RULES FOR CLASSIFICATION

Ships

Edition October 2015

Part 4 Systems and components
Chapter 9 Control and monitoring systems
FOREWORD

DNV GL rules for classification contain procedural and technical requirements related to obtaining and retaining a class certificate. The rules represent all requirements adopted by the Society as basis for classification.

© DNV GL AS October 2015

Any comments may be sent by e-mail to rules@dnvgl.com

If any person suffers loss or damage which is proved to have been caused by any negligent act or omission of DNV GL, then DNV GL shall pay compensation to such person for his proved direct loss or damage. However, the compensation shall not exceed an amount equal to ten times the fee charged for the service in question, provided that the maximum compensation shall never exceed USD 2 million.

In this provision "DNV GL" shall mean DNV GL AS, its direct and indirect owners as well as all its affiliates, subsidiaries, directors, officers, employees, agents and any other acting on behalf of DNV GL.
CHANGES – CURRENT

This is a new document.
The rules enter into force 1 January 2016.
## CONTENTS

**Changes – current**

Section 1 General Requirements

1 Classification
   1.1 Rule Applications
   1.2 Classification principles
   1.3 Software and hardware change handling
   1.4 Assumptions

2 Definitions
   2.1 General terms
   2.2 Terms related to computer based system

3 Documentation
   3.1 General

4 Tests
   4.1 General
   4.2 Verification of software development
   4.3 Integration testing
   4.4 System testing
   4.5 On-board testing

Section 2 Design principles

1 System configuration
   1.1 General
   1.2 Field instrumentation
   1.3 System
   1.4 Integrated system

2 Response to failures
   2.1 Failure detection
   2.2 System response

Section 3 System design

1 System elements
   1.1 General
   1.2 Automatic control
   1.3 Remote control
   1.4 Protective safety system


DNV GL AS
1.5 Alarms............................................................................................................ 25
1.6 Indication......................................................................................................... 27
1.7 Planning and reporting..................................................................................... 27
1.8 Calculation, simulation and decision support.................................................. 28

2 General Requirements.......................................................................................... 28
2.1 System operation and maintenance................................................................. 28
2.2 Power supply requirements for control and monitoring systems..................... 28

Section 4 Additional requirements for computer based systems............................ 30

1 General Requirements.......................................................................................... 30
1.1 Assignment of responsibility when installing integrated systems...................... 30
1.2 System dependency.......................................................................................... 30
1.3 Computer design principles............................................................................ 30
1.4 Storage devices............................................................................................... 30
1.5 Computer usage.............................................................................................. 30
1.6 System response and capacity....................................................................... 31
1.7 Temperature control....................................................................................... 31
1.8 System maintenance....................................................................................... 31
1.9 System access............................................................................................... 31

2 System software.................................................................................................. 32
2.1 Software requirements.................................................................................... 32
2.2 Software development.................................................................................... 33

3 Control system networks and data communication links.................................... 33
3.1 General........................................................................................................... 33
3.2 Network analysis............................................................................................ 35
3.3 Network test and verification......................................................................... 35
3.4 Network documentation requirements............................................................ 36
3.5 Wireless communication............................................................................... 36
3.6 Documentation of wireless communication.................................................... 37

Section 5 Component design and installation......................................................... 38

1 General............................................................................................................. 38
1.1 Environmental strains.................................................................................... 38
1.2 Materials........................................................................................................ 38
1.3 Component design and installation................................................................. 38
1.4 Maintenance, checking................................................................................... 39
1.5 Marking........................................................................................................... 39
1.6 Standardising.................................................................................................. 39

2 Environmental conditions, instrumentation.......................................................... 39
2.1 General ................................................................................................................. 39
2.2 Electric power supply ............................................................................................ 40
2.3 Pneumatic and hydraulic power supply .................................................................. 41
2.4 Temperature .............................................................................................................. 41
2.5 Humidity .................................................................................................................... 41
2.6 Salt contamination .................................................................................................... 41
2.7 Oil contamination .................................................................................................... 41
2.8 Vibrations ............................................................................................................... 41
2.9 Inclination .................................................................................................................. 42
2.10 Electromagnetic compatibility ................................................................................. 42
2.11 Miscellaneous ......................................................................................................... 42

3 Electrical and electronic equipment .......................................................................... 44
3.1 General ....................................................................................................................... 44
3.2 Mechanical design, installation ............................................................................... 44
3.3 Protection provided by enclosure .............................................................................. 45
3.4 Cables and wires ........................................................................................................ 45
3.5 Cable installation ....................................................................................................... 45
3.6 Power supply ............................................................................................................ 45
3.7 Fibre optic equipment ............................................................................................... 46

Section 6 User interface .................................................................................................. 47

1 General ......................................................................................................................... 47
1.1 Application .................................................................................................................. 47
1.2 Introduction ................................................................................................................ 47

2 Workstation design and arrangement ........................................................................... 47
2.1 Location of visual display units (VDU) and user input devices (UID) ...................... 47

3 User input device and visual display unit design .......................................................... 48
3.1 User input devices (UID) ......................................................................................... 48
3.2 Visual display units (VDU) ....................................................................................... 49
3.3 Colours ...................................................................................................................... 49
3.4 Requirements for preservation of night vision (UIDs and VDUs for installation on the navigating bridge) ......................................................... 49

4 Screen based systems ................................................................................................ 50
4.1 General ....................................................................................................................... 50
4.2 Computer dialogue .................................................................................................... 50
4.3 Application screen views .......................................................................................... 51
SECTION 1 GENERAL REQUIREMENTS

1 Classification

1.1 Rule Applications

1.1.1 The requirements of this section apply to all control and monitoring systems required by the rules. Guidance note:
Additional requirements for specific applications may be given under rules governing those applications.
---e-n-d---of---g-u-i-d-a-n-c-e---n-o-t-e---

1.1.2 All control and monitoring systems installed, but not necessarily required by the rules, that may have an impact on the safety of main functions (see Pt.1 Ch.1 Sec.1 [1.2]), shall meet the requirements of this section.

