RULES FOR CLASSIFICATION OF

Ships / High Speed, Light Craft and Naval Surface Craft

PART 4 CHAPTER 9

NEWBUILDING
MACHINERY AND SYSTEMS – MAIN CLASS

Control and Monitoring Systems

JULY 2011

DET NORSKE VERITAS AS

FOREWORD

DET NORSKE VERITAS (DNV) is an autonomous and independent foundation with the objectives of safeguarding life, property and the environment, at sea and onshore. DNV undertakes classification, certification, and other verification and consultancy services relating to quality of ships, offshore units and installations, and onshore industries worldwide, and carries out research in relation to these functions.

The Rules lay down technical and procedural requirements related to obtaining and retaining a Class Certificate. It is used as a contractual document and includes both requirements and acceptance criteria.

Any comments may be sent by e-mail to *rules@dnv.com*
For subscription orders or information about subscription terms, please use distribution@dnv.com
Computer Typesetting (Adobe Frame Maker) by Det Norske Veritas

CHANGES

General

The present edition of the rules includes additions and amendments approved by the Executive Committee as of June 2011 and supersedes the July 2010 edition of the same chapter.

The rule changes come into force as indicated below.

Text affected by the main rule changes is highlighted in red colour in the electronic pdf version. However, where the changes involve a whole chapter, section or sub-section, only the title may be in red colour.

This chapter is valid until superseded by a revised chapter.

Main changes coming into force 1 January 2012

- **General**

— Software and hardware change handling requirements have been amended, also requirements for remote software maintenance.
— Guidance notes have been amended related to the documentation requirements, in particular related to the FMEA requirements.
— Requirements for on-board testing of the remote control system and associated machinery have been slightly amended
— Power supply requirements for control and monitoring systems amended and aligned with Pt.4 Ch.8.
— A new requirement for consistent use of naming and tagging of the main components has been added.
— The requirement for certification of remote control systems for vessel's main functions was moved from Pt.4 Ch.1.
— Definitions of emergency- and primary alarms have been deleted. These notations are no longer relevant, as the basic definition is found in Code on alerts and indicators (IMO).

- **Sec.4 Additional Requirements for Computer Based Systems**

— C501 is modified in order to be in line with UR E22 / Rev.1 Sept 2010, opening for the use of wireless systems.

Corrections and Clarifications

In addition to the above stated rule requirements, a number of corrections and clarifications have been made in the existing rule text.

CONTENTS

Sec. 1 General Requirements 6

A. Classification 6
A 100 Rule applications 6
A 200 Classification principles 6
A 300 Software and hardware change handling 7
A 400 Assumptions 8

B. Definitions 8
B 100 General terms 8
B 200 Terms related to computer based system 9

C. Documentation 10
C 100 General 10
C 200 Type approved products 13
C 300 Plans and particulars 14

D. Tests 14
D 100 General 14
D 200 Software module testing 14
D 300 Integration testing 15
D 400 System testing 15
D 500 On-board testing 15

Sec. 2 Design Principles 16

A. System Configuration 16
A 100 General 16
A 200 Field instrumentation 16
A 300 System 16
A 400 Integrated system 16

B. Response to Failures 16
B 100 Failure detection 16
B 200 System response 17

Sec. 3 System Design 18

A. System Elements 18
A 100 General 18
A 200 Automatic control 18
A 300 Remote control 18
A 400 Protective safety system 19
A 500 Alarms 19
A 600 Indication 20
A 700 Planning and reporting 21
A 800 Calculation, simulation and decision support 21

B. General Requirements 21
B 100 System operation and maintenance 21
B 200 Power supply requirements for control and monitoring systems 21

Sec. 4 Additional Requirements for Computer Based Systems 23

A. General Requirements 23
A 100 Assignment of responsibility when installing integrated systems 23
A 200 System dependency 23
A 300 Storage devices 23
A 400 Computer usage 23
A 500 System response and capacity 23
A 600 Temperature control 24
A 700 System maintenance 24
A 800 System access 24

B. System Software 24
B 100 Software requirements 24
B 200 Software development 25

C. Control System Networks and Data Communication Links 25
C 100 General 25
C 200 Network analysis **27**

C 300 Network test and verification 27
C 400 Network documentation requirements 27
C 500 Wireless communication 27
C 600 Documentation of wireless communication 28

Sec. 5 Component Design and Installation 29

A. General 29
A 100 Environmental strains 29
A 200 Materials 29
A 300 Component design and installation 29
A 400 Maintenance, checking 29
A 500 Marking 29
A 600 Standardising 30

B. Environmental Conditions, Instrumentation 30
B 100 General 30
B 200 Electric power supply 30
B 300 Pneumatic and hydraulic power supply 31
B 400 Temperature 31
B 500 Humidity 31
B 600 Salt contamination 31
B 700 Oil contamination 31
B 800 Vibrations 31
B 900 Inclination 31
B 1000 Electromagnetic compatibility 32
B 1100 Miscellaneous 32

C. Electrical and Electronic Equipment 34
C 100 General 34
C 200 Mechanical design, installation 34
C 300 Protection provided by enclosure 34
C 400 Cables and wires 35
C 500 Cable installation 35
C 600 Power supply 35
C 700 Fibre optic equipment 35

Sec. 6 User Interface 36

A. General 36
A 100 Application 36
A 200 Introduction 36

B. Workstation Design and Arrangement 36
B 100 Location of visual display units and user input devices 36

C. User Input Device and Display Unit Design 37
C 100 User input devices 37
C 200 Visual display units 37
C 300 Colours 37
C 400 Requirements for preservation of night vision (UIDs and VDUs for installation on the navigating bridge) 37

D. Screen Based Systems 37
D 100 General 37
D 200 Illumination 38
D 300 Colour screens 38
D 400 Computer dialogue 38
D 500 Application screen views 39

SECTION 1
GENERAL REQUIREMENTS

A. Classification

A 100 Rule applications

101 The requirements of this chapter shall apply to all control and monitoring systems required by the rules.

Guidance note:

Additional requirements for specific applications will be given under rules governing those applications.

---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

102 All control and monitoring systems installed, but not necessarily required by the rules, that may have an impact on the safety of main functions (listed in Pt.1 Ch.1 Sec.1 A200 of the Rules for Classification of Ships), shall meet the requirements of this chapter.

A 200 Classification principles

201 Classification of control and monitoring systems shall generally be according to the following principles:

— plan approval
— certification of major units of equipment associated with essential and important control and monitoring systems
— on-board inspection (visual inspection and functional testing).

Guidance note:

The plan approval normally includes case-by-case document assessment of each delivery, alternatively partly covered by type approval as specified in Standards for Certification 1.2 and 2.4.

---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

202 Major units of equipment associated with essential and important control and monitoring systems, as specified in the rules, shall be provided with a product certificate unless exemption is given in a DNV issued Type Approval Certificate or the logic is simple and the failure mechanisms are easily understood.

The certification procedure normally consists of:

— assessment of certain manufacturer documentation
— visual inspection
— verification of performance according to functional requirements based on approved test programs
— verification of failure mode behaviour
— verification of implementation software quality plan covering life cycle activities, if applicable
— issue certificate.

Other control and monitoring systems, which when found to have an effect on the safety of the ship may be required to be certified.

Guidance note:

Control and monitoring systems for the following systems shall be certified unless the above mentioned exemptions apply (in general, the certification requirements are given in the relevant application rule section, this list is for guidance only):

1A1

Pt.3 Ch.3 (ship rules): water tight doors, side and stern doors

Pt.4 Ch.3: diesel engines, electronic engine management, steam turbines, gas turbines

Pt.4 Ch.5: propellers, water jets, propulsion thrusters, dynamic positioning thrusters

Pt.4 Ch.7: boilers, thermal-oil installations, oil fired water heaters,

Pt.4 Ch.8: power management

Pt.4 Ch.9: main alarm system, integrated control and monitoring systems

Pt.4 Ch.14: steering gears

Ferries

Pt.5 Ch.2 (ship rules): bow doors monitoring

Oil Carriers

Pt.5 Ch.3 (ship rules): cargo tank level measurement, cargo tank overflow protection, cargo valves and pumps, flammable gas detection (permanent system only), inert gas, offshore loading and unloading

Chemical carriers

Pt.5 Ch.4 (ship rules): cargo tank level, cargo tank overflow protection, cargo valves and pumps, flammable gas detection (permanent system only), inert gas

Liquefied Gas Carriers

Pt.5 Ch.5 (ship rules): cargo tank level measurement, cargo tank overflow protection, cargo valves and pumps, flammable gas detection (permanent system only), inert gas, cargo and vapour pressure, oxygen indication equipment (permanent system only)

Well Stimulation Vessels

Pt.5 Ch.7 (ship rules): cargo tank level measurement, cargo tank overflow protection, emergency shut-down

Offshore Service Vessels for Transportation of Low Flashpoint Liquids

Pt.5 Ch.7 (ship rules): cargo tank level measurement

Slop Reception and Processing Facilities

Pt.5 Ch.10 (ship rules): oil separating, fire detection, inert gas

Ships for Carriage of Refrigerated Cargoes and Containers

Pt.5 Ch.10 (ship rules): cargo hold temperature

Dynamic Positioning systems

Pt.6 Ch.7 (ship rules): dynamic positioning, independent joystick with auto heading

Gas fuelled engine installations

Pt.6 Ch.13 (ship rules): Gas control system, gas safety system, ventilation system.

---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

203 The following control and monitoring systems are subject to certification, if installed, in addition to those specified in other sections:

— remote control of vessel main functions
— main alarm system
— integrated control and monitoring system.

A 300 Software and hardware change handling

301 The requirements in this section apply to software and hardware changes done after the certification, i.e. changes done after approval and issuance of the certificate.

302 Manufacturers or system suppliers shall maintain a system to track changes as a result of defects being detected in hardware and software, and inform users of the need for modification in the event of detecting a defect.

303 Major changes or extensions in hardware or software of approved systems shall be described and submitted for evaluation. If the changes are deemed to affect compliance with rules, more detailed information may be required submitted for approval and a survey may be required to verify compliance with the rules.

