DNV·GL

OFFSHORE STANDARDS

DNVGL-OS-D202 Edition July 2019

Automation, safety and telecommunication systems

DNV GL AS

FOREWORD

DNV GL offshore standards contain technical requirements, principles and acceptance criteria related to classification of offshore units.

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

CHANGES – CURRENT

This document supersedes the January 2017 edition of DNVGL-OS-D202.

Changes in this document are highlighted in red colour. However, if the changes involve a whole chapter, section or subsection, normally only the title will be in red colour.

Changes July 2019

Topic	*Reference*	*Description*
Simplified requirements for FSU giving additional credit for the ship class/ SOLAS requirements for units being converted from **Tanker for oil**.	Previous Ch.2 Sec.8	Supplementary requirements for storage units deleted.

Editorial corrections

In addition to the above stated changes, editorial corrections may have been made.

CONTENTS

CHAPTER 1 INTRODUCTION

SECTION 1 GENERAL

1 Introduction

1.1 Objectives

The objectives of this standard shall be:

— provide an internationally acceptable standard for general requirements to safety, automation, and telecommunication systems by defining minimum requirements for design, materials, fabrication, installation, testing, commissioning, operation, maintenance, re-qualification, and abandonment
— serve as a technical reference document in contractual matters between purchasers and contractors
— serve as a guideline for designers, purchasers and contractors
— specify procedures and requirements for offshore units or installations subject to DNV GL certification and classification

Guidance note:

Additional requirements for specific applications will be given in the DNV GL offshore standard covering those applications.

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

1.2 Scope

1.2.1 The requirements of this standard, shall apply to all safety, automation, and telecommunication systems required by the DNV GL offshore standards.

1.2.2 All safety, automation, and telecommunication systems installed, but not necessarily required by the DNV GL offshore standards, that may have an impact on the safety of main functions (see DNVGL-OS-A101), shall meet the requirements of this standard.

1.2.3 The requirements of this standard are considered to meet the regulations of the MODU Code, with regard to safety, automation, and telecommunication systems.

1.2.4 For telecommunication only relevant parts are applicable. For specific requirement to telecommunication equipment see DNVGL-OS-A101 Ch.2 Sec.5 [6].

1.3 Application

1.3.1 Interpretations

This standard has been based on international accepted principal requirements, defined in the normative references as listed in [2]. In cases where these a) contain only functional requirements, b) allow alternative solutions to prescriptive requirements or c) are generally or vaguely worded, a DNV GL interpretation has been added.

1.3.2 The interpretations are not aiming at introducing additional requirements but at achieving uniform application of the principal requirements. The interpretations can be regarded as norms for fulfilling the principle requirements.

1.3.3 The interpretations do not preclude the use of other alternative solutions. Such solutions shall be documented and approved for compliance to the principal requirement equivalent to the original interpretation.

1.3.4 Classification

For use of this standard as technical basis for offshore classification as well as description of principles, procedures, and applicable class notations related to classification services, see the applicable *DNV GL rules for classification: Offshore units* as listed in Table 1.

Table 1 DNV GL rules for classification: Offshore units

Reference	*Title*
DNVGL-RU-OU-0101 Ch.1	Offshore drilling and support units
DNVGL-RU-OU-0102 Ch.1	Floating production, storage and loading units
DNVGL-RU-OU-0103 Ch.1 Sec.1	Floating LNG/LPG production, storage and loading units
DNVGL-RU-OU-0104 Ch.1	Self-elevating units

1.3.5 The scope of classification may be extended by the voluntary notation **ES**. The applicable sections or requirements as indicated accordingly shall only be enforced in case this notation is part of this extended classification scope.

1.4 Structure

1.4.1 Ch.2 Sec.1 to Ch.2 Sec.5 give common requirements which are considered applicable to all types of offshore units and installations.

1.4.2 Ch.2 Sec.6 gives supplementary requirements to drilling units.

Guidance note:

It should be noted that separate automation and safety requirements related to the voluntary notation **DRILL** is described in DNVGL-OS-E101.

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

1.4.3 Ch.2 Sec.7 gives supplementary requirements to oil and gas production and storage units.

1.4.4 Ch.3 gives procedures and requirements applicable when this standard is used as part of DNV GL classification. Documentation requirements are also given.