1.2 Classification principles

1.2.1 Control and monitoring systems belong to three different system categories as shown in Table 1 in accordance with the possible consequence a failure may inflict on the vessels manoeuvrability in regard to propulsion and steering, refer to Ch.8 Sec.13.

Table 1 System categories

<table>
<thead>
<tr>
<th>Service</th>
<th>Effects upon failure</th>
<th>System functionality</th>
</tr>
</thead>
<tbody>
<tr>
<td>Non-important</td>
<td>Failure of which will not lead to dangerous situations for human safety, safety of the vessel and/or threat to the environment</td>
<td>Monitoring function for informational / administrative tasks</td>
</tr>
<tr>
<td>Important</td>
<td>Failure could eventually lead to dangerous situations for human safety, safety of the vessel and/or threat to the environment</td>
<td>— Alarm and monitoring functions</td>
</tr>
<tr>
<td></td>
<td></td>
<td>— Control functions which are necessary to maintain the ship in its normal operational and habitable conditions</td>
</tr>
<tr>
<td>Essential services and safety functions</td>
<td>Failure could immediately lead to dangerous situations for human safety, safety of the vessel and/or threat to the environment</td>
<td>— Control functions for maintaining the vessel’s propulsion and steering</td>
</tr>
<tr>
<td></td>
<td></td>
<td>— Safety functions</td>
</tr>
</tbody>
</table>

Guidance note:
The machinery arrangement and eventual system redundancy, eventual additional notations and possible means for alternative back-up control beyond main class may affect the system category. See IACS UR E22.
---e-n-d---of---g-u-i-d-a-n-c-e---n-o-t-e---

1.2.2 Classification of control and monitoring systems shall be according to the following principles:
— type approval (see [1.2.5])
— 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 Class Guidelines DNVGL-CG-0338 and DNVGL-CG-0339.

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

1.2.3 Essential and important control, monitoring and safety systems, as specified in the rules, shall be provided with a product certificate unless exemption is given in a Society issued Type Approval Certificate or the logic is simple and the failure mechanisms are easily understood.

The certification procedure consists of:

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

1.2.4 In general, the required certification of control and monitoring systems are given in the various application rules.

Guidance note:
The following list gives an extract of the certification requirements given in the application rules.
The list is for guidance only, refer to the applicable parts of the rules for exact requirements:

Pt.3 Ch.1 Sec.3: internal water tight doors and shell doors
Ch.1 Sec.1 Table 3: propulsion control and monitoring
Ch.3 Sec.1 Table 7: reciprocating internal combustion engines:
  — alarm and monitoring
  — safety
  — speed control / governor
Ch.3 Sec.2: gas turbines:
  — alarm and monitoring
  — safety
  — speed control / governor
Ch.3 Sec.3 Table 2: Steam turbines:
  — alarm and monitoring
  — safety
  — speed control / governor
Ch.5 Sec.1 Table 2: propeller pitch
Ch.5 Sec.2 Table 2: water jets
Ch.5 Sec.3 Table 3: podded and geared thrusters for propulsion and dynamic positioning
Ch.6 Sec.1 Table 5: exhaust cleaning for NO\textsubscript{X} and SO\textsubscript{X}
Ch.6 Sec.6 [1.3.1]: refrigeration
Ch.7 Sec.1 Table 9: boilers, thermal-oil installations, oil fired water heaters,
Ch.8 Sec.1 Table 3: power management
  Table 2:
  — main alarm system
  — integrated control and monitoring
  — safety management systems and decision support systems
Part 4 Chapter 9 Section 1

Table 2 Certification required for control systems – additional to specific required certification given in other sections of the rules

<table>
<thead>
<tr>
<th>Object</th>
<th>Certificate type</th>
<th>Issued by</th>
<th>Certification standard</th>
<th>Additional description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Main alarm system</td>
<td>PC</td>
<td>Society</td>
<td>(N/A)</td>
<td></td>
</tr>
<tr>
<td>Integrated control and monitoring system</td>
<td>PC</td>
<td>Society</td>
<td>(N/A)</td>
<td></td>
</tr>
<tr>
<td>Safety management systems and decision support systems</td>
<td>PC</td>
<td>Society</td>
<td>(N/A)</td>
<td>where such systems interface the control, monitoring and safety systems required by the rules</td>
</tr>
</tbody>
</table>

Guidance note:
For a definition of the certificate types, see Pt.1 Ch.3.

Guidance note:
A Safety management system may be a separate system providing an integrated user interface for various safety related systems, e.g. emergency shutdown systems, watertight doors, fire detection etc. The Safety management system normally provides user interface that are supplementary / additional to mandatory user interface required by the rules and regulations.
A decision support system is a system providing manual or automatic support to the operator based on logical functions and algorithms with input from the various control and monitoring systems.

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

1.2.5 In addition to [1.2.4], the control and monitoring systems listed in Table 2 shall be certified, if fitted.
1.2.6 The main components for essential and important control, monitoring and safety systems covered by the rules of this section (see [1.2.4] guidance note) shall be type approved.

**Guidance note:**
The requirement normally applies to the following components:
- Controllers, PLC’s
- I/O cards, communication cards
- Operator stations, computers
- Network switches, routers, firewalls
- Other components that may be essential for the control system functionality

Case by case approval of the components may, based on suitable documentation, be accepted as an alternative to the type approval.

Refer to IACS UR (E22, M3, M29, M44, M67) for type approval or documented evidence of compliance according to E10

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

1.3 Software and hardware change handling

1.3.1 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.

1.3.2 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.

1.3.3 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.

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

1.3.5 A procedure for how to handle changes like corrections, modifications, upgrades) in both basic- and application software shall be submitted for approval when requested. The procedure shall describe how to ensure traceability in the software change handling process for any changes that may be done after the certification of the system. The procedure shall cover the necessary steps to ensure compliance with at least the following principles:

- major modifications which may affect compliance with the rules shall be described and submitted to the society for evaluation before the change is implemented on-board
- 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 including the objective and reason for the change, description, authorisation, test record, signatures, date, and new incremented SW revision no shall be documented.
- 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.