304 Software versions shall be identifiable as required in Sec.4.

305 When basic- or application software is changed on an approved control system, the following requirements apply:

— a procedure for software change handling shall be available on request, describing the necessary steps and precautions related to SW handling
— major modifications which may affect compliance with the rules shall be described and submitted to the society for evaluation before the change is implemented onboar
— no modification shall be done without the acceptance and acknowledgement by the ships responsible
— the modified system shall be tested and demonstrated for the ships responsible
— the modification shall be documented (including objective/reason for the change, description, authorisation, test record, signatures, date, new incremented SW revision no)
— a test program for verification of correct installation and correct functioning of the applicable functions shall be available
— in case the new software upgrade has not been successfully installed, the previous version of the system shall be available for re-installation and re-testing.

306 If the control system is approved for remote software maintenance (i.e. from outside the vessel), the following requirements apply supplementary to 304:

— A particular procedure for the remote SW maintenance operation shall exist
— No remote access or remote SW modification shall be possible without the acceptance and acknowledgement by the ships responsible
— The security of the remote connection shall be ensured by preventing unauthorized access (e.g. password, and other means of verification) and by protecting the data being transferred (e.g. by encryption methodologies).

— Before the updated software is put into real-time use, the integrity of the new software shall be verified by appropriate means
— The remote session shall be logged in accordance with the above procedure for remote SW maintenance.

A 400 Assumptions

401 The rules of this chapter are based on the assumptions that the personnel using the equipment to be installed on board are familiar with the use of, and able to operate this equipment.

B. Definitions

B 100 General terms

101 *Alarm* is for warning of an abnormal condition and is a combined visual and audible signal, where the audible part calls the attention of personnel, and the visual part serves to identify the abnormal condition.

102 A *control and monitoring system* includes all components necessary for control and monitoring, including sensors and actuators. In this chapter, *system* is short for control and monitoring system. A system includes all resources required, including:

— the field instrumentation of one or more process segments
— all necessary resources needed to maintain the function including system monitoring and adequate self-check
— all user interfaces.

103 An *essential control and monitoring system* (hereafter called *essential system*) is a system which needs to be in continuous operation for maintaining the vessel's propulsion and steering. Examples of services are given in Ch.8 Sec.13. Additional class notations may extend the term essential services. Such extensions, if any, can be found in the relevant rule chapters.

Guidance note:
The objective for an essential function is that it should be in continuous operation. However the rules do not in all respects fulfil this objective as single failures may lead to unavailability of a function.

---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

104 An *important control and monitoring system* (hereafter called *important system*) is a system supporting services which need not necessarily be in continuous operation for maintaining the vessel's manoeuvrability, but which are necessary for maintaining the vessels functions as defined in Pt.1 Ch.1 Sec.1 A200 of the Rules for Classification of Ships, or other relevant parts of the rules. Additional class notations may extend the term important services. Such extensions, if any, can be found in the relevant rule chapters.

105 *Non-important control and monitoring systems* (hereafter called *non-important systems*) are systems supporting functions for which the Society has no requirements according to relevant definitions in the rules.

106 *Field instrumentation* comprises all instrumentation that forms an integral part of a process segment to maintain a function.

The field instrumentation includes:

— sensors, actuators, local control loops and related local processing as required to maintain local control and monitoring of the process segment
— user interface for manual operation (when required).

Other equipment items do not, whether they are implemented locally or remotely, belong to the field instrumentation. This applies to data communication and facilities for data acquisition and pre-processing of information utilised by remote systems.

107 A *process segment* is a collection of mechanical equipment with its related field instrumentation, e.g. a machinery or a piping system.

Process segments belonging to essential systems are referred to as essential.

108 An *integrated system* is a combination of computer based systems which are interconnected in order to allow common access to sensor information and/or command and control.

109 *Operator station* in an integrated system is a unit consisting of a user interface, i.e. UIDs and VDU, and interface controller(s).

110 *User* is any human being that will use a system or device, e.g. captain, navigator, engineer, radio operator, stock-keeper, etc.

111 *Workstation* is a work place at which one or several tasks constituting a particular activity are carried out and which provides the information and equipment required for safe performance of the tasks.

112 *Equipment under control (EUC)* is the mechanical equipment (machinery, pumps, valves, etc.) or environment (smoke, fire, waves, etc.) monitored and/or controlled by a control and monitoring system.

113 *Independent systems:* see Sec.2 A201.

114 *Redundancy* is defined as two mutually independent systems that can maintain a function.

115 *Remote control systems* comprise all equipment necessary to operate units from a control position where the operator cannot directly observe the effect of his actions.

(HSC Code 11.1.1)

116 *Back-up control systems* comprise all equipment necessary to maintain control of essential functions required for the craft's safe operation when the main control systems have failed or malfunctioned.

(HSC Code 11.1.2)

117 *Monitoring* includes indication, alarming and/or protective safety functions.

Guidance note:
Which of these elements a particular system contains depends upon the rule requirements for the application.

---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

118 *A protective safety system* is a system that is activated on occurrence of predefined abnormal process condition to bring the process / EUC to a safe state. The safety action may be automatic or manual.

119 Engineers' alarm is an alarm system, which shall be provided to operate from the engine control room or the manoeuvring platform, as appropriate, and shall be clearly audible in the engineers' accommodation.

(SOLAS Ch. II-1/38)

Guidance note:
The engineers' alarm is normally an integrated part of the extension alarm system, but may be a separate system.

---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

B 200 Terms related to computer based system

201 *Visual display unit (VDU)* is normally a computer monitor, but may also be any area where information is displayed including indicator lamps or panels, instruments, mimic diagrams, light emitting diode (LED) display, cathode ray tube (CRT), and liquid crystal display (LCD).

202 *User input device (UID)* is any device from which a user may issue an input including handles, buttons, switches, keyboard, joystick, pointing device, voice sensor and other control actuators.

203 A *software module* is an assembly of code and data with a defined set of input and output, intended to accomplish a function and where verification of intended operation is possible through documentation and tests.

204 *Basic software* is the software necessary for the hardware to support the application software.

Guidance note:
Basic software normally includes the operating system and additional general software necessary to support the general application software and project application software.

---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

205 *Application software* is ship specific computer software performing general tasks related to the EUC being controlled or monitored, rather than to the functioning of the computer itself.

206 *SW manufacturer* is a manufacturer of equipment/systems in which programmable electronic systems are a component in the delivery.

207 A *computer task* is, in a multiprocessing environment, one or more sequences of instructions treated by a control program as an element of work to be accomplished by a computer.

208 *Data communication links* include point to point links, instrument net and local area networks, normally used for inter-computer communication. A data communication link includes all software and hardware necessary to support the data communication.

Guidance note:
For local area networks, this includes network controllers, network transducers, the cables and the network software on all nodes.

---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

209 *A node in a network* is a processing location and can be a computer or other device, such as a printer. Every node has a unique network address.

C. Documentation

C 100 General

101 Overview documentation as listed in Table C1 is required submitted prior to commencement of approval work, applicable for ships with integrated systems installed.

Guidance note:
Typically submitted by yard based upon their detailed specification.

---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

102 For document assessment, documentation listed in Table C2 is required submitted in order to adequately describe control and monitoring systems.

103 For a system subject to certification, documentation listed in Table C3 shall be available for the surveyor at testing at the manufacturer.

104 For on-board inspection, documentation listed in Table C4 is required submitted to survey station.

105 For control and monitoring systems subject to approval an operation manual (Z160) and a maintenance manual (Z180) are to be kept onboard.

106 The documentation shall be limited to describe and explain the relevant aspects governed by the rule requirements.

Guidance note:
Documentation for a specific control and monitoring system should be complete (as required in Table C2) in one submittal.
A document may cover more than one instrumented system. A document may cover more than one documentation type.

---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

Guidance note:
Typically submitted by manufacturers based upon their project specific specification.

---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

107 Symbols used shall be explained, or reference to a standard code given.

108 The documentation type number together with identification of the control and monitoring system can be used as a unique identifier for the document. The “T” indicates that the documentation type is required also for control and monitoring systems where type approved components or software modules are used.

Table C1 Documentation required submitted prior to commencing approval work
(typically submitted by yard based upon their detailed specification, applicable for ships with integrated systems installed)

Documentation type	*Information element*	*Purpose*	*Where to*
System philosophy (I010) (T)	— the tasks allocated to each sub-system, divided between system tasks and manual tasks, including emergency recovery tasks — principles that will be used in the technical implementation of each system	Information	Approval centre
General arrangement for the ship	General ship information	Information	Approval centre
General arrangement for the main engine room	Main equipment layout	Information	Approval centre
Specification of main electro/mechanical equipment	Electric power generation. Main propulsion line(s) with machinery and essential auxiliaries. Miscellaneous machinery or equipment (where control and monitoring systems are specified by other sections of the rules). The following shall be specified: — manufacturer and type — rating — number of — purpose	Information	Approval centre

Table C2 Documentation required for assessment
(project specific documentation typically submitted by manufacturers)

Documentation type	*Information element*	*Purpose*
Functional description (system requirement specification) (I020) (T) *See Guidance Note 1*	— clear text description of the system configuration — clear text description of scope of supply and what is controlled and monitored and how — clear text description of safe state(s) for each function implemented — clear text description of switching mechanisms for systems designed with redundancy R0 — P&I/hydraulic/pneumatic diagrams if relevant.	Approval
System block diagrams (I030) (T)	— a diagram showing connections between all main components (units, modules) of the system and interfaces with other systems.	Approval
User interface documentation (I040)	— a description of the functions allocated to each work and operator station — a description of transfer of responsibility between work and operator stations.	Approval
Power supply arrangement (I050) (T)	— electrical supply: diagram showing connection to distribution board(s), batteries, converters or UPS.	Approval
Functional failure analysis (Z070) (T) Only where specifically requested by the DNV rules, or in special cases	The purpose of this functional failure analysis is to document that for single failures, essential systems will fail to safety and that systems in operation will not be lost or degraded beyond acceptable performance criteria when specified by the rules. The following aspects shall be covered: — a description of the boundaries of the system including power supply preferably by a block diagram — a list of items which are subject to assessment with a specification of probable failure modes for each item, with references to the system documentation — a description of the system response to each of the above failure modes identified — a comment to the consequence of each of these failures.	Approval

Table C2 Documentation required for assessment (Continued)
(project specific documentation typically submitted by manufacturers)