1.5 Assumptions

The requirements of this standard 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 References

2.1 Normative references

The standards listed in Table 2 include provisions which, through reference in this text, constitute provisions of this offshore standard. The latest issue of the references shall be used unless otherwise agreed. Other recognised standards may be used provided it can be demonstrated that these meet or exceed the requirements of the standards referenced.

Table 2 Normative references

Reference	*Title*
IACS UR E22	On board use and application of programmable electronic systems
IEC 60529	Degrees of protection provided by enclosures (IP Code)
IEC 60533	Electrical and electronic installations in ships - Electromagnetic compatibility
IEC 60945	Maritime navigation and radiocommunication equipment and systems - General requirements - Methods of testing and required test results
IEC 61000-4-2	Electromagnetic compatibility (EMC), part 4: testing and measurement techniques, section 2: electrostatic discharge immunity test. Basic EMC publication
IEC 61000-4-3	Electromagnetic compatibility (EMC), part 4: testing and measurement techniques, section 3: radiated, radio-frequency, electromagnetic field immunity test
IEC 61000-4-4	Electromagnetic compatibility (EMC), part 4: testing and measurement techniques, section 4: electrical fast transient/burst immunity test. Basic EMC publication
IEC 61000-4-5	Electromagnetic compatibility (EMC), part 4: testing and measurement techniques, section 5: surge immunity test
IEC 61000-4-6	Electromagnetic compatibility (EMC), part 4: testing and measurement techniques, section 6: immunity to conducted disturbances, induced by radio-frequency fields
IEC 60092-504	Electrical installations in ships
IMO Resolution A.1021.(26)	Code on alerts and indicators
ISA 5.1	Instrumentation Symbols and Identification
ISO 3511-1/2/3/4	Process measurement control functions and instrumentation, symbolic representation

2.2 Offshore standards

2.2.1 The latest revision of the DNV GL Offshore standards listed in Table 3 applies.

Table 3 DNV GL offshore standards and other DNV GL references

Standard	*Title*
DNVGL-OS-A101	Safety principles and arrangement
DNVGL-OS-D101	Marine and machinery systems and equipment

Standard	Title
DNVGL-OS-D201	Electrical installations
DNVGL-OS-D301	Fire protection
DNVGL-OS-E101	Drilling plant
DNVGL-OS-E201	Oil and gas processing systems
DNVGL-OS-E301	Position mooring

2.2.2 Other reference documents are given in Table 4.

Table 4 Informative references

Standard	Title
DNVGL-CP-0338	DNV GL type approval scheme (DNV GL class programmes)
DNVGL-CG-0339	Environmental test specification for electrical, electronic and programmable equipment and systems (DNV GL class guidelines)
2009 MODUm Code (IMO)	Code for the Construction and Equipment of Mobile Offshore Drilling Units, 2009, as amended
IMO FSS Code	International Code for Fire Safety Systems

3 Definitions

3.1 Verbal forms

Table 5 Verbal forms

Term	Definition
shall	verbal form used to indicate requirements strictly to be followed in order to conform to the document
should	verbal form used to indicate that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others
may	verbal form used to indicate a course of action permissible within the limits of the document.

3.2 General terms

Table 6 General terms

Term	Definition
alarm	combined visual and audible signal for warning of an abnormal condition, where the audible part calls the attention of personnel, and the visual part serves to identify the abnormal condition
automation system	system that is able to control, and/or monitor fully of partly, the operation of equipment under control (EUC)

