impact. Significant pollution demanding urgent measures for the control of the situation and/or cleaning of affected areas Significant off-site property damage or short term health effects to public	100 - 10 000 t
5	Catastrophic	Extensive environment impact. Major pollution with difficult control of situation and/or difficult cleaning of affected areas Extensive off-site property damage, fatalities or short term health effects to public	> 10 000 t

		Frequency index (F)	Severity index (S)			Risk index (R)		
Hazard	Consequence		Human	Ship	Environ- ment	Human	Ship	Environ- ment
Failure of ship's IT systems (e.g. due to bugs)	Loss of localisation	4	1	2	1	5	6	5
Failure in position fixing (due to e.g. GPS selective availability)	Grounding	5	2	3	3	7	8	8
Low visibility	Collision	7	3	4	3	10	11	10
Fire	Sinking	3	4	5	4	7	8	7

Table 13 : Risk index (R)

2.5.2 Risk acceptance criteria

It is the designer, shipyard, manufacturer and/or shipowner responsibility to specify the risk acceptance criteria.

The risk acceptance criteria should at minimum consider the following risks:

- risk to human (risk of injury, loss of lives)
- risk to the environment (risk of pollution)
- risk to the ship (risk of damage).

Specific requirements about risk acceptance criteria may be defined by the Administration and / or other Authorities.

The risk acceptance criteria considered for the risk assessment are to be submitted to the Society for information.

The Society reserves the right to reject risk acceptance criteria that would be considered to provide higher risks levels than the implicit ones in Society Rules for conventional ships having the same purpose or design.

2.6 Risk control options (RCO)

2.6.1 Principles

Considering the results of the risk evaluation, risk control options (RCO) may be defined.

The RCO should be determined to prevent the occurrence or to mitigate the consequences of an accident scenari.

2.6.2 Risk reduction measures

The RCO should be categorised by considering one or more, but not limited to, of the following attributes:

- preventive: when reducing the frequency of the event through better design, procedures, organisation policies, training, etc.
- mitigating: when reducing the severity of the outcome of the event

The following categorisation should also be considered:

- inherent: when choices are made in the design concept that restrict the level of potential risk
- engineering: when safety features (either built in or added on) are within the design
- procedural: when crew or operators control the risk by behaving in accordance with defined procedures.

As a general guidance, the risk control options selection process should focus on preventive rather than mitigating measures and inherent or engineering rather than procedural measures.

Typical RCO for ships covered by this Guidance Note are given 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.

This technology assessment should be done following the recommendations of Society Guidance Note NI525 "Risk Based Qualification of New Technology - Methodological Guidelines".

3.2 General

3.2.1 Qualification is a process by which a novel technology (a new technology or an existing technology used in a new context) is validated.

3.2.2 The qualification process is intended to prove with an acceptable level of confidence and in a cost effective manner that a technology is fit for purpose, that it complies with the specifications that the designer developed and that it is sufficiently reliable and is safe for the people and the environment.

3.2.3 The time frame and the costs are also important parameters: it is often impossible to perform tests for the duration of the entire expected life of the product that uses a novel technology and the qualification is to be cost effective with regards to the expected results.

3.2.4 The application of Risk Based Qualification of New Technology changes the standard processes of design review and inspection. The Guidance Note NI525 provides guidance as to how to perform them.

Table 14	: Risk	Control	Options
----------	--------	---------	---------

Category	Risk Control Option
Unmanned ship	Design of RCC for a proper control and monitor Suitable RCC manning as well as training of operators
and Remote Control	Ship should be directly controlled in heavy or complex traffic
	A ship without accommodation is easier to secure against stowaways
	Design of aboard systems for easy maintenance and accurate monitoring of maintenance state Must also be fast to repair
Unmanned mainte-	Need redundant power generation, distribution, propulsion and steering
operations	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.
Hoovy weather	Software are to be able to avoid heavy or otherwise dangerous weather – use of weather routing.
Heavy weather	Restricted navigation notation.
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 RCC may be particularly vulnerable. Data communication links must also have sufficient redundancy.

SECTION 3

FUNCTIONALITY OF AUTOMATION 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 of any ship covered by this Guidance Note.

For each automation 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 Navigating Automation System (NAS) 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 NAS should deal with all matters related to navigation, including voyage planning, docking and undocking, mooring and unmooring, navigation, anchoring and assistance in distress situations.