Documentation type	*Information element*	*Purpose*
Failure mode and effect analysis (FMEA) (Z071) (T) where specifically required by DNV Rules *See Guidance Note 2*	A failure modes and effect analysis (FMEA) shall be carried out for the entire system. The FMEA shall be sufficiently detailed to cover all the systems' major components and shall include but not be limited to the following information: — a description of all the systems' major components and a functional block diagram showing their interaction with each other — all significant failure modes — the most predictable cause associated with each failure mode — the transient effect of each failure on the vessels position — the method of detecting that the failure has occurred — the effect of the failure upon the rest of the system's ability to maintain station — an analysis of possible common failure mode. Where parts of the system are identified as non-redundant and where redundancy is not possible, these parts shall be further studied with consideration given to their reliability and mechanical protection. The results of this further study shall be submitted for review.	Approval
List of control & monitored points (I110) (T)	A list and or index identifying all input and output signals to the system as required in the rules, containing at least the following information: — service description — instrument tag-number — system (control, safety, alarm, indication) — type of signal (digital / analogue input / output).	Approval
Circuit diagrams (I150)	— for essential hardwired circuits (for emergency stop, shutdown, interlocking, etc.) details of input and output devices and power source for each circuit.	Approval
Test program for testing at the manufacturer (Z120) (T)	Description of test configuration and test simulation methods. Based upon the functional description, each test shall be described specifying: — initial condition — how to perform the test — what to observe during the test and acceptance criteria for each test. The tests shall cover all normal modes as well as failure modes identified in the functional failure analysis, including power and communication failures.	Approval
Data sheets with environmental specifications (I080)	— environmental conditions stipulated in Sec.5 for temperature, vibration, humidity, enclosure and EMC.	Information

Guidance note 1:
If the control system is simple, does not contain programmable components and the functionality and failure mechanisms can be easily understood from submitted drawings, the textual part of the functional description may upon agreement be omitted.

---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

Guidance note 2:
Where an overall ship FMEA is requested in the application rules, this FMEA is normally supplied by the yard, and often made by an independent FMEA supplier. The manufacturers of control systems related to the application (e.g. propulsion, steering, power management,) normally provide an FMEA covering their scope of delivery. Then these FMEAs from the control system manufacturers are supposed to be evaluated by the overall FMEA supplier with respect to the overall design intention, and the conclusions shell be incorporated into the overall FMEA.

---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

Table C3 Documentation required available for the testing at the manufacturer		
Documentation type	*Information element*	*Purpose*
Software quality plan, based upon life cycle activities (I140)	The software life cycle activities shall minimum contain procedures for: — software requirements specification — parameters data requirements — software function test: — parameter data test — validation testing — system project files stored at the manufacturer — software change handling and revision control.	Available for information at testing at the manufacturer.
Operation manual (Z160)	A document intended for regular use on board, providing information as applicable about: — operational mode for normal system performance, related to normal and abnormal performance of the EUC — operating instructions for normal and degraded operating modes — details of the user interface — transfer of control — redundancy — test facilities — failure detection and identification facilities (automatic and manual) — data security — access restrictions — special areas requiring user attention — procedures for start-up — procedures for restoration of functions — procedures for data back-up — procedures for software re-load and system regeneration.	Available for information at testing at the manufacturer.
Installation manual (Z170)	A document providing information about the installation procedures.	Available for information at testing at the manufacturer.
Maintenance manual (Z180)	A document intended for regular use on board providing information about: — maintenance instructions — fault identification and repair — list of the suppliers' service net.	Available for information at testing at the manufacturer.

Table C4 Documentation required for on-board inspection, typically supplied by the yard		
Documentation type	*Information element*	*Purpose*
Test program for quay and sea trials (Z140)	A description of all tests that shall be carried out at the quay or at sea trial including: — initial condition — what to test — how to perform the test — acceptance criteria for the test.	Approval at local DNV station

C 200 Type approved products

201 For type approved components or software modules, reference shall be made to the type approval certificate number, the manufacturer's name and product type identification.

Guidance note:

Documentation that has been approved during the type approval process should not be submitted, unless it has been revised or when asked for in the certificate.

---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

202 For systems where type approved components or software modules are incorporated, only the documentation types marked with "T" in 100 shall be submitted. However, documentation types not marked with "T" may also be submitted if their contents vary for different deliveries of the component or software module.

203 For type approved systems, where different options exist for the configuration, the type approval certificate shall be completed with information about the components and software modules that are incorporated.

C 300 Plans and particulars

301 Plans for control and monitoring the following systems shall be submitted when mandatory and/or installed, as applicable, found in the respective parts of the rules.

The following shall in addition be documented, if installed:

— remote control of vessel main functions
— main alarm system
— integrated control and monitoring system
— engineers alarm.

Guidance note:

List taken from respective parts of the rules, except Pt.6:

Pt.3 Ch.3: Water tight doors, side and stern doors, water leakage monitoring. (Rules for Classification of Ships)

Pt.4 Ch.3: Main and auxiliary engines, gas turbines, steam turbines.

Pt.4 Ch.4: Shafting, clutches/elastic couplings.

Pt.4 Ch.5: Propeller/water jets, thrusters.

Pt.4 Ch.6: Valves and pumps, remote control. (Rules for Classification of Ships)

Pt.4 Ch.7: Boilers, thermal-oil installations, incinerators, oil fired water heaters.

Pt.4 Ch.8: Power management system

Pt.4 Ch.9: Remote control of vessel main functions, main alarm system, integrated control and monitoring system, engineers' alarm

Pt.4 Ch.14: Steering gear

Pt.5 Ch.2: Bow doors monitoring, fire doors, water ingress detection system, ventilation, container refrigerating. (Rules for Classification of Ships)

Pt.5 Ch.3: Cargo and vapour temperature, cargo tank level, cargo tank overflow protection, cargo valves and pumps, flammable gas detection system (permanent system only), inert gas, offshore loading and unloading, oil discharge. (Rules for Classification of Ships)

Pt.5 Ch.4: Cargo tank oil/water interface detection, cargo and vapour temperature, cargo tank level, cargo tank overflow protection, cargo valves and pumps, flammable gas detection system (permanent system only), inert gas. (Rules for Classification of Ships)

Pt.5 Ch.5: Cargo and vapour temperature, cargo tank level, cargo tank overflow protection, cargo valves and pumps, cargo and vapour pressure, emergency shut-down system, Flammable gas detection system (permanent system only), inert gas, oxygen indication equipment (permanent system only). (Rules for Classification of Ships).

---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

D. Tests

D 100 General

101 All tests shall be according to test programs approved by the Society.

102 Tests in the presence of a DNV surveyor according to 200, 300 and 400 shall be performed at the manufacturers works.

103 The following shall be evaluated during test of computer based system:

— tools for system set-up and configuration of the EUC
— implementation of software quality plan, see also Sec.4 B200.

104 The tests and visual examinations shall verify that all relevant rule requirements are met. The tests are only to cover requirements given by these rules. The test programs shall specify in detail how the various functions shall be tested and what shall be observed during the tests.

105 Failures shall be simulated as realistically as possible, preferably by letting the monitored parameters exceed the alarm and protective safety limits. Alarm and protective safety limits shall be checked.

106 It shall be verified that all automatic control functions are working satisfactorily during normal load changes.

D 200 Software module testing

201 Documentation of compliance with software module testing according to requirements for software quality plan as described in Sec.4 B200 shall be available in connection with survey at manufacturers' works.

D 300 Integration testing

301 Integration tests include integration of hardware components into hardware units and integration of software modules in the same hardware unit.

302 Integration tests shall be done with the actual software and hardware to be used on board and shall include:

a) Hardware tests

— hardware failures.

b) Basic software tests

— basic software failures.

c) Application software tests.

d) Function tests of normal system operation and normal EUC performance, in accordance with the rules. Function tests are also to include a degree of performance testing outside of the normal operating parameters.

e) User interface tests.

Guidance note:

The tests may be done on a representative test system if the computer hardware is type approved.

---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

D 400 System testing

401 System tests shall include the entire system, integrating all units. The tests may also include several systems.

402 System tests shall be done with the software installed on the actual systems to be used on board, interconnected to demonstrate the functions of the systems with several units and / or the functions of several systems.

Guidance note:

The tests may be done on a representative test system if the computer hardware is type approved.

---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

403 The tests shall include those tests which were not/could not be completed on unit level.

D 500 On-board testing

501 The tests shall include:

a) During installation the correct function of individual equipment packages, together with establishment of correct parameters for alarm, control and protective safety (time constants, set points, etc.).

b) During installation and sea trials, the correct function of systems and integration of systems, including the ability of the control systems to keep any EUC within the specified tolerances.

c) The correct protection and capacity of power supplies.

d) Back-up and emergency control functions for essential vessel systems.

502 The tests shall demonstrate that the essential vessel functions are operable on the available back-up means of control as required in the relevant application rules, and in a situation where the main control system is disabled as far as is practical.

503 The test program for harbour and sea trials shall be approved by the local DNV station.

504 The remote control system shall, if fitted, be tested at sea to demonstrate stable control and operation of the propulsion system with its necessary auxiliaries over the full operating range, and regardless of the type of propulsion. It shall be demonstrated that necessary ramping / controller functions are implemented to ensure that any operation of the manoeuvring levers do not cause shutdown, instability or damage to the propulsion machinery or power generating units.

505 If the machinery system is designed for different normal operational modes, e.g. dual fuel engines, the test described in 504 shall be run for each relevant mode of operation.

SECTION 2
DESIGN PRINCIPLES

A. System Configuration

A 100 General

101 Essential and important systems shall be so arranged that a single failure in one system or one unit cannot spread to another unit.

102 Failure of any remote or automatic control systems shall initiate an audible and visual alarm and shall not prevent normal manual control.

A 200 Field instrumentation

201 The field instrumentation belonging to separate essential process segments shall be mutually independent.

Guidance note:

System B is *independent* of system A when any single system failure occurring in system A has no effect on the maintained operation of system B. A single system failure occurring in system B *may* have an effect on the maintained operation of system A.

Two systems are *mutually independent* when a single system failure occurring in either of the systems has no consequences for the maintained operation of the other system according to above.

---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

202 When the field instrumentation of a process segment is common for several control and monitoring systems, and any of these systems are essential, failures in any of these control and monitoring systems shall not affect this field instrumentation.

203 When manual emergency operation of an essential process segment is required, separate and independent field instrumentation is required for the manual emergency operation.