Term	*Definition*
back-up control system	comprises all hardware and software necessary to maintain control when main control systems have failed, malfunctioned or are being maintained
equipment under control (EUC)	the mechanical equipment (machinery, pumps, valves, etc.) or environment (smoke, fire, waves, etc.) monitored and/or controlled by an automation and safety system
essential safety, automation or telecommunication system (hereafter called an essential system or essential function)	system supporting equipment, which needs to be in continuous operation or continuous available for on demand operation for maintaining the unit's safety Systems supporting the propulsion and steering functions are considered as essential for all units incorporating such functions. The definition essential system may also apply to other functions when these are defined as such in the DNV GL offshore standards. **Guidance note:** The objective for an essential function is that it should be in continuous operation for relevant operational modes, i.e. transit, operation, e.g. the emergency shutdown (ESD) system for an offshore unit. ---e-n-d---o-f---g-u-i-d-a-n-c-e---n-o-t-e---
field instrumentation	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.
fire panel/central	a standalone system for presenting of fire alarms and system failure
important safety, automation or telecommunication system (hereafter called an important system or function)	system supporting functions in order to perform in accordance to class requirement, unless specified otherwise in other DNV GL offshore standards
independency:	*mutually independent:* 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 as described above. *independent:* 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 affect the maintained operation of system A.
indications	the visual presentation of values for the EUC or system status to a user (lamps, dials, VDU displays, etc.)
integrated system	combination of computer based systems which are interconnected in order to allow common access to sensor information and/or command or control
monitoring system	system that is able to monitor and issue alarms relating to the operation of an equipment under control (EUC)

Term	*Definition*
non-important safety, automation and telecommunication systems (hereafter called non-important systems or non-important function)	systems supporting functions that are not required by the DNV GL offshore standards
normally de-energised (NDE) circuit	circuit where energy is present when the circuit is activated by the activating function
normally energised (NE) circuit	circuit where energy is present when the circuit is not activated by the activating function
process segment	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.
process	the result of the action performed by the EUC
redundancy	system with redundancy is one with duplication which prevents failure of the entire system in the event of failure of a single component
remote control system	comprises all hardware and software necessary to operate the EUC from a control position where the operator cannot directly observe the effect of his actions
safety and automation system (SAS)	term used for integrated safety, automation, and/or telecommunication system **Guidance note:** Other terms used for such systems are: Integrated control and safety system (ICSS) and safety and instrumentation system (SIS). The term is also commonly used on stand alone system not integrated with other systems. ---e-n-d---o-f---g-u-i-d-a-n-c-e---n-o-t-e---
safety shutdown	safety action that will be initiated upon EUC failure or by other predefined events (e.g. gas detection) and shall result in the shutting down of the EUC or part of the EUC in question
safety system	systems, including required utilities, which are provided to prevent, detect/ warn of an accidental event/abnormal conditions and/or mitigate its effects **Guidance note:** Examples of safety systems are: — ESD including blowdown where relevant — PSD — fire & gas detection — PA/GA — fire-fighting systems — BOP control system — safety systems for equipment. ---e-n-d---o-f---g-u-i-d-a-n-c-e---n-o-t-e---

Term	*Definition*
separated	terms used on cables, networks nodes, etc. to indicate that they are physically located with distance or mechanical separation sufficient to prevent a single failure taking out the entire function **Guidance note:** The best separation that is reasonably practicable in order to minimise the chances of a single incident affecting both systems should be applied. Redundant controllers in the same cabinet are considered to be acceptable because the cabinet is located in a well protected safe area. ---e-n-d---o-f---g-u-i-d-a-n-c-e---n-o-t-e---
system	system includes all components necessary for performing safety, automation or telecommunication functions, including sensors and actuators As used in this standard, system is short for safety, automation or telecommunication system. A system includes all resources required to support one specific function, 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 — initiate required actions — feedback on activated actions, when relevant.
system availability	the time the system is available
telecommunication system	system providing internal communication within the unit (e.g. telephones, public address, general alarm) or externally to the unit (e.g. radio)
uninterruptible power supply (UPS)	device supplying output power in some limited time period after loss of input power with no interruption of the output power
user	any human being that will use a system or device, e.g. captain, navigator, engineer, radio operator, stock-keeper, etc.
warning	indication of equipment under control (EUC) or system state that needs attention
workstation	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