1.3.6 If the control system is intended for remote software maintenance, i.e. from outside the vessel, the functionality shall be part of the system documentation as required in Table 5. The following requirements apply supplementary to [1.3.5], and shall be part of the procedure required in [1.3.5]:

- 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 realtime 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.

1.4 Assumptions

1.4.1 The rules of this section 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.

2 Definitions

2.1 General terms

Table 3 Definitions – General terms

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alarm</td>
<td>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.</td>
</tr>
<tr>
<td>Back-up control systems</td>
<td>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)</td>
</tr>
</tbody>
</table>
| Control and monitoring system       | includes all components necessary for control and monitoring, including sensors and actuators. In this section, 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. |
| 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. See 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. |
| 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. |
### Essential control and monitoring system

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 sections. (hereafter called essential system)

**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.

---end---of---guidance---note---

### 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.

### Important control and monitoring system

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 vessel's functions as defined in Pt.1 Ch.1 Sec.1 [1.2] 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 sections. (hereafter called important system)

### Independent systems

See Sec.2 [1.2.1].

### Integrated system

A combination of computer-based systems which are interconnected in order to allow common access to sensor information and/or command and control.

In the context of class, an integrated system contains control, monitoring, alarm or safety functions for multiple vessel services in a topology of controllers and operator stations communicating via networks and/or communication links.

### Manufacturing survey of control and monitoring systems

Inspection and verification of performance (normal, abnormal and degraded operation) according to functional requirements based on approved test programmes and to verify compliance with the rules including requirements software development.

### 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.

---end---of---guidance---note---

### Non-important control and monitoring systems

Are systems supporting functions for which the Society has no requirements according to relevant definitions in the rules. (hereafter called non-important systems)

### Operator station

In an integrated system is a unit consisting of a user interface, i.e. UIDs and VDU, and interface controller(s).

### Process segment

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.
### 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.

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

### 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)

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

### 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.

## 2.2 Terms related to computer based system

### Table 4 Definitions – terms related to computer based systems

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application software</td>
<td>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.</td>
</tr>
<tr>
<td>Basic software</td>
<td>is the software necessary for the hardware to support the application software.</td>
</tr>
<tr>
<td><strong>Guidance note:</strong></td>
<td>Basic software normally includes the operating system and additional general software necessary to support the general application software and project application software.</td>
</tr>
<tr>
<td></td>
<td>---e-n-d---of---g-u-i-d-a-n-c-e---n-o-t-e---</td>
</tr>
<tr>
<td>Computer task</td>
<td>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</td>
</tr>
<tr>
<td>Data communication links</td>
<td>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.</td>
</tr>
<tr>
<td><strong>Guidance note:</strong></td>
<td>For local area networks, this includes network controllers, network transducers, the cables and the network software on all nodes.</td>
</tr>
<tr>
<td></td>
<td>---e-n-d---of---g-u-i-d-a-n-c-e---n-o-t-e---</td>
</tr>
<tr>
<td>Hardware</td>
<td>in the context of control and monitoring systems, <em>hardware</em> is the collection of physical elements that comprise the control and monitoring system</td>
</tr>
<tr>
<td>A Node in a network</td>
<td>is a processing location and can be a computer or other device, such as a printer. Every node has a unique network address.</td>
</tr>
<tr>
<td>Software module</td>
<td>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.</td>
</tr>
<tr>
<td>SW manufacturer</td>
<td>is a manufacturer of equipment/systems in which programmable electronic systems are a component in the delivery</td>
</tr>
</tbody>
</table>
### 3 Documentation

#### 3.1 General

**3.1.1** Documentation requirements for control and monitoring systems shall be submitted as specified in Table 5 and in the various application rules. See listed functions below, referring to the respective parts and sections of the rules.

**Guidance note:**
Documentation for control and monitoring systems found in the respective parts of the rules. Note that documentation requirements for the voluntary notations in Pt.6 are not listed here.

- Pt.3 Ch.3: Water tight doors, side and stern doors, water leakage monitoring. (Rules for Classification of Ships)
- Ch.1: Propulsion remote control system
- Ch.3: Main and auxiliary engines, gas turbines, steam turbines.
- Ch.4: Shafting, clutches/elastic couplings.
- Ch.5: Propeller/water jets, thrusters.
- Ch.6: Valves and pumps, remote control. (Rules for Classification of Ships)
- Ch.7: Boilers, thermal-oil installations, incinerators, oil fired water heaters.
- Ch.8: Power management system
- RU SHIP Pt.4 Ch.9: Remote control of vessel main functions, main alarm system, integrated control and monitoring system, engineers’ alarm
- Ch.10: Steering gear
- Pt.5 Ch.1: Bow doors monitoring, fire doors, water ingress detection system, ventilation, container refrigerating. (Rules for Classification of Ships)
- Pt.5 Ch.5: 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.6: 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.7: 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---

**3.1.2** In addition to [3.1.1], documentation for the control and monitoring systems listed in Table 5 shall be submitted for approval.

<table>
<thead>
<tr>
<th>User input device (UID)</th>
<th>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.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Visual display unit (VDU)</td>
<td>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).</td>
</tr>
</tbody>
</table>
Table 5 Documentation requirements

<table>
<thead>
<tr>
<th>Object</th>
<th>Documentation type</th>
<th>Additional description</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>Main alarm system</td>
<td>I200 - Control and monitoring system documentation</td>
<td></td>
<td>AP</td>
</tr>
<tr>
<td>Integrated control and monitoring system</td>
<td>I200 - Control and monitoring system documentation</td>
<td>Refer to</td>
<td>AP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>— Sec.2 [1.4], Integrated system arrangement</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>— Sec.4 [3.3] and Sec.4 [3.4] and Network analysis</td>
<td></td>
</tr>
<tr>
<td>Integrated control and monitoring system</td>
<td>Z070 – Functional Failure Analysis</td>
<td></td>
<td>AP</td>
</tr>
<tr>
<td>Engineers alarm</td>
<td>I200 - Control and monitoring system documentation</td>
<td></td>
<td>AP</td>
</tr>
<tr>
<td>Safety management system</td>
<td>I200 - Control and monitoring system documentation</td>
<td>See guidance note under Table 2</td>
<td>AP</td>
</tr>
<tr>
<td>Decision support system</td>
<td>I200 - Control and monitoring system documentation</td>
<td>See guidance note under Table 2</td>
<td>AP</td>
</tr>
</tbody>
</table>

3.1.3 The documentation package for all control and monitoring systems shall contain information as defined for documentation type I200, refer to Pt.1 Ch.3 for description of the contents. Where additional documentation is required, this is specified in the application rules.