204 Electronic governors shall have their power supply independent of other consumers and arranged with redundancy type R0. Governors for engines, other than those driving electrical generators, which keep the last position upon power failure, are regarded as fulfilling the redundancy type R0. Speed sensor cabling shall be mechanically well protected.

Guidance note:

Electrical and electronic fuel injectors should be designed to permit the necessary functionality, in case of the most probable failures.

---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

205 The accuracy of an instrument shall be sufficient to serve the functionality and safe operation of the EUC.

A 300 System

301 For an essential system having more than one process segment, failure in the field instrumentation of one process segment shall not result in failure for the remaining parts of the system.

A 400 Integrated system

401 Control shall only be available on workstations from where control is intended and access shall be provided via a command transfer system.

402 At least two operator stations shall be available at the main work station ensuring that all functions that may need simultaneous attention are available.

B. Response to Failures

B 100 Failure detection

101 Essential and important systems shall have facilities to detect the most probable failures that may cause reduced or erroneous system performance.

Failures detected shall initiate alarms.

102 The self-check facilities shall cover at least, but not limited to, the following failure types:

— power failures.

Additionally for essential systems,

— loop failures, both command and feedback loops (normally short circuit and broken connections)
— earth faults.

Additionally for computer based systems,

— communication errors
— computer hardware failures
— see also Sec.4.

B 200 System response

201 The most probable failures, e.g. loss of power or wire failure, shall result in the least critical of any possible new conditions.

Guidance note:
Total loss of power to any single control system should not result in loss of propulsion or steering.

---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

202 For redundant systems, any failure shall not cause an interruption of the process control that jeopardizes safe operation of the EUC. This applies also to the most time critical functions.

Guidance note:
This typically applies to duplicated networks or controllers where a failure in one unit or network shall not lead to a downtime that may jeopardize the time response of the activation of a critical function, like e.g. a shutdown.

---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

SECTION 3
SYSTEM DESIGN

A. System Elements

A 100 General

101 A system consists of one or several system elements where each system element serves a specific function.

102 System elements belong to the following categories:

— automatic control
— remote control
— alarm
— protective safety
— indications
— planning and reporting
— calculation, simulation and decision support.

103 Whenever automatic shutdown is required in the application rules, this function shall be implemented in a system unit that is mutually independent of the control and alarm systems related to the same Equipment Under Control (EUC). For an EUC where the automatic shutdown system is independent, control and alarm functions may be implemented in common system units.

When the application rules only require control and alarm functions for a EUC, these functions shall be implemented in either mutually independent system units or alternative in common system units if the system is redundant.

A redundant system shall, upon failure, have sufficient self diagnostics to effectively ensure transfer of active execution to the standby unit.

Exceptions from these general principles may be given if specified in the application rules for the EUC.

Guidance note:

The independency requirement does not intend to prevent the different control-, alarm- and safety system units from communicating status information over e.g. a network, but each unit shall be able to perform its main functions autonomously, and not be dependent on the other control system units.

Redundancy in system design is in general not accepted as an alternative way to meet the requirement for independency between systems.

---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

A 200 Automatic control

201 Automatic control shall keep process equipment variables within the limits specified for the process equipment (e.g. the machinery) during normal working conditions.

202 The automatic control shall be stable over the entire control range. The margin of stability shall be sufficient to ensure that variations in the parameters of the controlled process equipment that are expected under normal conditions, will not cause instability. The automatic control system element shall be designed so as to accomplish the function it shall serve.

203 Automatic control such as automatic starting and other automatic operations shall include provisions for manually overriding the automatic controls unless safe manual operation is not feasible. Failure of any part of such systems shall not prevent the use of the manual override.

204 In closed loop systems, feedback failures shall initiate an alarm, and the system shall enter the least critical of possible new conditions. This normally implies the system to either remain in its present state or move controlled to “zero” state.

205 Where indication of the automatically controlled parameter is required, the sensor for indication shall not be common with the sensor for feedback to the automatic control.

A 300 Remote control

301 At the remote work station being in command, the user shall receive continuous information on the effects of his orders.

302 One work station shall be designated as the main work station.

Guidance note:

A work station may consist of multiple operator stations.

---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

303 When control is possible from several work stations, only one workstation shall be in control at any one time.

304 Control shall not be transferred before being acknowledged by the receiving work station, unless the work stations are located close enough to allow direct visual and audible contact. Transfer of control shall give an audible pre-warning.

305 The main work station shall be able to take control without acknowledgement, but an audible warning shall be given at the work station that relinquishes control. The action for taking control shall not be the same as the normal control action.

306 Means shall be provided to prevent significant alteration of process equipment parameters when transferring control from one location to another, or from one means or mode of operation to another. If this involves manual alignment of control levers, indicators shall show how the levers shall be set to become aligned.

307 It shall be indicated at each alternative work station, when control is held.

308 Safety interlocks in different parts of the systems shall not conflict with each other.

Basic safety interlocks must be hardwired and shall be active during remote and local operation.

Guidance note:

Hardwired safety interlocks should not be overridden by programmable interlocks.

---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

A 400 Protective safety system

401 The protective safety system element shall be so designed that the most probable failures, e.g. loss of power supply or wire failure, result in the least critical of any possible new condition (fail to safety) taking into consideration the safety of the machinery itself as well as the safety of the vessel.

For essential systems which have a stopped unit as it's fail to safety principle, loop monitoring according to Sec.2 B100 shall be provided and arranged such that loop failure initiates an alarm and do not stop the unit. Where loop failure monitoring is not possible, a two out of two voting system may be accepted.

402 Protective safety actions shall give alarm at predefined work stations.

403 When the protective safety system element stops a unit, the unit shall not start again automatically.

404 When a protective safety system element is made inoperative by a manual override, this shall be clearly indicated at predefined workstations.

405 When the protective safety system element has been activated, it shall be possible to trace the cause of the safety action by means of central or local indicators.

406 When two or more protective safety actions are initiated by one failure condition (e.g. start of standby pump and stop of engine at low lubricating oil pressure), these actions shall be activated at different levels, with the least drastic action activated first.

An alarm shall be activated prior to a protective safety action, except when it is regarded as not being possible due to urgency, see Ch.1, related Guidance note (Rules for Classification of Ships).

A 500 Alarms

501 Alarm indicating devices shall be arranged such as to ensure attention of the responsible duty officer, e.g. machinery alarm indicating devices located in the normal working areas of the machinery space.

Guidance note 1:

Several suitably placed low volume audible signal units should be used rather than a single unit for the whole area. A combination of audible signals and rotating light signals may be of advantage.

---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

Guidance note 2:

IMO resolution A.1021 (26) clause 9.5, requires that alarms and indicators on the navigation bridge should be kept at a minimum. Alarms and indicators not required for the navigation bridge should not be placed there unless permitted by the administration.

---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

502 Visual indication shall be easily distinguishable from other indications by use of colour and special representation.

Guidance note:
In view of standardising, visual alarm signals should preferably be red. Special representation may be a symbol.

---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

503 Audible signals used for alarms shall be readily distinguishable from signals indicating normal conditions, telephone signals, and noise.

504 Responsibility for alarms shall not be transferred before acknowledged by the receiving location. Transfer of responsibility shall give audible pre-warning. At each alternative location, it shall be indicated when in charge.

505 Acknowledgement of alarms shall only be possible at the workstation(s) dedicated to respond to the alarm. In normal operation (also including unattended mode), it shall not be possible to transfer the acknowledgement rights from the machinery space / engine control room to a work station located outside the machinery space.

Guidance note:
Alarm lists may be available on any workstation.

---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

506 Alarms shall be annunciated by visual indication and audible signal. It shall be possible to see and distinguish different statuses of the alarms e.g. normal, active, unacknowledged, acknowledged and blocked.

Silencing and acknowledgement of alarms shall be arranged as follows:

Silencing the audible signal:

— Silencing the alarm shall cause the audible signal to cease, in addition to extinguishing any related light signals.
— The visual alarm indication shall remain unchanged.

Acknowledgement of an alarm:

— When an alarm is acknowledged the visual indication shall change. An indication shall remain if the alarm condition is still active.
— If the acknowledge alarm function is used prior to silencing of the audible signal, the acknowledgement may also silence the audible signal.

An active alarm signal shall not prevent indication of any new alarms, with related audible signal and visual indication. This requirement shall also apply for group alarms.

In case the alarms are presented on a screen, only visible alarms may be acknowledged.

507 Acknowledgement of visual signals shall be separate for each signal or common for a limited group of signals. Acknowledgement shall only be possible when the user has visual information on the alarm condition for the signal or all signals in a group.

508 Local audible signal for an alarm included in a centralised alarm handling system shall be suppressed when localised in the same workplace as the centralised alarm handling system.

509 Manual suppression of separate alarms may be accepted, when this is continuously indicated when suppressed.

510 Sufficient information shall be provided to ensure optimal alarm handling. The presence of active alarms shall be continuously indicated, and alarm text shall be easily understood.

511 The more frequent failures within the alarm system, such as broken connections to measuring elements, shall initiate alarm.

512 Interlocking of alarms shall be arranged so that most probable failures in the interlocking system, e.g. broken connection in external wiring, does not prevent alarms.

513 Inhibiting of alarm and protective safety functions in certain operating modes (e.g. during start-up) shall be automatically disabled in other modes.

514 It shall be possible to delay alarms to prevent false alarms due to normal transient conditions.

A 600 Indication

601 Indications sufficient to allow safe operation of essential and important functions shall be installed at all control locations from where the function can be accomplished. Alarms or pre-warnings are not considered as substitutes for indications for this purpose.

Guidance note:
It is advised that indicating and recording instruments are centralised and arranged to facilitate watch-keeping, e.g. by standardising the scales, applying mimic diagrams, etc.

---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

602 Adequate illumination shall be provided in the equipment or in the ship to enable identification of controls and facilitate reading of indicators at all times. Means shall be provided for dimming the output of any equipment light source which is capable of interfering with navigation.

603 Indication panels shall be provided with a lamp test function.

A 700 Planning and reporting

Guidance note:
Planning and reporting functions are used to present a user with information to plan future actions.

---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

701 Planning and reporting system elements shall have no outputs for real-time process equipment control during planning mode.

Guidance note:
The output may however be used to set up premises for process equipment control, e.g. route plan used as input to an autopilot or load plan used as input for automatic or user assisted sequence control of the loading.