3.3 Terms related to computer based system

Table 7 Terms related to computer based system

Term	*Definition*
application software	standard software which is required for developing, running, configuring or compiling application software and project specific program(s) with associated parameters which carry out operations related to the EUC being con-trolled or monitored
complex system	system for which all functional and failure response properties for the completed system cannot be tested with reasonable efforts Systems handling application software belonging to several functions, and software that includes simulation, calculation and decision support modules are normally considered as complex.
computer	computer includes any programmable electronic system, including main-frame, mini-computer or micro-computer (PLC)
computer task	in a multiprocessing environment, this means one or more sequences of instructions treated by a control program as an element of work to be accomplished by a computer
critical alarm and action panel (CAAP)	panel used to present vital safety related information, and to activate vital safety related functions independent of operator stations
data communication links	this includes point to point links, instrument net and local area networks, normally used for inter-computer communication on board units A data communication link includes all software and hardware necessary to support the data communication. **Guidance note:** For local area networks, this includes network controllers, network transducers, the cables and the network software on all nodes. ---e-n-d---o-f---g-u-i-d-a-n-c-e---n-o-t-e---
fire and gas node	the system elements related to fire and gas detection and related actions within a safety system, organised as an independent node within the system
function block	small self-contained function with a set of defined inputs and outputs that carries out a clearly defined task and is intended to operate within an application program
instrument net	network used for data communication within the field instrumentation connecting instruments in a network
local area network	network used for data communication between the automation, safety and the other parts of a system, and between different systems
multifunction VDUs and UIDs	VDUs and UIDs that are used for more than one essential and/or important function for both safety and/or automation, e.g. VDUs and UIDs used for integrated computer systems
network components	all hardware devices directly connected to a communication network
node in a system	computer based controller, usually with associated field device I/O, capable of carrying out logic, control and calculation functions and communicating data with other nodes and stations on the system network(s)
operator station	in an integrated system is a unit consisting of a user interface, i.e. UIDs and VDU, and interface controller(s) An integrated operator station is one serving two or more systems.

Term	*Definition*
point to point	link used for data communication between two dedicated nodes
software module	small self-contained program which carries out a clearly defined task and is intended to operate within a larger program
system software	software used to control the computer and to develop and run applications **Guidance note:** Typically the operating system or system firmware. ---e-n-d---o-f---g-u-i-d-a-n-c-e---n-o-t-e---
user input device (UID)	any device from which a user may issue an input including handles, buttons, switches, keyboard, joystick, pointing device, voice sensor and other control devices
visual display unit (VDU)	any area where information is displayed including indicator lamps or panels, instruments, mimic diagrams, and computer display monitors

3.4 Abbreviations

The abbreviations given in Table 8 are used.

Table 8 Abbreviations

Abbreviation	*In full*
BOP	blow out preventer
CAAP	critical alarm and action panel
CCR	central control room on MOUs, on tankers CCR normally refers to cargo control room
DCS	drilling control system
DP	dynamic positioning
DSSS	direct sequence spread spectrum
ECR	engine control room
EMC	electromagnetic compatibility
EUC	equipment under control
EUT	equipment under test
ESD	emergency shut down
EPROM	erasable programmable read-only memory
EEPROM	electrically erasable programmable read-only memory
F&G	fire and gas
FAT	factory acceptance test
FHSS	frequency hopping spread spectrum
HVAC	heating, ventilation and air conditioning
I/O	input and/or output

Abbreviation	*In full*
ICSS	integrated control and safety system
IEC	International Electrotechnical Commission
LAN	local area network
LED	light emitting diode
LCD	liquid crystal display
MOU	mobile offshore unit
MS	manufacturing survey
NDE	normally de-energised
NE	normally energised
OTDR	optical time domain reflectometry
PA/GA	public address & general alarm system
PCS	process control system
PLC	programmable logical controller
RPM	rotations per minute
RP	redundant propulsion
PROM	programmable read only memory
PSD	process shutdown
SAS	safety and automation system
SW	software
UID	user input device
UPS	uninterruptible power system
VDU	visual display unit
VLAN	virtual local-area network
VMS	vessel management system
WPA	WiFi protected access

CHAPTER 2 TECHNICAL PROVISIONS

SECTION 1 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 system cannot spread to another system.

1.1.2 Failure of any remote or automatic control system shall initiate an audible and visual alarm at a manned control station and shall not prevent manual control.

1.2 Field instrumentation

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

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

1.2.3 Electronic governors shall have power supply independent of other consumers and system availability of 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.

(See IACS UR M3.1.3)

Guidance note:

Electric or electronic fuel injectors should be designed to permit the necessary functionality in case of the most probable failures.