2.2.2 The NAS should include also RCC communication capabilities for remotely controlled or remotely supervised operations.

2.2.3 The NAS 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 docking, undocking, mooring, unmooring and anchoring operations, as well as the harbour navigation or port approach and the assistance in distress situations should be controlled or remotely supervised in case the degree of automation does not allow a full automation for these operations.

2.3 References

2.3.1 The navigation system should be compliant with the applicable requirements related to the assignment of the following additional class notation from Society classification Rules listed in Sec 1, [3.2.1], as applicable:

 for integrated bridge system SYS-IBS

e.g. see NR467, Pt F, Ch 4, Sec 2

 for dynamic positioning with redundancy DYNAPOS AM/AT R

e.g. see NR467, Pt F, Ch 11, Sec 6

2.3.2 The applicable requirements related to the assignment of these additional class notations may be adjusted to the satisfaction of the Society according to the results of the risk and technology assessment, the degree of automation, the degrees of direct control and remote control, the navigation notation, the operational limitations, the possibility of external rescue, etc.

2.4 Voyage planning

2.4.1 The voyage plan describing the full voyage from departure to arrival should be definable and updatable at any time by the crew or remotely by the operators.

2.4.2 The voyage plan should be defined taking into account the latest updates of charts, weather forecasts and all relevant information relating to the planned area of operations.

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

2.4.4 In particular, the crew or remote operators should program control points (or appointments) in order to control the progress of the ship.

2.4.5 Depending on the degree of automation, the NAS should be able to notify the RCC 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.

2.5 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 RCC, AIS transceivers or data providers (Navigational Telex NAVTEX, SafetyNET).

2.5.3 It should be demonstrated that the NAS is able to 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 degree of automation 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.

2.5.5 The NAS should also be able to initiate fail-safe sequences, see [8].

2.6 Docking and undocking

2.6.1 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.

2.6.2 A device should be available to stop the sequence of docking or undocking at any time in the event that the system has not been able to detect a hazardous situation.

2.7 Lookout

2.7.1 Any ship covered by this Guidance Note should comply with the principles of the Rule 5 of the COLREG as amended by maintaining at all times a proper lookout 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.

This lookout may be carried out:

- by crew
- by remote operators from the RCC with continuous access to on-board or off-board surveillance and warning systems to prevent collisions
- by an automation system equipped with warning sensors and actuators allowing the ship to react to a collision situation in accordance with international rules (COLREG).

2.7.2 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 RCC.

2.7.3 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.

See also [2.11] about collision avoidance and [2.12] about situational awareness.

2.7.4 Sensors protection devices should be provided to ensure the good quality of the data transmitted in all weather conditions (high brightness, presence of water, salt, ice,...).

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 RCC.

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 manoeuvrability conditions a route optimization should be conducted under weather routing criteria.

2.9 Ship status and dynamics

2.9.1 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.

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

2.9.3 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).

2.9.4 It is the crew and remote operators responsibility to load and operate the ship in a proper manner.

In particular, it will be assumed that:

- the draught of the ship in operating conditions will not exceed that corresponding to the freeboard assigned
- the ship will be properly loaded taking into account both its stability and the stresses imposed on its structures
- cargoes will be properly stowed and suitably secured
- the speed and course of the ship are adapted to the prevailing sea and weather conditions according to the normal prudent seamanship.

2.9.5 Particular attention should be paid by operators to the remote monitoring and control of operations: full situational awareness may be impaired for the remote operators by the absence of certain human senses at the remote control station such as balance, acceleration, smell, temperature, vibrations, etc.

2.10 Voyage recording

2.10.1 Data from essential services and any other significant process identified during the risk assessment should be received and stored in the log book or equivalent data

recording device. 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 RCC and their associated intervals and amount should depend on the current ship control mode (e.g. remote or full automation).

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

2.11 Collision avoidance

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

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

2.11.3 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.

2.12 Situational awareness

2.12.1 Relevant input parameters for the process of navigation should be provided by devices (e.g. sensors) to have an accurate situational awareness, which provides the NAS 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 Radionavigation system, GNSS and shipborne Position, Navigation and Timing (PNT) data processing should be compliant with the applicable requirements of the following standards as amended:

- IMO Resolution A.1046(27) Worldwide radionavigation system
- IMO Resolution A.915(22) Revised maritime policy and requirements for a future Global Navigation Satellite System (GNSS)
- IMO Resolution MSC.401(95) Performance standards for multi-system shipborne radionavigation receivers
- IMO MSC.1/CIRC.1575 Guidelines for shipborne Position Navigation and Timing (PNT) data processing

2.12.3 Special attention should be paid to the limitations due to technical reasons and legal reasons (COLREG). 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 kilometre).