---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

A 800 Calculation, simulation and decision support

801 Output from calculation, simulation or decision support modules shall not suppress basic information necessary to allow safe operation of essential and important functions.

Guidance note:
Output from calculation, simulation or decision support modules may be presented as additional information.

---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

B. General Requirements

B 100 System operation and maintenance

101 Start-ups and restarts shall be possible without specialised system knowledge. On power-up and restoration after loss of power, the system shall be restored and resume operation automatically.

102 Testing of essential systems and alarm systems shall be possible during normal operation. The system shall not remain in test mode unintentionally, and an active test mode shall be clearly indicated on the operator interface.

Guidance note:
Automatic return to operation mode or alarm should be arranged.

---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

B 200 Power supply requirements for control and monitoring systems

201 This part of the rules gives requirements for the power supply to different categories of control and monitoring systems. The principal requirements for the arrangement of the power supply are defined in Ch.8 Sec.2 A101 and F300.

202 Essential control and monitoring systems shall be provided with two independent power supplies. This applies to both single and redundant control and monitoring systems.

Guidance note:
For redundant control and monitoring systems, it is acceptable that each independent power supply are feeding both systems.

---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

203 Redundant control and monitoring systems for important services, and control and monitoring systems required to be independent, shall be supplied by independent power supplies.

204 Redundant units in an integrated control and monitoring systems shall be provided with independent power supplies.

205 The following categories of control and monitoring systems shall be provided with uninterruptible power supply:

— Control and monitoring systems required to be operable during black-out.
— Control and monitoring systems required to restore normal conditions after black-out.
— Control and monitoring systems serving functions with redundancy type R0.

— Control and monitoring systems serving functions with redundancy type R1 - unless the control and monitoring system will be immediately available upon restoration of main power supply (i.e. no booting process).
— Control and monitoring systems for services with other redundancy types if the restoration time of the control and monitoring system exceeds the corresponding allowed unavailable time.
— Certain control and monitoring systems where specific requirements for stand-by power supply are given.

The capacity of the stored energy providing the uninterruptible power shall be at least 30 minutes, unless otherwise specified.

Refer to Ch.8 Sec.2 Table C1.

206 If the user interface is required to be duplicated, the requirement for independent power supplies also applies to the user interface. If uninterruptible power supply is required for the control system, this also applies to at least one user interface at the dedicated work stations.

SECTION 4
ADDITIONAL REQUIREMENTS FOR COMPUTER BASED SYSTEMS

A. General Requirements

A 100 Assignment of responsibility when installing integrated systems

101 There shall be one named body responsible for the integration of the total integrated system. This body shall have the necessary expertise and resources enabling a controlled integration process.

Guidance note:
The responsible body may be the yard, a major manufacturer or another competent body.

---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

A 200 System dependency

201 Where a computer based system is part of an essential function, back-up or emergency means of operation shall be provided, which to the largest extent possible shall be independent of the normal control system, with its user interface.

A 300 Storage devices

301 The on-line operation of essential functions shall not depend on the operation of rotating bulk storage devices, such as hard discs.

Guidance note:
This does not exclude the use of such storage devices for maintenance and back-up purposes.

---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

302 Software and data necessary to ensure satisfactory performance of essential and important functions shall normally be stored in non-volatile memory (e.g. EPROM, EEPROM or FLASH). Exception may be given for RAM with battery backup if the following three conditions are met:

— low battery voltage results in an alarm or visual indication detectable by routine inspections
— battery can easily be replaced by crew personnel without danger of losing data
— battery failure has no influence on performance as long as normal power supply is maintained.

A 400 Computer usage

401 Computers serving essential and important functions shall only be used for purposes relevant to vessel operation.

A 500 System response and capacity

501 Systems used for control and monitoring shall provide response times compatible with the time constants of the related EUC (equipment under control).

Guidance note:
The following response times are applicable for typical EUC on vessels:

Data sampling for automatic control purposes (fast changing parameters)	0.1 s
Data sampling, indications for analogue remote controls (fast changing parameters)	0.1 s
Other indications	1 s
Alarm presentations	2 s
Display of fully updated screen views	2 s
Display of fully updated screen views including start of new application	5 s

---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

502 System start-up and system restoration after power failures shall take place with sufficient speed to comply with the maximum unavailable time for the systems concerned, reverting thereafter to a pre-defined state providing an appropriate level of safety.

503 System capacities shall be sufficient to provide adequate response times for all functions, taking the maximum load and maximum number of simultaneous tasks under normal and abnormal conditions for the EUC into consideration.

A 600 Temperature control

601 Wherever possible, computers shall not have forced ventilation. For systems where cooling or forced ventilation is required for keeping the temperature at an acceptable level, alarm for high temperature or maloperation of the temperature control function, shall be provided.

A 700 System maintenance

701 Integrated systems supporting one or more essential or important function shall be arranged to allow individual units to be tested, repaired and restarted without interference with the maintained operation of the remaining parts of the system.

702 Essential systems shall have diagnostic facilities to support finding and repairs of failures.

A 800 System access

801 Access to system set-up or configuration functions for the EUC shall be protected to avoid unauthorised modifications of the system performance. For screen based systems, tools shall be available to allow easy and unambiguous modification of configuration parameters provided modifications are allowable under *normal operation*.

Guidance note:

As a minimum, this applies to:

- calibration data
- alarm limit modification
- manual alarm inhibiting.

The operator should only have access to the application(s) related to the operation of the functions covered by the system according to 301, while access to other applications or installations of such, should be prevented. Hot keys normally giving access to other functions or program exits (Alt+Tab, Ctrl+Esc, Alt+Esc, double-clicking in background, etc.) must be disabled on the UID's intended for normal operation.

---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

802 Unauthorised access to the operation of essential and important systems, from a position outside of the vessel, shall not be possible. Refer to Sec.1 A300.

B. System Software

B 100 Software requirements

101 Basic software on processor systems running application software belonging to different functions, shall have facilities for:

— running several modules under allocated priorities
— detection of execution failures of individual modules
— discrimination of faulty modules to ensure maintained operation at least of modules of same or higher priority.

102 Individual application software modules allocated as tasks under an operating system as specified above shall not perform operations related to more than one function. These modules shall be allocated priorities in accordance with the relative priority between the functions they serve.

103 When hardware belonging to inputs, outputs, communication links and user interface is configured to minimise the consequences of failures, the related software shall be separated in different computer tasks to secure the same degree of separation.

104 When calculation, simulation or decision support elements are used to serve essential functions, and a basic functionality can be maintained without these elements, the application software shall be designed so as to allow such simplified operation.

105 System set-up, configuration of the EUC and the setting of parameters for the EUC onboard shall take place without modification of program code or recompilation. The Society must be notified if such actions cannot be avoided.

106 Running application software versions shall be uniquely identified by number, date or other appropriate means. Modifications shall not be made without also changing the version identifier. A record of changes to the system since the original issue (and their identification) shall be maintained and made available to the surveyor on request.

Guidance note:

- When the setting of parameters is equivalent to programming then version identification of these settings should be available. Version identification may be a check sum.
- For integrated systems, identification should be available in the system overview.
- For any screen based system, identification should be readily available on the VDU during normal operation.
- PROM's to be labelled.

---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

B 200 Software development

201 All relevant actions under the development phase of a complex system software, shall be taken to ensure that the probability of errors that could occur in the program code is reduced to an acceptable level.

Relevant actions shall include at least:

— actions to ensure that the programming of applications is based on complete and valid specifications
— actions to ensure that software purchased from other parties has an acceptable track record and is subject to adequate testing
— actions to impose a full control of software releases and versions during manufacturing, installation onboard and during the operational phase
— actions to ensure that program modules are subject to syntax and function testing as part of the process
— actions to minimise the probability of execution failures.

Guidance note:

Typical execution failures are:

- deadlocks
- infinite loops
- division by zero
- inadvertent overwriting of memory areas
- erroneous input data.

---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

202 The actions taken to comply with 201 shall be documented and implemented, and the execution of these actions shall be retraceable. The documentation shall include a brief description of all tests that apply to the system (hardware and software), with a description of the tests intended made by sub-vendors, those carried out at the manufacturer's and those that remain until installation onboard.

203 When novel software is developed for essential systems, DNV “approval of the manufacturer” may be required, either prior to or as part of the actual product development.

C. Control System Networks and Data Communication Links

C 100 General

101 Any network integrating control and/or monitoring systems shall be single point of failure-tolerant. This normally implies that the network with its necessary components and cables shall be designed with adequate redundancy.

Guidance note:

If the fault tolerance is based on other design principles, e.g. a ring net, the fault tolerance shall be documented specifically. The requirement applies to the network containing the integrated control and monitoring systems, and not eventual external communication links to single controllers, remote I/O or similar (e.g. a serial line to an interfaced controller) when such units otherwise can be accepted without redundancy.

---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

102 The integrity and autonomy of each network segment within an integrated system shall be secured with appropriate network components, e.g. switches or routers. It shall be possible to protect each segment from unnecessary traffic on the remaining network, and each segment shall be able to work independent and with necessary operator interface.

Guidance note:

Virtual networks (VLAN) are normally not accepted as an alternative to segmentation.

---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

103 In a network integrating control and/or monitoring systems all network components controlling the network traffic and nodes communicating over the network shall be designed with inherent properties to prevent network overload at any time. This implies that neither the nodes nor the network components shall,

be able to generate excessive network traffic or consume extra resources that may degrade the network performance.

Guidance note:

This may imply that the nodes and network components shall have properties to monitor it's own communication through the network, and to be able to detect, alarm and respond in a predefined manner in case of an excessive traffic event.

---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

104 The performance of the network shall be continuously monitored, and alarms shall be generated if malfunctions or reduced/degraded capacity occurs.

105 Cables and network components belonging to redundant networks shall be physically separated; by separate cable routing and installation of network components belonging to the redundant network in separate cabinets, power supply to such units included.

106 It shall be possible to maintain local control of machinery as required by Ch.1 Guidance Note (ship rules) independent of network status. This may imply that essential nodes hosting such control functions shall be able to work autonomously, and with necessary operator interface independent of the network.

Guidance note:

To be demonstrated during sea-trial.

---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

107 Internode signals shall reach the recipient within a pre-defined time. Any malfunctions shall be alarmed.

Guidance note:

The 'pre-defined time' shall as a minimum correspond to the time constants in the EUC, which implies that the detection and alarming shall be initiated quickly enough to enable appropriate operator intervention to secure the operation of the EUC.