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

---e-n-d---o-f---g-u-i-d-a-n-c-e---n-o-t-e---

3.1.4 For systems subject to certification, documentation listed in Table 6 shall be presented for the surveyor prior to the manufacturing survey.

3.1.5 For on-board tests and inspections, documentation listed in Table 7 shall be submitted to the local survey station for approval.

Guidance note:
The test program(s) is normally developed by the yard and contains relevant tests for all control and monitoring systems installed on board. The test program is normally based on input from the various system manufacturers.

---e-n-d---o-f---g-u-i-d-a-n-c-e---n-o-t-e---

3.1.6 Operation manual (Z161) and a maintenance manual (Z163) for the control systems shall be kept on-board.

3.1.7 For type approved components or systems, the type approval certificate contains a list of documentation that shall be submitted for (case-by-case) approval.

Guidance note:
The documentation package I200 should contain a reference to type approval certificates relevant for the control and monitoring systems in the scope of delivery.

---e-n-d---o-f---g-u-i-d-a-n-c-e---n-o-t-e---
### Table 6 Documentation required for the manufacturing survey

<table>
<thead>
<tr>
<th>Documentation type</th>
<th>Definition</th>
</tr>
</thead>
</table>
| I140 - Software quality plan | The software life cycle activities shall minimum contain procedures for:  
  - software requirements specification  
  - parameters data requirements  
  - software function  
  - test  
  - parameter data test  
  - validation testing  
  - traceability of system project files  
  - software change handling and revision control |
| Z161 - Operation manual | 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. |
| Z162 - Installation manual | A document providing information about the installation procedures. |
| Z163 - Maintenance manual | A document intended for regular use on board providing information about:  
  - maintenance instructions  
  - acceptance criteria  
  - fault identification and repair  
  - list of the suppliers’ service net. |

### Table 7 Documentation required for on-board inspection

<table>
<thead>
<tr>
<th>Object</th>
<th>Documentation type</th>
<th>Additional description</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vessel control and monitoring systems</td>
<td>Z253 - Test procedure for quay and sea trial</td>
<td>Typically submitted by the yard. To be approved by the local station. Contain relevant tests for all control systems covered by class.</td>
<td>AP</td>
</tr>
</tbody>
</table>
4 Tests

4.1 General

4.1.1 All tests shall be according to test programs approved by the Society. The manufacturing survey according to [4.3] and [4.4] shall be performed by a Society surveyor. The verification of the software development process according to [4.2] shall be part of the survey.

4.1.2 For control and monitoring systems that are considered particularly complex; or prototypes or not proven in use in Society classed vessels, the manufacturing survey may be extended.

4.1.3 The control and monitoring system shall as far as practicable be completed prior to the manufacturing survey, and the manufacturer shall perform sufficient internal testing covering also the scope of the approved test program to ensure that the control system is mature and ready for the certification.

4.1.4 The following shall be evaluated during test of computer based systems:
— tools for system set-up and configuration of the EUC
— implementation of software quality plan, see also Sec.4 [2.2].

4.1.5 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.

4.1.6 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.

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

4.2 Verification of software development

4.2.1 Evidence of the development process for the application software shall be made available by the control system manufacturer and be presented upon request for the surveyor during the manufacturing survey, (refer to the software quality plan in documentation requirements Table 6).

Guidance note:
The evidence of the development process for the application software will typically be in the form of documentation covering at least the following elements of information for the specific control system delivery:
— software requirements specification
— parameters data requirements
— software function test
— parameter data test
— validation testing
— system project files stored at the manufacturer

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

Guidance note:
In addition the procedure for software change handling is an element in the development process, refer to [1.3.5].

---e-n-d---of---g-u-i-d-a-n-c-e---n-o-t-e---
4.3 Integration testing

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

4.3.2 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---o-f---g-u-i-d-a-n-c-e---n-o-t-e---

4.4 System testing

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

4.4.2 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---o-f---g-u-i-d-a-n-c-e---n-o-t-e---

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

4.5 On-board testing

4.5.1 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.

4.5.2 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.
4.5.3 The test program for harbour and sea trials shall be approved by the local Society station.

4.5.4 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.

4.5.5 If the propulsion system is designed for different modes of operation, the test described in [4.5.4] shall be run for each relevant mode of operation.

**Guidance note:**
This applies to e.g. dual fuel engines or combinations of gas and diesel engines, propulsion arrangements with PTI/PTO (power take in/-out), hybrid systems with combinations of different principles for providing propulsion power etc.

---e-n-d---of---g-u-i-d-a-n-c-e---n-o-t-e---
SECTION 2 DESIGN PRINCIPLES

1 System configuration

1.1 General

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

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

1.2 Field instrumentation

1.2.1 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---

1.2.2 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.

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

1.2.4 Electronic governors shall have their power supply independent of other consumers and the governor including its power supplies shall be 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---

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

1.3 System

1.3.1 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.
1.4 Integrated system

1.4.1 An integrated system shall be arranged with sufficient redundancy and/or segregation so as to prevent loss of control, monitoring or alarm functions for multiple main functions upon a single failure.

1.4.2 If safety functions required by the rules are implemented in an integrated system, these shall be implemented in dedicated and autonomous hardware units. Communication to other parts of the integrated system shall be secured in accordance with Sec.4 [3] to ensure integrity of the safety functions.

1.4.3 Functions in an integrated system shall be arranged in accordance with any redundancy requirements applicable for the equipment or system being served.