2.12.4 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 hectometres).

2.12.5 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 RCC, 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 RCC and 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 kilometres.

3.5 Performance

3.5.1 Remotely controlled ship should require more communication bandwidth for operation than a conventional ship and should require 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 RCC or ship to shore due to the amount of data transmitted by the automation 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.

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

Table 1 : Minimum bandwidth and latency

4 Machinery system

4.1 Goal

4.1.1 The goal of the machinery automation 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 machinery automation system should monitor and control the propulsion plant and steering system.

4.2.2 The machinery automation 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 related to the assignment of the following additional class notation from Society classification Rules listed in Sec 1, [3.2.1], as applicable:

for integrated machinery spaces

AUT-IMS

e.g. see NR467, Pt F, Ch 3, Sec 4

 for automated operation in port AUT-PORT

e.g. see NR467, Pt F, Ch 3, Sec 3

for availability of machinery **AVM-IPS**

e.g. see NR467, Pt F, Ch 2, Sec 3

4.3.2 The applicable requirements related to the assignment of these additional class notations may be adjusted to the satisfaction of the Society according to the results of the risk and technology assessment, the degree of automation, the degrees of direct control and remote control, the navigation notation, the operational limitations, the possibility of external rescue, etc.

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, in particular for ships with high degrees of automation (e.g. degree A3 or A4) and for unmanned ships.

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 crew or operators.

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 the RCC.

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 operators from the RCC. 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 cargo management automation 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 cargo management automation system should collect and monitor the main cargo parameters.

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

5.3 References

5.3.1 The cargo management system should be compliant with the applicable requirements related to the assignment of the following additional class notation from Society classification Rules listed in Sec 1, [3.2.1], as applicable:

• for liquid cargo in bulk

CARGOCONTROL

e.g. see NR467, Pt F, Ch 11, Sec 9

- for liquid cold cargo
- COLD CARGO

e.g. see NR467, Pt F, Ch 11, Sec 11

for refrigerated cargo

REF-CARGO

e.g. see NR467, Pt F, Ch 7, Sec 2

5.3.2 The applicable requirements related to the assignment of these additional class notations may be adjusted to the satisfaction of the Society according to the results of the risk and technology assessment, the degree of automation, the degrees of direct control and remote control, the navigation notation, the operational limitations, the possibility of external rescue, etc.

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 crew or the operators 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 cargo management automation 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.

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 aboard should be designed to avoid any deliberate or unwilled interference or obstruction by a passenger.

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

6.3 References

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

6.3.2 The passenger management system should be compliant with the applicable requirements related to the assignment of the following additional class notation from Society classification Rules listed in Sec 1, [3.2.1], as applicable:

• for man overboard detection MOB

e.g. see NR467, Pt F, Ch 11, Sec 27.

6.3.3 The applicable requirements related to the assignment of this additional class notation may be adjusted to the satisfaction of the Society according to the results of the risk and technology assessment, the degree of automation, the degrees of direct control and remote control, the navigation notation, the operational limitations, the possibility of external rescue, etc.

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 Life saving

6.5.1 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.

6.5.2 In case of a passenger overboard, an alarm should be accessible to the passengers aboard (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.

6.5.3 Any ship should be able to detect the presence of a liferaft or person in the water near the ship and this detection should be reported to the RCC if any.

7 Remote Control Centre

7.1 Goal

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

7.2 Functional requirements

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

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

7.2.3 The RCC should be designed and operated in accordance with land-based regulations as applicable.

7.2.4 The RCC should be included in the scope of the Safety Management System (SMS), see Sec 1, [3.7], and Security management, see Sec 1, [3.8].

7.3 References

7.3.1 The ergonomics and the layout of the RCC should be based on the following international standards:

• ISO 11064 (all parts) Ergonomics design of control centres.

7.4 Means of communication

7.4.1 The RCC 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).

7.4.2 With regard to the obligation of assistance (SOLAS Chapter V Reg.33), it should be ensured at a minimum that distress signals are received and relayed by the RCC to the relevant search and rescue authorities.