---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

108 If the automation system is connected to administrative networks, the connection principle shall ensure that any function or failure in the administrative net can not harmfully affect the functionality of the control and monitoring system. The administrative functions shall be hosted in separate servers and shall, if at all necessary, have 'read only' access to the control network.

Guidance note:

The “administrative network” in this connection may contain functions like e.g. report generation, process analysis, decision support etc. i.e. functions that by definition are not essential for vessel operation and not covered by the rules.

---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

109 Functions being irrelevant for vessel operation (e.g. miscellaneous office- or entertainment-related functions) shall not be connected in any way to any control and monitoring system or utilise its network.

110 It shall not be possible for unauthorised personnel to connect equipment to the control and monitoring network or otherwise have access to such network.

Guidance note:

This pertain to both communication onboard the vessel as well as remotely via external communication. Any access point to be clearly marked and shall be sufficiently secured e.g. by location with restricted access, a lockable device or password access.

---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

111 Any powered network component controlling the network traffic shall automatically resume to normal operation upon restoration of power after a power failure.

112 All nodes in a network shall be synchronized to allow a uniform time tagging of alarms (and events) to enable a proper sequential logging.

113 The network shall be designed with adequate immunity to withstand possible exposure to electromagnetic interference in relevant areas.

Guidance note:

This implies the use of suitable network media in areas exposed to high voltage equipment.

---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

114 Systems allowing for remote connection (e.g. via internet), for e.g. remote diagnostics or maintenance purposes, shall be secured with sufficient means to prevent unauthorised access, and functions to maintain the security of the control and monitoring system. The security properties shall be documented. Refer also to Sec.1 A300 for software change handling requirements.

Guidance note:

Any remote access to the control system shall be authorised onboard. The system shall have appropriate virus protection also related to the possibility of infection via the remote connection.

If remote connection for e.g. the above purposes is possible, the function is subject to special considerations and case-by-case approval.

---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

115 The CCTV system (Closed Circuit Television) shall not be part of an integrated control system.

C 200 Network analysis

201 The control and monitoring network with its components, connected nodes, communication links (also external interfaces) shall be subject to an analysis where all relevant failure scenarios are identified and considered. The analysis may be in the form of e.g. an FMEA, and shall specifically focus on the integrity of the different network functions implemented in separate network segments as well as the main network components (switches, routers etc.)

Guidance note:

The main purpose of the analysis shall identify possible failures that may occur in the network, identify and evaluate the consequences and to ensure that the consequences of failures are acceptable.

The analysis shall be performed in connection with the system design, and not after the system is implemented.

The requirement is basically applicable for all control and monitoring systems containing nodes connected on a common network. However, for simpler systems, the above requirement may be fulfilled by covering the most relevant failure scenarios in a test programme

---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

C 300 Network test and verification

301 The network functionality shall be verified in a test where at least the following items shall be verified:

1) The main observations / items from the FMEA
2) Self diagnostics, alarming upon different network failures
3) Worst-case scenarios – network storm
4) Segment segregation – autonomous operation of segments
5) Individual controller node integrity – nodes working without network communication
6) Consequence of single cabinet failure.

Guidance note:

In order to simulate e.g. fire in a single cabinet / cubicle, and to verify that essential vessel functions are still available

---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

C 400 Network documentation requirements

401 The following information related to the network properties shall be included in the documentation submitted for approval, (with reference to Sec.1, table C2):

1) Topology and network details including power supply arrangement
2) Functional description, with special focus on interfaces
3) Identification of critical network components
4) Qualitative reliability analysis (e.g. FMEA)
5) Failure response test programme.

C 500 Wireless communication

501 Wireless communication links may be used in systems as defined by IACS UR E22.

502 The wireless equipment shall not cause interference to licensed users of the ISM frequency bands in the geographical areas where the ship shall operate. The radiated power level should be adjustable.

Guidance note:

The wireless-equipment should be certified according to technical requirements established by applicable IEEE802 standards for operation within the ISM band. The user manual should identify any relevant spectrum and power restrictions for the ISM bands that may have been enforced by the authorities in the various states of relevance in the operating area of the vessel.

---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

503 The wireless broadcasting shall operate in the radio bands designated for ISM.

Guidance note:

The industrial, scientific and medical (ISM) bands are located at 900 MHz (902-928 MHz), 2.4 GHz (2400-2483.5 MHz) and 5.8 GHz (5725-5850 MHz).

---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

504 The wireless broadcasting shall sustain the anticipated electromagnetic environment on board and be tolerant towards interference from narrow-band signals.

Guidance note:

The type of modulation used should be of the category "spread spectrum" and be in compliance with the IEEE 802 series. Direct Sequence Spread Spectrum (DSSS) and Frequency Hopping Spread Spectrum (FHSS) are recognised standards for modulation.

If DSSS modulation is used and more than one access point (AP) may be active simultaneously, these APs should be physically separated and also use separate channels. The minimum processing gain should not be less than 10 dB.

---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

505 The wireless system shall entail a fixed topology and support prevention of unauthorised access to the network.

Guidance note:

The access to the network shall be restricted to a defined set of nodes with dedicated MAC (media access control) addresses.

---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

506 In case more than one wireless system shall operate in the same area onboard and there is a risk of interference, a frequency coordination plan shall be made and the interference resistance shall be documented and then demonstrated on board.

507 The wireless equipment shall employ recognised international protocols supporting adequate means for securing message integrity.

Guidance note:

The protocol should be in compliance with the IEEE 802 standard and the nodes should execute at least a 16-bit cyclic redundancy check of the data packets

---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

508 In case any form of control signals or confidential data is transferred over the wireless network, data encryption according to a recognised standard shall be utilised.

Guidance note:

Secure encryption schemes such as WiFi Protected Access (WPA) should be used to protect critical wireless data

---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

509 The data handling and final presentation of information shall comply with rules and regulations being applicable to the information category.

Guidance note:

Isochronous (real-time) or asynchronous (transmit-acknowledgment) transport will be required depending on the application.

---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

C 600 Documentation of wireless communication

601 The following information related to the wireless communication shall be included in the documentation submitted for approval, (with reference to Sec.1 Table C2):

— functional description
— ISM certificate (IEEE802) from a licence authority (typical flag state) or alternatively applicable test reports
— single line drawings of the WLAN topology with power arrangements
— specification of frequency band(s), power output and power management
— specification of modulation type and data protocol
— description of integrity and authenticity measures.

SECTION 5
COMPONENT DESIGN AND INSTALLATION

A. General

A 100 Environmental strains

101 Instrumentation equipment shall be suitable for marine use, and is normally to be designed to operate under environmental conditions as described in B, unless means are provided to ascertain that the equipment parameters are not exceeded. These means are subject to approval on case-by-case basis.

102 Data sheets, sufficiently detailed to ensure proper application of the instrumentation equipment, shall be available.

103 Performance and environmental testing may be required to ascertain the suitability of the equipment.

A 200 Materials

201 Explosive materials and materials which may develop toxic gases, shall not be used. Covers, termination boards, printed circuit cards, constructive elements and other parts that may contribute to spreading fire, shall be of flame-retardant material.

Guidance note:

Materials with a high resistance to corrosion and ageing should be used. Metallic contact between different materials should not cause electrolytic corrosion in a marine atmosphere. As base material for printed circuit cards, glass-reinforced epoxy resin or equivalent should be used.

---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

A 300 Component design and installation

301 Component design and installation shall facilitate operation, adjustment, repair and replacement. As far as practicable, screw connections shall be secured.

302 Mechanical resonances with amplification greater than 10 shall not occur.

303 Electric cables and components shall be effectively separated from all equipment, which, in case of leakage, could cause damage to the electrical equipment. In desks, consoles and switchboards, which contain electrical equipment, pipes and equipment conveying oil, water or other fluids or steam under pressure shall be built into a separate section with drainage.

304 Means shall be provided for preventing moisture (condensation) accumulating inside the equipment during operation and when the plant is shut down.

305 Differential pressure elements (dp-cells) shall be able to sustain a pressure differential at least equal to the highest pressure for the EUC (equipment under control).

306 Thermometer wells shall be used when measuring temperature in fluids, steam or gases under pressure.

307 The installation of temperature sensors shall permit easy dismantling for functional testing.

308 Clamps used to secure capillary tubes shall be made of a material that is softer than the tubing.

A 400 Maintenance, checking

401 Maintenance, repair and performance tests of systems and components are as far as practicable to be possible without affecting the operation of other systems or components.

Provisions for testing, (e.g. three-way cocks) shall be arranged in pipes connecting pressure switches/ transducers to EUC normally in operation at sea.

Guidance note:

The installation should as far as possible be built up from easily replaceable units and designed for easy troubleshooting, checking and maintenance. When a spare unit is mounted, only minor adjustments or calibrations of the unit should be necessary. Faulty replacements should not be possible.

---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

A 500 Marking

501 All units and test points shall be clearly and permanently marked. Transducers, controllers and actuators shall be marked with their system function, so that they can be easily and clearly identified on plans and in instrument lists. See also Ch.8 Sec.3 E.

Guidance note:

Marking of test points with e.g alarm or tag numbers is acceptable as long as they can easily be identified in the alarm list or other documentation.

The marking of system function should preferably not be placed on the unit itself, but adjacent to it.

---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

A 600 Standardising

Guidance note:

Systems, components and signals should be standardised as far as practicable.

---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

B. Environmental Conditions, Instrumentation

B 100 General

101 The environmental parameters given in 200 to 1100, including any of their combinations, represent "average adverse" conditions, which will cover the majority of applications on board vessels. Where environmental conditions will exceed those specified, special arrangements and special components will have to be considered.

Table B1 Parameter class for the different locations on board

Parameter	*Class*	*Location*
Temperature	A	Machinery spaces, control rooms, accommodation, bridge
	B	Inside cabinets, desks. etc. with temperature rise of 5°C or more installed in location A
	C	Pump rooms, holds, rooms with no heating
	D	Open deck, masts and inside cabinets, desks etc. with a temperature rise of 5°C or more installed in location C
Humidity	A	Locations where special precautions are taken to avoid condensation
	B	All locations except as specified for location A
Vibration	A	On bulkheads, beams, deck, bridge
	B	On machinery such as internal combustion engines, compressors, pumps, including piping on such machinery
	C	Masts
Electro-magnetic compatibility (EMC)	A	All locations except as specified for bridge and open deck
	B	All locations including bridge and open deck

Components and systems designed in compliance with IEC environmental specifications for ships, Publication No. 60092-504 (1994), and for EMC, IEC Publication No. 60533, may be accepted after consideration.