1.4.4 Functions for cargo and ship handling systems shall be mutually independent of hardware units used for- or supporting essential vessel functions.

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

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

   Guidance note:
   Note the requirement for operator interface for each network segment in Sec.4 [3.1.2].

1.4.6 For integrated systems, compliance with the above requirements shall be documented in a functional failure analysis (Z070), see Sec.1 Table 5.

2 Response to failures

2.1 Failure detection

2.1.1 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.

2.1.2 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.
2.2 System response

2.2.1 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.

---end-of-guidance-note---

2.2.2 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 should not lead to a downtime that may jeopardize the time response of the activation of a critical function, like e.g. a shutdown.

---end-of-guidance-note---
SECTION 3 SYSTEM DESIGN

1 System elements

1.1 General

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

1.1.2 System elements belong to the following categories:
- automatic control
- remote control
- alarm
- protective safety
- indications
- planning and reporting
- calculation, simulation and decision support.

1.1.3 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.

---end---of---guidance---note---

1.2 Automatic control

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

1.2.2 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.

1.2.3 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.
1.2.4 In closed loop systems, feedback failures shall initiate an alarm, and the system shall enter the least critical of possible new conditions. This implies the system to either remain in its present state or move controlled to “zero” state.

1.2.5 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.

1.3 Remote control

1.3.1 At the remote workstation being in command, the user shall receive continuous information on the effects of the orders given.

1.3.2 One workstation shall be designated as the main workstation.

Guidance note:
A workstation may consist of multiple operator stations.

---e-n-d---o-f---g-u-i-d-a-n-c-e---n-o-t-e---

1.3.3 When control is possible from several workstations, only one workstation shall be in control at any one time.

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

1.3.5 The main workstation shall be able to take control without acknowledgement, but an audible warning shall be given at the workstation that relinquishes control. Audible warning is not required if the stations are located in close proximity allowing visual and audible contact. The action for taking control shall not be the same as the normal control action.

1.3.6 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.

1.3.7 It shall be indicated at each alternative workstation, which control station that holds the command rights.

1.3.8 Safety interlocks in different parts of the systems shall not conflict with each other. Basic safety interlocks shall 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---o-f---g-u-i-d-a-n-c-e---n-o-t-e---

1.4 Protective safety system

1.4.1 A protective safety system shall be designed so that failures result in the least critical of any possible new states (fail safe) considering the safety of the vessel versus the safety of the machinery.

Guidance note 1:
The ‘Safety of the vessel’ denotes the need to maintain operation of the essential functions. The requirement implies that for each probable failure in the protective safety system including its loops, the system should be designed to minimize the consequences, evaluating the need to maintain operation versus the risk of causing unacceptable hazard due to breakdown of the machinery. In
this respect, the risk of continuing operation without the safety function and the possibility for manual supervision and intervention should be considered.

---end---of---guidance---note---

1.4.2 Safety systems for essential vessel services shall be designed according to a "fail-to-maintain" principle in order to prevent loss of essential services upon failures. Adequate self-diagnostics (e.g. loop monitoring) shall be implemented to distinguish between a failure in the loop and an alarm condition in the machinery/process.

Guidance note:
For essential systems that have a stopped unit as its fail-to-safe principle (e.g. one engine in a multiple engine plant), loop monitoring need not be arranged.

---end---of---guidance---note---

1.4.3 Any required protective safety system shall be arranged so that failures rendering the safety function out of operation are detected and alarmed.

1.4.4 A protective safety systems shall be arranged so that the automatic safety actions do not depend on the network communication. This applies also where the safety system is part of an integrated system.

1.4.5 Protective safety actions shall give alarm at predefined workstations.

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

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

1.4.8 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.

1.4.9 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.

1.4.10 An alarm shall be activated prior to a protective safety action, except for failure conditions where a protective safety action is required within a short time in order to prevent total failure of the component (e.g. overspeed shutdown of a diesel engine).

Guidance note:
When two or more protective safety actions are initiated by one failure condition (see [1.4.9]), the initial alarm for the failure condition (e.g. low lubricating oil pressure alarm) will cover the requirement for prior alarm for all subsequent protective safety actions for the same failure condition.

For pre-warning of slowdown or shutdown of the propulsion machinery to the navigation officers on bridge (SOLAS Ch. II-1/31.2.10), see Ch.1 Sec.4 [1.4.8].

---end---of---guidance---note---

1.5 Alarms

1.5.1 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.
1.5.2 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.

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

1.5.4 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.

1.5.5 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 workstation located outside the machinery space.

**Guidance note:**
Alarm lists should be available on any workstation.

1.5.6 Alarms shall be announced 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 that have been acknowledged.

In case the alarms are presented on a screen, the most recent alarm shall always be displayed, and only visible alarms may be acknowledged.

Where different alarms are combined in a group alarm, it shall be possible to identify the individual alarms initiating the group alarm.

**Guidance note:**
The individual alarms in an alarm group may be identified on a local panel.
1.5.7 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.

1.5.8 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.

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

1.5.10 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.

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

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

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

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

1.6 Indication

1.6.1 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-o-f-g-u-i-d-a-n-c-e-n-o-t-e---

1.6.2 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.

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

1.7 Planning and reporting

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

---e-n-d-o-f-g-u-i-d-a-n-c-e-n-o-t-e---

1.7.1 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-o-f-g-u-i-d-a-n-c-e-n-o-t-e---
1.8 Calculation, simulation and decision support

1.8.1 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.

---end of guidance note---

2 General Requirements

2.1 System operation and maintenance

2.1.1 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.

2.1.2 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.

---end of guidance note---

2.2 Power supply requirements for control and monitoring systems

2.2.1 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 [1.1.1] and Ch.8 Sec.2 [6.3].

2.2.2 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 is feeding both systems.

---end of guidance note---

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

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

2.2.5 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 1.

2.2.6 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 workstations.
SECTION 4 ADDITIONAL REQUIREMENTS FOR COMPUTER BASED SYSTEMS

1 General Requirements

1.1 Assignment of responsibility when installing integrated systems

1.1.1 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.