7.5 Monitoring and control

7.5.1 The RCC should be able to plan and to upload voyage data to the ship.

7.5.2 The RCC operators 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 RCC.

7.5.3 The same RCC may simultaneously monitor and control several ships operating in a coordinated (swarm) or independent manner.

In this last case, it is recommended to gather information about essential services on one dashboard for each ship under monitoring and control.

7.5.4 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.

7.5.5 The dashboard should display an information panel summarizing essential services to have a clear view of the situation of the ship with for each of them, a coloured flag indicator:

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

7.5.6 See also Sec 4, [3] about Human Machine interface.

7.6 Manning

7.6.1 The RCC should be manned with qualified, certified and medically fit personnel, such as operators, supervisors, ship engineers and captains.

7.6.2 The RCC should be appropriately manned in order to encompass all aspects of maintaining safe operations aboard ships remotely monitored and controlled.

7.6.3 Personnel should have sufficient sea-going or in service experiences related to an equivalent ship under control.

7.6.4 Simulator training should be used for practicing of operators and supervisors.

7.6.5 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.

7.6.6 The RCC should be manned for uninterrupted supervision during operations.

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

8 Failures or malfunctions

8.1 Fail-safe sequences

8.1.1 In the event of failure or malfunction of one or more automation systems, fail-safe sequences should be defined.

8.1.2 The purpose of these fail-safe sequences is to recover a safe situation for the ship itself, for people, for other ships and for the environment.

8.1.3 These fail-safe sequences should be defined depending on the automation system concerned, the degree of automation and the operating mode (e.g. manoeuvring in harbour or at sea).

8.1.4 At least two different fail-safe sequences should be available at all times and under all circumstances during normal operations of the ship.

8.1.5 The crew or remote operators should be able to select and prioritise potential fail-safe sequences during the preparation of the voyage plan.

8.1.6 For example, in case the connection between ship and RCC or between ship and shore is unavailable for a period of time, the ship should enter into a fail-safe sequence to be defined depending on the degree of automation.

This fail-safe sequence could include for instance the following options to be considered with regard to the risk assessment, considering that at least two of these options should be available:

- a) crew attempts to take a manual control
- b) ship slows down to the next waypoint and waits for the crew, the remote operators or the system to regain control
- c) ship stops and stays at the current position, waiting for the crew, the remote operators or the system to regain control
- d) ship sails back to the previous waypoint and waits for the crew, the remote operators or the system to regain control

8.2 Minimum communication link

8.2.1 A minimum communication link between the ship and the RCC should be maintained at all times and under all circumstances with, for example, a simplified radio or

satellite link, in order to be able to exchange a regular status report specifying the status of the ship (for instance that there are no incidents in progress and no alarms triggered).

8.2.2 Similarly, ship automation systems associated with essential services such as for example navigation, communication, machinery, cargo management and passenger management systems should receive this status report so that they can react accordingly in the event of an incident or an alarm being triggered. If no action is taken at the RCC, the ship should be able to enter into a failure sequence on its own.

8.2.3 In the case of remote control, it is the responsibility of remote operators to ensure that the ship remains within the range of its means of communication at all times and under all circumstances. When a ship is no longer within the range of its means of communication allowing its control, this ship should be able to enter into a failure sequence on its own.

8.3 Degraded modes

8.3.1 When the communication link between the RCC and the ship is degraded or interrupted for a significant period of time identified in the risk analysis, the ship should be monitoring and controlled by the crew and/or by automation systems capable of performing the following functions:

- navigation monitoring and control including location, speed regulation, heading and manoeuvring control, buoyancy and stability control
- monitoring and prevention of collisions at sea
- visual and audible signalling
- damage detection
- alert to any persons on board in the event of damage
- receive distress signals and relay them to the relevant search and rescue authorities
- initiate fail-safe sequences

8.3.2 In the event of a situation that could present a risk to navigation, such as partial or complete loss of manoeuvrability or persistent loss of communication between the RCC and the ship, the crew or remote operators should be able to report this situation by urgent notification to other ships (conventional ships included) operating in the vicinity and by an appropriate visual or audible alert. This limitation should be also reported by AIS.