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

1.2.4

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

1.3 Integrated systems

1.3.1 An integrated system shall be arranged with sufficient redundancy and/or segregation so as to prevent loss of essential functions or multiple main functions upon a single failure.

1.3.2 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.3 [3] to ensure integrity of the safety functions.

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

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

1.3.5 Simultaneous display of overview and detailed-information for relevant control, monitoring and safety systems shall be ensured.

Interpretation:

For control and monitoring systems:

— Sufficient number of operator stations should be available at the main work station ensuring that all functions that may need simultaneous attention are available.

For safety systems:

— Sufficient overall status should be provided without browsing between screen pictures. This implies that it should be possible to both have fixed overview of safety related information as well as detailed information about the incident.

---e-n-d---o-f---i-n-t-e-r-p-r-e-t-a-t-i-o-n---

Guidance note:

The number of VDUs and UIDs at control stations should be sufficient to ensure that all functions may be provided for with any one VDU or UID out of operation, taking into account any functions that should be continuously available. Note the requirement for operator interface for each network segment in Sec.3 [3.2.4].

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

1.3.6

For integrated systems, compliance with the above requirements shall be documented in a functional failure analysis (Z070), see

1.4 Redundancy

1.4.1 Redundancy shall be built in to the extent necessary for maintaining the safe operation of the unit. Changeover to redundant systems shall be simple even in cases of failure of parts of the safety and automation system (SAS).

1.4.2 The redundancy requirement shall imply redundant communication links, power supplies, computers and operator stations.

Guidance note:

Redundancy of computers may be limited to controllers with CPUs; single I/O cards/modules are accepted. Consideration should be given to the allocation of signals to I/O modules in order to minimise the consequences of a single card/module failure.

Addressable loops for fire detector systems with single CPU central units are presently accepted for living quarter and marine areas as well as for drilling areas, but areas with more than one detector should normally be covered by at least two loops. Consideration should be given to distribution of detectors on different loops.

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

2 System availability

2.1 General

2.1.1 The availability requirements for the SAS shall be adapted to the availability requirements imposed on the function served.

2.1.2 The system availability for the various SAS applications shall be arranged in accordance with the different categories as given in Table 1.

Table 1 System availability

System category	*Repair time*
Continuous availability (R0)	None
High availability (R1)	30 s
Manual system restoration (R2)	10 minutes
Repairable systems (R3)	3 hours

2.2 Continuous availability (R0)

2.2.1 A system serving a function that shall be continuously available shall be designed to provide no interrupts of the function neither in normal operation modes nor in case of a single system failure.

2.2.2 Changeover between redundant systems shall take place automatically and with no disturbances for the continuous operation of the function in case of system failure. User requested changeovers shall be simple and easily initiated and take place with no unavailable time for the function.

2.2.3 User interfaces of redundant systems shall allow supervision of both systems from the same position.

2.3 High availability (R1)

2.3.1 A system serving a function that shall have high availability shall be designed to provide continuous availability in normal operation modes.

2.3.2 In case of system failures, changeover between redundant systems shall take place automatically if redundancy is required. User requested changeover in normal operation shall be simple and easily initiated and take place within the same repair time.

2.3.3 User interfaces of redundant systems shall be located close to each other and changeover between the systems shall have no significant effect on the user's maintained execution of other tasks.

2.4 Manual system restoration (R2)

A system serving a function that requires manual system restoration shall be designed to provide restoration of the function within a repair time specified for R2, in case of system failures.

Guidance note:

Restoring a function may involve a limited number of simple manual actions.

User interfaces of redundant systems may be designed for manning of normally unattended workstations when required, provided such manning is immediately available.

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

2.5 Repairable systems (R3)

A system serving a function of category R3 shall be designed to provide restoration of the function within a repair time specified for R3 in case of system failures.

Guidance note:

Restoring a function may involve a number of manual operations, including minor replacements or repair of equipment.

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

3 Response to failures

3.1 Failure detection

3.1.1 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 in an assigned manned control station.

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

— power failures

Additionally for computer based systems:

— communication errors
— computer hardware failures.

Additional for essential/safety systems:

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

See also Sec.3.

3.2 Fail-safe functionality

3.2.1 The most probable failures, for example loss of power or wire failure, shall result in the least critical of any possible new conditions.