---end---of---guidance---note---

1.2 System dependency

1.2.1 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.

1.3 Computer design principles

1.3.1 The controllers on the process level in a computer based system shall have deterministic response time and be provided with sufficient self-diagnostic properties to ensure a fail-to-safe behaviour.

Guidance note:
This normally excludes the use of Commercial Off The Shelf (COTS) computers running on general purpose operating systems as process- or safety controllers.

---end---of---guidance---note---

1.4 Storage devices

1.4.1 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.

---end---of---guidance---note---

1.4.2 Software and data necessary to ensure satisfactory performance of essential and important functions shall be stored in non-volatile memory.

1.5 Computer usage

1.5.1 Computers serving essential and important functions shall only be used for purposes relevant to vessel operation.
1.6 System response and capacity

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

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

<table>
<thead>
<tr>
<th>Description</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data sampling for automatic control purposes (fast changing parameters)</td>
<td>0.1 s</td>
</tr>
<tr>
<td>Data sampling, indications for analogue remote controls (fast changing parameters)</td>
<td>0.1 s</td>
</tr>
<tr>
<td>Other indications</td>
<td>1 s</td>
</tr>
<tr>
<td>Alarm presentations</td>
<td>2 s</td>
</tr>
<tr>
<td>Display of fully updated screen views</td>
<td>2 s</td>
</tr>
<tr>
<td>Display of fully updated screen views including start of new application</td>
<td>5 s</td>
</tr>
</tbody>
</table>

1.6.2 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.

1.6.3 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.

1.7 Temperature control

1.7.1 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.

1.8 System maintenance

1.8.1 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.

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

1.9 System access

1.9.1 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
Control and monitoring systems

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

1.9.2 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 [1.3].

2 System software

2.1 Software requirements

2.1.1 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.

2.1.2 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.

2.1.3 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.

2.1.4 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.

2.1.5 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 shall be notified if such actions cannot be avoided.

2.1.6 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.
— 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.
2.2 Software development

2.2.1 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 are 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.

2.2.2 The actions taken to comply with [2.2.1] shall be documented and implemented, and the execution of these actions shall be retractable. 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.

2.2.3 When novel software is developed for essential systems, DNVGL Approval of the manufacturer may be required, either prior to or as part of the actual product development.

3 Control system networks and data communication links

3.1 General

3.1.1 Any network integrating control and/or monitoring systems shall be single point of failure-tolerant or alternatively designed so that the effect of a single failure does not exceed the principles given in Sec.2 [1.4.1]. This implies that the network with its necessary components and cables shall be designed with adequate redundancy.

Guidance note:
The fault tolerance should be documented specifically see [3.2] and [3.4]. 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.

3.1.2 The integrity and autonomy of each network segment within an integrated system shall be secured with appropriate network components, e.g. firewalls 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.
3.1.3 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 have properties to monitor its 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.

---end---of---guidance---note---

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

3.1.5 Cables and network components belonging to redundant networks shall be arranged to support the single fault tolerance required by [3.1.1].

Guidance note:
This implies that cables and network components belonging to redundant networks as far as practicable should 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.

---end---of---guidance---note---

3.1.6 It shall be possible to maintain local control of machinery as required by Ch.1 Sec.4 [1.1.3] 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:
When applicable should be demonstrated during sea-trial.

---end---of---guidance---note---

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

Guidance note:
The "pre-defined time" should as a minimum correspond to the time constants in the EUC, which implies that the detection and alarming is initiated quickly enough to enable appropriate operator intervention to secure the operation of the EUC.

---end---of---guidance---note---

3.1.8 If the automation system is connected to administrative networks, the connection principle shall ensure that any function or failure in the administrative net cannot 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.

---end---of---guidance---note---

3.1.9 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.

Guidance note:
Upon special consideration and agreement, additional functions may be accepted as part of the network if sufficiently analysed, documented and tested.

---end---of---guidance---note---
3.1.10 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 pertains 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.

---end of guidance note---

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

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

3.1.13 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.

---end of guidance note---

3.1.14 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 [1.3] for software change handling requirements.

Guidance note:
Any remote access to the control system should 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.

---end of guidance note---

3.1.15 The data stream serving a CCTV system (Closed Circuit Television) and other bandwidth-intensive applications shall not be part of the network in a control system covered by the rules, unless sufficient integrity can be documented in a network analysis.

3.2 Network analysis

3.2.1 The control and monitoring network with its components, connected nodes, communication links (also external interfaces) shall be subject to a failure 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 would be to 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 should 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.

---end of guidance note---
3.3 Network test and verification

3.3.1 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 functional failure analysis
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:
Item 6 is to verify that essential vessel functions are still available after e.g. a fire in a single cabinet / cubicle.

---end---of---guidance---note---

3.4 Network documentation requirements

3.4.1 For integrated systems, the network analysis ([3.2]) including a procedure for the test and verification ([3.3]) shall be submitted for approval as part of the functional failure analysis (Z070), see Sec.1 Table 5.

3.5 Wireless communication

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

3.5.2 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 (Industrial, scientific and Medical) 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.

---end---of---guidance---note---

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

Guidance note:
The ISM bands are located at 900 MHz (902-928 MHz), 2.4 GHz (2400-2483.5 MHz) and 5.8 GHz (5725-5850 MHz).

---end---of---guidance---note---

3.5.4 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.

---end---of---guidance---note---
3.5.5 The wireless system shall entail a fixed topology and support prevention of unauthorised access to the network.

**Guidance note:**
The access to the network should be restricted to a defined set of nodes with dedicated media access control (MAC) addresses.

---end-of-guidance-note---

3.5.6 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.

3.5.7 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.

---end-of-guidance-note---

3.5.8 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.

---end-of-guidance-note---

3.5.9 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.

---end-of-guidance-note---

3.6 Documentation of wireless communication

3.6.1 The following information related to the wireless communication shall be included in the documentation submitted for approval, see Sec.1 Table 5:

— 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

1 General

1.1 Environmental strains

1.1.1 Instrumentation equipment shall be suitable for marine use, and shall be designed to operate under environmental conditions as described in [2], unless means are provided to ascertain that the equipment parameters are not exceeded. These means are subject to approval on case-by-case basis.