Guidance note:

For details on environmental conditions for instrumentation, see Standard for Certification 2.4.

Navigation and radio equipment shall comply with IEC Publication No. 60945, Marine navigational equipment - General requirements.

For EMC only, all other bridge-mounted equipment; equipment in close proximity to receiving antennas, and equipment capable of interfering with safe navigation of the ship and with radio-communications shall comply with IEC Publication No. 60945 (1996) Clause 9 (covered by EMC class B).

---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

B 200 Electric power supply

201 Power supply failure with successive power breaks with full power between breaks.

— 3 interruptions during 5 minutes
— switching-off time 30 s each case.

202 Power supply variations for equipment connected to A.C. systems:

— combination of permanent frequency variations of ±5% and permanent voltage variations of ±10% of nominal

— combination of frequency transients (5 s duration) ±10% of nominal and voltage transients (1.5 s duration) ±20% of nominal.

203 Power supply variations for equipment connected to D.C. systems:

— voltage tolerance continuous ±10% of nominal
— voltage transients cyclic variation 5% of nominal.
— voltage ripple 10%.

204 Power supply variations for equipment connected to battery power sources:

— +30% to -25% for equipment connected to battery during charging
— +20% to -25% for equipment connected to battery not being charged
— voltage transients (up to 2 s duration) ±25% of nominal.

B 300 Pneumatic and hydraulic power supply

301 Nominal pressure ±20% (long and short time deviations).

B 400 Temperature

401 Class A:
Ambient temperatures +5°C to +55°C.

402 Class B:
Ambient temperatures +5°C to +70°C.

403 Class C:
Ambient temperatures -25°C to +55°C.

404 Class D:
Ambient temperatures -25°C to +70°C.

B 500 Humidity

501 Class A:
Relative humidity up to 96% at all relevant temperatures, no condensation.

502 Class B:
Relative humidity up to 100% at all relevant temperatures.

B 600 Salt contamination

601 Salt-contaminated atmosphere up to 1 mg salt per m^3 of air, at all relevant temperatures and humidity conditions. Applicable to equipment located in open air and made of material subject to corrosion.

B 700 Oil contamination

701 Mist and droplets of fuel and lubricating oil. Oily fingers.

B 800 Vibrations

801 Class A:

Frequency range 3 to 100 Hz.
Amplitude 1 mm (peak value) below 13.2 Hz.
Acceleration amplitude 0.7 g above 13.2 Hz.

802 Class B:

Frequency range 3 to 100 Hz.
Amplitude 1.6 mm (peak value) below 25 Hz.
Acceleration amplitude 4.0 g above 25 Hz.

803 Class C:

Frequency range 3 to 50 Hz.
Amplitude 3 mm (peak value) below 13.2 Hz.
Acceleration amplitude 2.1 g above 13.2 Hz.

B 900 Inclination

901 For ships, see Rules for Classification of Ships Ch.1. For HS, LC and NSC, see Rules for Classification of HS, LC and NSC Pt.4 Ch.1 Sec.1 A200.

B 1000 Electromagnetic compatibility

1001 The minimum immunity requirements for equipment are given in Table B2, and the maximum emission requirements are given in Table B3.

Guidance note:

Electrical and electronic equipment should be designed to function without degradation or malfunction in their intended electromagnetic environment. The equipment should not adversely affect the operation of, or be adversely affected by any other equipment or systems used on board or in the vicinity of the vessel. Upon installation, it may be required to take adequate measures to minimise the electromagnetic noise signals, see Classification Note No. 45.1. Such measures may be in form of a list of electromagnetic noise generating- and sensitive equipment, and an estimate on required noise reduction, i.e. an EMC management plan. Testing may also be required to demonstrate electromagnetic compatibility.

---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

B 1100 Miscellaneous

1101 In particular applications other environmental parameters may influence the equipment, e.g.:

— acceleration
— fire
— explosive atmosphere
— temperature shock
— wind, rain, snow, ice, dust
— audible noise
— mechanical shock or bump forces equivalent to 20 g of 10 ms duration
— splash and drops of liquid
— corrosive atmospheres of various compositions, (e.g. ammonia on an ammonia carrier).

1102 Acceleration caused by the ship's movement in waves. Peak acceleration ±1.0 g for ships with length less than 90 m, and ±0.6 g for ships of greater length. Period 5 to 10 s.

Table B2 Minimum immunity requirements for equipment

Port	*Phenomenon*	*Basic Standard*	*Performance criteria*	*Test value*
A.C. power	Conducted low frequency interference	IEC 60945	A	50 - 900 Hz: 10% A.C. supply voltage 900 - 6000 Hz: 10 - 1% A.C. supply voltage 6 - 10 kHz: 1% A.C. supply voltage
	Electrical fast transient (Burst)	IEC 61000-4-4	B	2 kV [3]
	Surge voltage	IEC 61000-4-5	B	0.5 kV [1] /1 kV [2]
	Conducted radio frequency interference	IEC 61000-4-6	A	3 Vrms [3]; (10 kHz)[6] 150 kHz - 80 MHz sweep rate ≤ 1.5 x 10^{-3} decade/s [7] modulation 80% AM (1 kHz)
D.C. power	Conducted low frequency interference	IEC 60945	A	50 Hz - 10 kHz: 10% D.C. Supply voltage
	Electrical fast transient (Burst)	IEC 61000-4-4	B	2 kV [3]
	Surge voltage	IEC 61000-4-5	B	0.5 kV [1] /1 kV [2]
	Conducted radio frequency interference	IEC 61000-4-6	A	3 Vrms [3]; (10 kHz)[6] 150 kHz - 80 MHz sweep rate ≤ 1.5 x 10^{-3} decade/s [7] modulation 80% AM (1 kHz)
I/O ports, signal or control	Electrical fast transient (Burst)	IEC 61000-4-4	B	1 kV [4]
	Conducted radio frequency interference	IEC 61000-4-6	A	3 Vrms [3]; (10 kHz)[6] 150 kHz - 80 MHz sweep rate ≤ 1.5 x 10^{-3} decade/s [7] modulation 80% AM (1 kHz)
Enclosure	Electrostatic discharge (ESD)	IEC 61000-4-2	B	6 kV contact/8 kV air
	Electromagnetic field	IEC 61000-4-3	A	10 V/m[5] 80 MHz-2 GHz sweep rate ≤ 1.5 x 10^{-3} decade/s [7] modulation 80% AM (1 kHz)

1) line to line

2) line to ground

3) capacitive coupling

4) coupling clamp

5) special situations to be analysed

6) test procedure to be described in the test report

7) for equipment installed in the bridge and deck zone (EMC Class B) the test levels shall be increased to 10 Vrms for spot frequencies in accordance with IEC 60945 at 2/3/4/6.2/8.2/12.6/16.5/18.8/22/25 MHz. For screened cables, a special test set-up shall be used enabling the coupling into the cable screen.

Performance criterion A: The equipment under test (EUT) shall continue to operate as intended during and after the test. No degradation of performance or loss of function is allowed as defined in the relevant equipment standard and in the technical specification published by the manufacturer.

Performance criterion B: The EUT shall continue to operate as intended after the test. No degradation of performance or loss of function is allowed as defined in the relevant equipment standard and in the technical specification published by the manufacturer. During the test, degradation or loss of function or performance that is self recoverable is however allowed but no change of actual operating state or stored data is allowed.

Table B3 Maximum emission requirements for equipment				
Class	*Location*	*Port*	*Frequency Range (Hz)*	*Limits*
A	All locations except bridge and open deck	Enclosure (Radiated Emission)	150 k – 30 M 30 – 100 M 100 M – 2 G except: 156 – 165 M	80 – 50 dBμV/m 60 – 54 dBμV/m 54 dBμV/m 24 dBμV/m
		Power (Conducted Emission)	10 – 150 k 150 – 500 k 500 k – 30 M	120 – 69 dBμV 79 dBμV 73 dBμV
B	All locations including bridge and open deck	Enclosure (Radiated Emission)	150 – 300 k 300 k – 30 M 30 M – 2 G except: 156 – 165 M	80 – 52 dBμV/m 52 – 34 dBμV/m 54 dBμV/m 24 dBμV/m
		Power (Conducted Emission)	10 – 150 k 150 – 350 k 350 k – 30 M	96 – 50 dBμV 60 – 50 dBμV 50 dBμV

C. Electrical and Electronic Equipment

C 100 General

101 Switching of the power supply on and off shall not cause excessive voltage or other strains that may damage internal or external components.

102 Units requiring insulating resistance in cables and wiring higher than 200 kΩ are normally not to be used. Exceptions can be made for special cable arrangements.

C 200 Mechanical design, installation

Guidance note:

Circuits should be designed to prevent damage of the unit or adjacent elements by internal or external failures. No damage should occur when the signal transmission lines between measuring elements and other units are short-circuited, grounded or broken. Such failures should lead to a comparatively safe condition (fail to safe).

---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

Guidance note:

The equipment should preferably function without forced cooling. Where such cooling is necessary, precautions should be taken to prevent the equipment from being damaged in case of failure of the cooling unit.

---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

201 The components shall be effectively secured to avoid mechanical stressing of wires and soldered joints through vibrations and mechanical shock.

Guidance note:

Components weighing more than 10 grams (0.35 oz), should not be fastened by their connecting wires only.

---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

C 300 Protection provided by enclosure

301 Enclosures for the equipment shall be made of steel or other flame retardant material capable of providing EMC protection and satisfy the minimum requirements of Table C1. The required degree of protection is specified in IEC 60529 (International Electrotechnical Commission, Publication No. 60529).

Table C1 Minimum requirements for enclosures		
Class	*Location*	*Degree of protection*
A	Control rooms, accommodation, bridge	IP 20
B	Machinery space	IP 44
C	Open deck, masts, below floor plates in machinery space	IP 56
D	Submerged application	IP 68

More detailed requirements for ingress protection of enclosure types related to location are given in Ch.8 Sec.10 Table B1.

Guidance note:

Automation equipment of class A and B that shall be in operation during emergency situations, located in areas exposed to wash down, should have IP 55 protection.