Guidance note:

See DNVGL-OS-A101 Ch.2 Sec.4 [2] and sections 6, 7 or 8 as applicable.

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

3.2.2 A single failure causing loss of single or multiple fire or gas detection signals shall lead to the safest of the available new condition/states, taking the unit or installation into consideration.

Guidance note:

See DNVGL-OS-A101 Ch.2 Sec.4 [2.1.3] and Table 2 Safest condition in case of failure to the shutdown system.

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

3.3 System response – redundant systems

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

Interpretation:

For redundant systems, any failure should not cause an interruption that jeopardizes safe operation. This applies also to the most time critical functions.

---e-n-d---o-f---i-n-t-e-r-p-r-e-t-a-t-i-o-n---

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.

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

4 User interface

For essential and important systems, deviations between a command action and expected result of the command action shall initiate an alarm.

5 Tests

5.1 General

5.1.1 All relevant tests shall be performed according to an approved test program.

5.1.2 Testing according to [5.2], [5.3], and [5.4] shall be performed at the manufacturers' works.

Interpretation:

For systems subject to certification an internal test according to [5.1.1] should be performed prior to certification/FAT.

---e-n-d---o-f---i-n-t-e-r-p-r-e-t-a-t-i-o-n---

Guidance note:

It is acknowledged that all project information may not be available at the time of final testing in the manufacturer's works. Testing should be performed to the extent possible prior to system delivery.

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

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

— means for access control and system configuration/modification
— implementation of software quality plan.

(See IACS UR E22, Appendix 1, sections 3, 5 and 6)

5.1.4 The tests and visual examinations shall verify that all requirements given by the applicable DNV GL offshore standards are met. The test procedures shall specify in detail how the various functions shall be tested and what shall be observed during the tests.

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

5.1.6 It shall be verified that all automation functions are working satisfactorily during normal load changes.

5.2 Software testing

5.2.1 Documentation of software module and function block testing shall be available at the manufacturer's works.

(See IACS UR E22, Appendix 5.1 and 5.2)

5.2.2 Application software testing shall be performed to demonstrate functionality in accordance with design documentation with respect to the equipment under control (EUC), including the operator interface.

(See IACS UR E22, Appendix 5.3)

5.3 Integration testing

Integration tests includes integration of hardware components and integration of software modules into the same hardware.

5.3.1 Integration tests shall be performed with the actual software and hardware to be used on board.

(See IACS UR E22, Appendix 6.1)

Interpretation:

1) The integration test should include at least the following:
   a) Hardware tests;
      hardware failures.
   b) System software tests;
      System software failures.
   c) Application software tests.
   d) Function tests of normal system operation and normal EUC performance, in accordance with the requirements of the DNV GL offshore standards. Function tests are also to include a degree of performance testing outside of the normal operating parameters.
   e) User interface tests.
2) If the integration test is not practicable before the hardware is installed on-board, the testing should be planned for and described in a test plan, describing where and how the necessary tests shall be performed to achieve the same level of verification. In such cases, the yard, supplier and DNV GL should agree on the plan.

---e-n-d---o-f---i-n-t-e-r-p-r-e-t-a-t-i-o-n---

5.4 System testing

System testing shall be performed to demonstrate that the system fulfills the requirements as stipulated by the applicable rules.

(See IACS UR E22, Appendix 6.3)

Interpretation:

1) System tests should include the entire system, integrating all hardware and software. The test may also include several systems.
2) System tests should be performed with the software installed on the actual systems to be used on-board, interconnected to demonstrate the functions of the systems.
3) The tests should include those tests which were not or could not be completed on hardware component or software module level.
4) If the system test is not practicable before the hardware is installed on-board, the testing shall be planned for and described in a test plan, describing where and how the necessary testsshall be

performed to achieve the same level of verification. In such cases, the yard, supplier and DNV GL shall agree on the plan.

---e-n-d---o-f---i-n-t-e-r-p-r-e-t-a-t-i-o-n---

5.5 On-board testing

5.5.1 The testing shall demonstrate, verify and document full functionality of all automation and safety systems and shall include:

a) During installation the correct function of individual equipment packages, together with establishment of correct parameters for automation and 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 automation and safety systems to keep any EUC within the specified tolerances and carry out all safety/protective actions.
c) The correct distribution, protection and capacity of power supplies.
d) Back-up and emergency automation and safety functions for essential unit/installation systems.