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

1.1.3 Performance and environmental testing to ascertain the suitability of the equipment shall be provided upon request.

1.2 Materials

1.2.1 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---o-f---g-u-i-d-a-n-c-e---n-o-t-e---

1.3 Component design and installation

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

1.3.2 Vibration resonances with amplification greater than 10 should not occur. Amplification greater than 10 may be accepted based on case-by-case evaluation for equipment designed for high vibrations.

1.3.3 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.

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

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

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

1.3.7 The installation of temperature sensors shall permit easy dismantling for functional testing.
1.3.8 Clamps used to secure capillary tubes shall be made of a material that is softer than the tubing.

1.4 Maintenance, checking

1.4.1 Maintenance, repair and performance tests of systems and components shall 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---o-f---g-u-i-d-a-n-c-e---n-o-t-e---

1.5 Marking

1.5.1 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 [5].

**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---o-f---g-u-i-d-a-n-c-e---n-o-t-e---

1.6 Standardising

**Guidance note:**
Systems, components and signals should be standardised as far as practicable.

---e-n-d---o-f---g-u-i-d-a-n-c-e---n-o-t-e---

2 Environmental conditions, instrumentation

2.1 General

2.1.1 The environmental parameters given in [2.2] to [2.11], 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 shall be considered.

**Table 1 Parameter class for the different locations on board**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Class</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Temperature</td>
<td>A</td>
<td>Machinery spaces, control rooms, accommodation, bridge</td>
</tr>
<tr>
<td></td>
<td>B</td>
<td>Inside cabinets, desks. etc. with temperature rise of 5°C or more installed in location A</td>
</tr>
</tbody>
</table>
Components and systems designed in compliance with IEC environmental specifications for ships 60092-504 (1994), and for EMC 60533, may be accepted after consideration.

Guidance note:
Refer to IACS UR E10.
For details on environmental conditions for instrumentation, see Standard for Certification 2.4.
For Navigation and radio equipment IEC 60945, Marine navigational equipment - General requirements, is applicable.
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 the IEC 60945 (2002) Clause 9 (covered by EMC class B) is applicable.

---e-n-d---o-f---g-u-i-d-a-n-c-e---n-o-t-e---

2.2 Electric power supply

2.2.1 Power supply failure with successive power breaks with full power between breaks.
— 3 interruptions during 5 minutes
— switching-off time 30 s each case.

2.2.2 Power supply variations for equipment connected to A.C. systems:
— combination of permanent frequency variations of ±5% and permanent voltage variations of +6% and -10% of nominal
— combination of frequency transients (5 s duration) ±10% of nominal and voltage transients (1.5 s duration) ±20% of nominal.

2.2.3 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%.

2.2.4 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.

2.3 Pneumatic and hydraulic power supply

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

2.4 Temperature

Table 2 Ambient temperature range and associated test temperatures

<table>
<thead>
<tr>
<th>Class</th>
<th>Ambient temperatures</th>
<th>Test temperatures</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>0°C to +45°C</td>
<td>+5°C and +55°C</td>
</tr>
<tr>
<td>B</td>
<td>0°C to +55°C</td>
<td>+5°C and +70°C</td>
</tr>
<tr>
<td>C</td>
<td>-25°C to +45°C</td>
<td>-25°C and +55°C</td>
</tr>
<tr>
<td>D</td>
<td>-25°C to +55°C</td>
<td>-25°C and +70°C</td>
</tr>
</tbody>
</table>

2.5 Humidity

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

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

2.6 Salt contamination

2.6.1 Salt-contaminated atmosphere up to 1 mg salt per m³ of air, at all relevant temperatures and humidity conditions. Applicable to equipment located in open air and made of material subject to corrosion.

2.7 Oil contamination

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

2.8 Vibrations

2.8.1 Class A:
— Frequency range 2 to 100 Hz.
— Amplitude 1 mm (peak value) below 13.2 Hz.
— Acceleration amplitude 0.7 g above 13.2 Hz.

2.8.2 Class B:
— Frequency range 2 to 100 Hz.
— Amplitude 1.6 mm (peak value) below 25 Hz.
— Acceleration amplitude 4.0 g above 25 Hz.
2.8.3 Class C:
— Frequency range 2 to 50 Hz.
— Amplitude 2.5 mm (peak value) below 15 Hz.
— Acceleration amplitude 2.3 g above 15 Hz.

2.9 Inclination

2.9.1 For ships, see Ch.1 Sec.3 [2.2]. For High speed, light craft and naval surface craft, see HSLC Pt.4 Ch.1.

2.10 Electromagnetic compatibility

2.10.1 The minimum immunity requirements for equipment are given in Table 3, and the maximum emission requirements are given in Table 4.

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. 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---o-f---g-u-i-d-a-n-c-e---n-o-t-e---

2.11 Miscellaneous

2.11.1 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).

2.11.2 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 3 Minimum immunity requirements for equipment

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

1) line to line  
2) line to ground  
3) capacitive coupling  
4) coupling clamp  
5) special situations to be analysed  
6) 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 4 Maximum emission requirements for equipment