8.3.3 Any ship covered by this Guidance Note should be fitted with towing arrangement that can be used in case of emergency to assist the ship and in compliance with the requirements of Society Rules for Steel Ships NR467, Pt B, Ch 9, Sec 4.

8.3.4 In case of loss of manoeuvrability, the possibility of anchoring (or using a floating anchor for small units) may be considered in order to limit drift.

8.3.5 For unmanned ship, it should be possible to perform towing and anchoring operations remotely or automatically.

RELIABILITY OF AUTOMATION SYSTEMS

1 General

1.1 Scope

1.1.1 This Section provides guidelines for improving the reliability of automation systems associated with essential services of any ship covered by this Guidance Note.

2 General system design

2.1 References

2.1.1 Design, construction, commissioning and maintenance of all computer based systems associated to essential services should be in accordance with the requirements of NR467, Pt C, Ch 3, Sec 3 and NR467, Pt C, Ch 3, Sec 6.

2.1.2 Any ship covered by this Guidance Note should be provided with a software registry in compliance with the applicable requirements related to the assignment of the additional service feature **SW-Registry**, see NR467, Pt C, Ch 3, Sec 3.

2.1.3 The computerized based system life cycle should be based on the following international standards:

- ISO/IEC/IEEE 15288 Systems and software engineering System life cycle processes
- ISO/IEC/IEEE 12207 Systems and software engineering -Software life cycle processes
- ISO/IEC 61508 (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:

- IMO A.1021(26) Code on alerts and indicators.
- IMO MSC/CIRC.982 Guidelines on ergonomic criteria for bridge equipment and layout
- ISO 9241-210 Ergonomics of human-system interaction Part 210 Human-centred design for interactive systems
- ISO 8468 Ships and marine technology Ship's bridge layout and associated equipment Requirements and guidelines
- ISO 2412 Shipbuilding Colours of indicator lights.

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 human. 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 The management and the prioritisation of warning and alarm indicators should be defined in the operational limitations. Warning and alarm indicators should only be activated when an action is required and should specified the required action.

3.4.6 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.

3.4.7 In case of an input error, the system is to require human to correct the error immediately.

3.4.8 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.

3.5.2 See also Sec 1, [3.9] about STCW and Sec 3, [7.6.4].

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:

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

4.2 Design

4.2.1 Permanent and reversible communication system between ship, RCC 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:

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

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, see [8.1].

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 Cyber security

7.1 References

7.1.1 The computer based systems and networks should be compliant with the applicable requirements related to the assignment of the additional class notation **CYBER SECURE** from Society Rule Note NR659, Cyber Security for the Classification of Marine Units.

7.1.2 The applicable requirements related to the assignment of these additional class notation may be adjusted to the satisfaction of the Society according to the results of the risk and technology assessment, the degree of automation, the degree of direct control and remote control, the navigation notation, the operational limitations, the possibility of external rescue, etc.

8 Testing

8.1 Software testing

8.1.1 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.

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

8.1.3 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.

8.1.4 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.

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

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

8.2 Simulation testing

8.2.1 The aim of the simulation tests is to demonstrate by virtual means (simulation) the safe operations of any ship covered by this Guidance Note and associated RCC if any.

8.2.2 Tests should be defined in order to cover all expected operating scenarios and should address the following topics:

• Functionality:

All functionalities of systems associated to essential services should be tested.

- Performance: Performance assessment criteria should be defined beforehand.
- Failure resiliency:

All hazards identified in the risk assessment (see Sec 2, [2]) should be simulated in order to confirm the resiliency of systems associated to essential services.

8.2.3 Hardware-in-the-loop (HWIL) testing could be considered for checking proper working of any embedded control systems: refer to the requirements of Society Rule Note NR632, Hardware-in-the-loop Testing.

8.3 Full scale testing

8.3.1 The results of all simulation tests as specified in [8.2] are to be verified as far as feasible by full scale testing during sea trials.

8.3.2 Full scale testing should be done in a specific tests area approved by the Administration.

8.3.3 See also Sec 1, [3.3.3] about the IMO Interim Guidelines for MASS trials MSC.1/Circ.1604.



Move Forward with Confidence

Marine & Offshore Le Triangle de l'Arche - 8 Cours du Triangle - CS 50101 92937 Paris La Defense Cedex - France Tel: + 33 (0)1 55 24 70 00 https://marine-offshore.bureauveritas.com/bv-rules © 2019 Bureau Veritas – All rights reserved