---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

C 400 Cables and wires

401 Cables and wires shall comply with the requirements in Ch.8 Sec.9.

C 500 Cable installation

501 Cable installations shall comply with the requirements in Ch.8 Sec.10 and Ch.8 Sec.3 D300.

C 600 Power supply

601 When using low voltage battery supply, the charging equipment, batteries and cables shall keep the voltage at equipment terminals within +25% to -20% of the nominal voltage during charging and discharging.

Provisions shall be made for preventing reverse current from the battery through the charging device.

602 Systems including a standby battery connected for continuous charging shall not be disturbed in any way by disconnection of the battery.

603 Battery installations shall be in accordance with Ch.8 Sec.10 B300.

604 Regulated rectifiers shall be designed for the variations in voltage and frequency stated in B.

605 Different system voltages shall be supplied through different cables.

606 Terminal lists shall be clearly marked. Various system voltages shall be distinguished.

607 Uninterruptible power supplies shall be according to the requirements given in Ch.8 Sec.2 A200.

C 700 Fibre optic equipment

701 Fabrication and installation of fibre optic cables shall comply with the requirements of Ch.8.

Guidance note:

The construction of fibre optic devices is generally to comply with relevant specifications of IEC Publications.

---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

702 Power budget calculation shall be used to:

— determine the length between I/O units,
— select components to obtain a safe reliable transmission system, and
— to demonstrate that adequate power reserve has been provided.

After installation, optical time domain reflectometry (OTDR) measurements for each fibre shall be used to correct and re-evaluate the power budget calculations.

703 The safety of personnel and operations shall be considered in the installation procedures. Warning signs and labels giving information to the operators shall be placed where hazard exists. Care must be taken to prevent fibres from penetrating eyes or skin.

Guidance note:

It is advised to use equipment with 'built-in' safety, e.g. interlock the power to the light sources with the covers, possible to disconnect/lock parts of the system under service, screen laser beams.

Safe distance between the light source or fibre end and the eye of the operator may be determined by applying the formulae:

$$L_{safe} = \frac{(P_n + 10)}{2}$$

Safe distance: L (cm) ; P_n: Nominal power (mW)

---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

704 Fibre optic systems using standard single- and multimode fibres to be used for intrinsically safe circuits in hazardous areas shall have a power level below 10 mW.

SECTION 6
USER INTERFACE

A. General

A 100 Application

101 The rules in this section apply for all main class vessels.

A 200 Introduction

201 The location and design of the user interface shall give consideration to the physical capabilities of the user and comply with accepted ergonomic principles.

202 This section gives requirements for the user interface to ensure a safe and efficient operation of the systems installed.

B. Workstation Design and Arrangement

B 100 Location of visual display units and user input devices

101 Workstations shall be arranged to provide the user with easy access to UIDs, VDUs and other facilities required for the operation.

102 The VDUs and UIDs shall be arranged with due consideration of the general availability parameters as shown in Fig.1 and Fig.2.

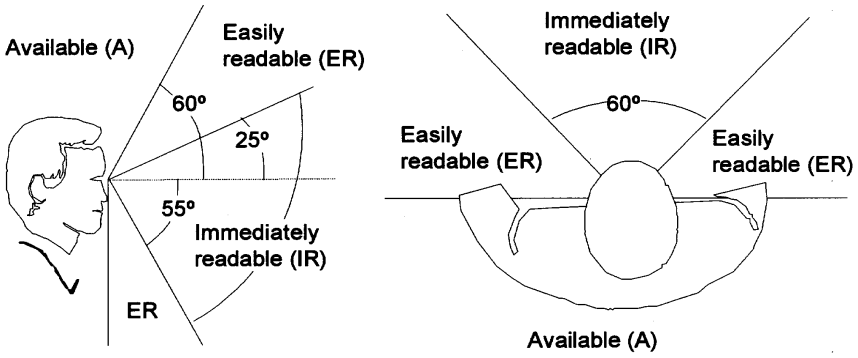

Fig. 1
VDU arrangement parameters.

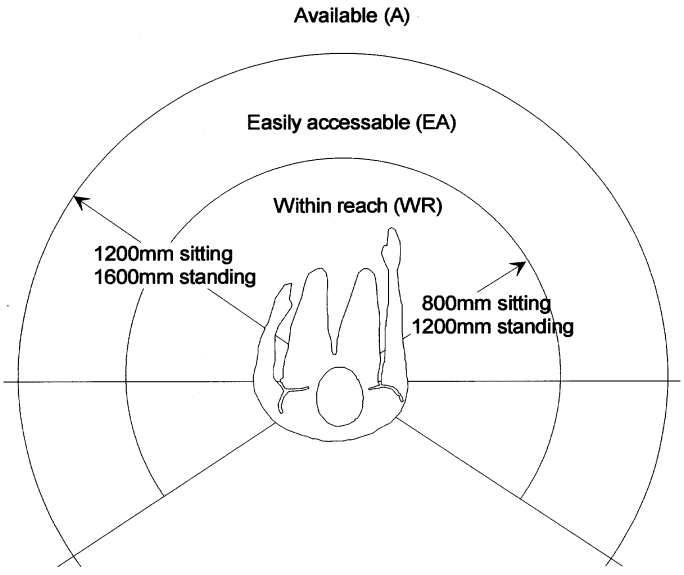

Fig. 2
UID arrangement parameters.

103 UIDs and VDUs serving the same function shall as far as possible be arranged and grouped together.

C. User Input Device and Display Unit Design

C 100 User input devices

101 The method of activating a UID shall be clear and unambiguous.

102 The direction of UID movements shall be consistent with the direction of associated process response and display movement. The purpose shall be to ensure easy and understandable operation, such as:

— a side thruster lever to be arranged athwart ships
— a propulsion thruster lever shall be arranged according to the vessel response
— the thruster response shall correspond to the lever movement.

103 The operation of a UID shall not obscure indicator elements where observation of these elements is necessary for adjustments.

104 UIDs or combined UIDs/indicating elements shall be distinguishable from elements used for indication only.

105 UIDs shall be simple to use, and shall normally allow for one hand operation. The need for fine motoric movements shall be avoided.

106 The naming, numbering and tagging for the different main components shall be consistent on the applicable VDUs, UIDs and signboards.

C 200 Visual display units

201 The information presented shall be clearly visible to the user, and permit reading at a practicable distance in the light conditions normally experienced, where installed.

202 In order to ensure readability, the update frequency of VDUs shall be consistent with the operational use of the VDU and the accuracy requirement, if any, to the data displayed.

203 VDU letter type shall be of simple, clear-cut design.

204 Set points shall always be indicated at the location of the UID.

C 300 Colours

301 The use of colours shall be consistent. Red shall be reserved to indicate danger, alarm and emergency only. Colour coding of functions and signals shall be in accordance with Table C3.

Table C3 Colour coding

Function	*Colour code*
Danger, Alarm, Emergency	Red
Attention, Pre-warning, Caution, Undefined	Yellow
Status of normal, safe situation	Green

C 400 Requirements for preservation of night vision (UIDs and VDUs for installation on the navigating bridge)

401 Warning and alarm indicators shall show no light in normal condition.

402 All UIDs and VDUs shall be fitted with internal or permanent external light source to ensure that all necessary information is visible at all times.

403 Means shall be provided to avoid light and colour changes during start-up and mode changes, which may affect night vision.

D. Screen Based Systems

D 100 General

101 The status of the information displayed shall be clearly indicated.

Guidance note:
This applies to e.g. indications not being updated or indication of inhibited alarm.

---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

102 Alarm required in the rules shall, when initiated, be given priority over any other information presented on the VDU. The entire list of alarm messages shall be easily available.

103 Alarms shall be time tagged.

104 Time tagging for all alarms shall be consistent throughout the system. The different nodes in the system shall be synchronised with sufficient accuracy to ensure consistent time tagging for all alarms throughout the system.

The accuracy of the synchronisation shall as a minimum correspond to the time constants in the process so that the true sequence of events may be traced in the alarm list.

105 For a main alarm system at least two independent VDUs shall be provided for alarm presentation, alternatively one VDU and one independent printer.

The two independent VDUs or VDU and printer shall not be driven from the same interface controller.

106 UIDs shall be designed and arranged to avoid inadvertent operation.

Guidance note:

The purpose shall prevent unintentional activation / de-activation of systems, e.g. by means of a lid over a stop button or two-step operation of critical screen-based functions.

---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

107 For essential and important systems, dedicated input devices shall be used.

Guidance note:

The input device is normally a dedicated function keyboard, but alternative arrangements like e.g. touch-screens or dedicated software-based dialogue boxes or switches may be accepted on special considerations.

---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

108 Symbols and their associated information in a mimic diagram shall have a logical relationship.

109 Means shall be provided to ensure that only correct use of numbers and letters and only values within reasonable limits will be accepted when data is entered manually into the system.

If the user provides the system with insufficient input, the system shall request the continuation of the dialogue by means of clarifying questions. Under no circumstances is the system to end the dialogue incomplete without user request.

D 200 Illumination

201 Means shall be provided for adjustment of illumination of all VDUs and UIDs to a level suitable for all applicable light conditions. However, to make adjustments down to a level making information belonging to essential and important functions unreadable is not permissible and shall be prevented.

Guidance note:

Adjustments may be arranged by use of different sets of colours suited for the applicable light conditions.

---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

D 300 Colour screens

301 For cathode ray tubes (CRTs), colours used for essential information shall not depend on a single source of light.

D 400 Computer dialogue

401 Frequently used operations shall be available in the upper menu level, on dedicated software or hardware buttons.

402 All menus and displays shall be self-explanatory or provided with appropriate help-functions.

403 When in dialogue mode, update of essential information shall not be blocked.

404 Relevant fields for entry of data shall occur with current or a default value. A valid data range shall be defined for each field.

405 The systems shall indicate the acceptance of a control action to the user without undue delay.

406 Confirmation of a command shall be used when the action requested has a critical consequence.

407 It shall be possible for the user to recognise whether the system is busy executing an operation, or waiting for additional user action. When the system is busy, buffering of more than one user input is not allowed. Manually initiated time-consuming operations shall be possible to cancel.

D 500 Application screen views

501 For integrated systems, all windows to be called to the VDU shall have a similar representation of all components (menus, buttons, symbols, colours, etc.).