<table>
<thead>
<tr>
<th>Class</th>
<th>Location</th>
<th>Port</th>
<th>Frequency Range (Hz)</th>
<th>Quasi-peak limits</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>All locations except bridge and open deck</td>
<td>Enclosure (Radiated Emission)</td>
<td>150 k – 30 M</td>
<td>80 – 50 dBμV/m</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>30 – 100 M</td>
<td>60 – 54 dBμV/m</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>100 M – 2 G</td>
<td>54 dBμV/m</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>except: 156 – 165 M</td>
<td>24 dBμV/m</td>
</tr>
<tr>
<td></td>
<td>Power (Conducted Emission)</td>
<td></td>
<td>10 – 150 k</td>
<td>120 – 69 dBμV</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>150 – 500 k</td>
<td>79 dBμV</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>500 k – 30 M</td>
<td>73 dBμV</td>
</tr>
<tr>
<td>B</td>
<td>All locations including bridge and open deck</td>
<td>Enclosure (Radiated Emission)</td>
<td>150 – 300 k</td>
<td>80 – 52 dBμV/m</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>300 k – 30 M</td>
<td>52 – 34 dBμV/m</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>30 M – 2 G</td>
<td>54 dBμV/m</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>except: 156 – 165 M</td>
<td>24 dBμV/m</td>
</tr>
<tr>
<td></td>
<td>Power (Conducted Emission)</td>
<td></td>
<td>10 – 150 k</td>
<td>96 – 50 dBμV</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>150 – 350 k</td>
<td>60 – 50 dBμV</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>350 k – 30 M</td>
<td>50 dBμV</td>
</tr>
</tbody>
</table>

1) Alternatively the radiation limit at a distance 3 m from the enclosure port for the frequency range 156 MHz to 165 MHz shall be 30 dBμV/m peak.

---end---of---g-u-i-d-a-n-c-e---n-o-t-e---

### 3 Electrical and electronic equipment

#### 3.1 General

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

#### 3.2 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).

---end---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.

---end---of---g-u-i-d-a-n-c-e---n-o-t-e---
3.3 Protection provided by enclosure

3.3.1 Enclosures for the equipment shall be made of steel or other flame retardant material capable of providing EMC protection and satisfying the minimum requirements of Table 5. The required degree of protection is specified in IEC 60529.

Table 5 Minimum requirements for enclosures

<table>
<thead>
<tr>
<th>Class</th>
<th>Location</th>
<th>Degree of protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Control rooms, accommodation, bridge</td>
<td>IP 20</td>
</tr>
<tr>
<td>B</td>
<td>Machinery space</td>
<td>IP 44</td>
</tr>
<tr>
<td>C</td>
<td>Open deck, masts, below floor plates in machinery space</td>
<td>IP 56</td>
</tr>
<tr>
<td>D</td>
<td>Submerged application</td>
<td>IP 68</td>
</tr>
</tbody>
</table>

More detailed requirements for ingress protection of enclosure types related to location are given in Ch.8 Sec.10 Table 1.

Guidance note:
Automation equipment of class A and B that should 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---

3.4 Cables and wires

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

3.5 Cable installation

3.5.1 Cable installations shall comply with the requirements in Ch.8 Sec.10 and Ch.8 Sec.3 [4.3].

3.6 Power supply

3.6.1 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.

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

3.6.3 Battery installations shall be in accordance with Ch.8 Sec.10 [2.3].

3.6.4 Regulated rectifiers shall be designed for the variations in voltage and frequency stated in [2].

3.6.5 Different system voltages shall be supplied through different cables.

3.6.6 Terminal lists shall be clearly marked. Various system voltages shall be distinguished.
3.6.7 Uninterruptible power supplies shall be according to the requirements given in Ch.8 Sec.2 [1.2].

3.7 Fibre optic equipment

3.7.1 Fabrication and installation of fibre optic cables shall comply with the requirements of Ch.8 Sec.9.

Guidance note:
The construction of fibre optic devices should generally comply with relevant specifications of IEC Publications.

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

3.7.2 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.

3.7.3 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 shall be taken to prevent fibres from penetrating eyes or skin.

Guidance note:
It is advised to use equipment with 'built-in' safety, e.g. to interlock the power to the light sources with the covers, to arrange disconnection/locking of parts of the system under service, to 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:

\[
L_{\text{safe}} = \frac{(P_n + 10)}{2}
\]

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---

3.7.4 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

1 General

1.1 Application

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

1.2 Introduction

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

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

2 Workstation design and arrangement

2.1 Location of visual display units (VDU) and user input devices (UID)

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

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

![Figure 1 VDU arrangement parameters](image-url)
2.1.3 UIDs and VDUs serving the same function shall as far as possible be arranged and grouped together.

3 User input device and visual display unit design

3.1 User input devices (UID)

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

3.1.2 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.

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

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

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

3.1.6 The naming, numbering and tagging for the different main components shall be consistent on the applicable VDUs, UIDs and signboards.
3.2 Visual display units (VDU)

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

3.2.2 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.

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

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

3.3 Colours

3.3.1 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 1.

**Table 1 Colour coding**

<table>
<thead>
<tr>
<th>Function</th>
<th>Colour code</th>
</tr>
</thead>
<tbody>
<tr>
<td>Danger, Alarm, Emergency</td>
<td>Red</td>
</tr>
<tr>
<td>Attention, Pre-warning, Caution, Undefined</td>
<td>Yellow</td>
</tr>
<tr>
<td>Status of normal, safe situation</td>
<td>Green</td>
</tr>
</tbody>
</table>

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

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

3.4.2 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.

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

3.4.4 Illumination

Means shall be provided for adjustment of illumination of all VDUs and UIDs to a level suitable for all applicable light conditions. However, it shall not be possible to adjust down to a level making information belonging to essential and important functions unreadable.

*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---
4 Screen based systems

4.1 General

4.1.1 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.

4.1.2 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.

4.1.3 Alarms shall be time tagged.

4.1.4 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.

4.1.5 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.

4.1.6 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.

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

4.1.8 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.

4.2 Computer dialogue

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

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

4.2.3 When in dialogue mode, update of essential information shall not be blocked.
4.2.4 Relevant fields for entry of data shall occur with current or a default value. A valid data range shall be defined for each field.

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

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

4.2.7 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.

4.3 Application screen views

4.3.1 For integrated systems, all windows to be called to the VDU shall have a similar representation of all components (menus, buttons, symbols, colours, etc.).
DNV GL
Driven by our purpose of safeguarding life, property and the environment, DNV GL enables organizations to advance the safety and sustainability of their business. We provide classification and technical assurance along with software and independent expert advisory services to the maritime, oil and gas, and energy industries. We also provide certification services to customers across a wide range of industries. Operating in more than 100 countries, our 16 000 professionals are dedicated to helping our customers make the world safer, smarter and greener.