Interpretation:
The tests should demonstrate that the essential installation functions are operable on the available back-up means of operation (as required in the relevant application standard), and in a situation where the control system for normal operation is disabled as far as practical.

---e-n-d---o-f---i-n-t-e-r-p-r-e-t-a-t-i-o-n---

5.5.2 The test program for harbour and sea trials shall be approved prior to tests by the local DNV GL station.

5.5.3 The on board testing should include all the tests which could not be completed during integration or system-testing/FAT.

5.5.4 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.

5.5.5 If the machinery system is designed for different normal operational modes, e.g. dual fuel engines, the test described in [5.5.4] shall be run for each relevant mode of operation.

5.6 Pneumatic and hydraulic systems

5.6.1 Hydraulic automation and shut-down systems shall be tested with maximum return flow to verify that return headers are adequately sized and free of blockages which could prevent correct system performance.

5.6.2 For pneumatic and hydraulic automation systems with accumulators used to ensure fail safe operation, tests shall include verification of accumulator charge level and capacity.

5.6.3 Piping and tubing to actuators and between actuators and local accumulators shall be hydrostatically tested according to the requirements given in DNVGL-OS-D101 Ch.2.

SECTION 2 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 categories:

— automation system
— remote control
— alarm
— safety
— indications
— planning and reporting
— calculation, simulation and decision support.

1.1.3 Whenever automatic or manual shutdown is required in the rules, the function shall be implemented in a safety system that is mutually independent of the control and alarm systems.

Control and alarm functions may then be implemented in common system units.

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

Interpretation:

ESD/PSD, F&G and automation nodes should be physically segregated in different cabinets.

---e-n-d---o-f---i-n-t-e-r-p-r-e-t-a-t-i-o-n---

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, provided that the network is designed according to Sec.3, but each unit should be able to perform its main functions autonomously.

The independency between safety systems and other systems is intended to provide a robust single fault tolerance. It is in general not acceptable to integrate safety systems with other systems even when arranged with redundancy or duplication - redundancy in system design is in general not accepted as an alternative way to meet the requirement for independency between systems.

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

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 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 may be expected under normal conditions, will not cause instability. The automation system element shall be able to accomplish the function it shall serve.

1.2.3 Automatic control such as automatic starting and other automatic operations, when relevant, shall include provisions for manually overriding the automatic controls provided that safe manual operation is 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 fail to safety which normally implies either to remain in its present state or move controlled to a predefined safe state.

1.3 Remote control

1.3.1 At the remote command location, the user shall receive continuous information on the effects of the commands given.

1.3.2 Each group of functions shall have a default main command location. The main command location shall have priority of other command locations.

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

1.3.4 Actual control shall not be transferred before acknowledged by the receiving command location unless the command locations are located close enough to allow direct visual and audible contact. Transfer of control shall give audible warning.

1.3.5 The main command location shall be able to take control without acknowledgement, but an audible warning shall be given at the work station that relinquish control.

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.

Interpretation:

If this involves manual alignment of control levers, indicators shall show how the levers must be set to become aligned.

---e-n-d---o-f---i-n-t-e-r-p-r-e-t-a-t-i-o-n---

1.3.7 On each alternative command location, it shall be indicated when this location is in control.

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

Basic safety interlocks shall be hard-wired and shall be active during remote and local operation.

Guidance note:

Hard-wired 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 Safety

1.4.1 A safety system element shall be arranged to automatically take safety actions on occurrence of predefined abnormal states for the EUC. The corresponding system element includes all resources required to execute these actions. Where fail safe condition is defined as continue for essential systems, a failure in the loop monitoring shall initiate an alarm and not stop the unit.

Interpretation:

Where loop failure monitoring is not possible, a two out of two voting system may be accepted.

---e-n-d---o-f---i-n-t-e-r-p-r-e-t-a-t-i-o-n---

Guidance note:

For fail safe condition reference is made to DNVGL-OS-A101 Ch.2 Sec.4 Table 2 andSec.6, Sec.7or DNVGL-OS-A101 Ch.2 Sec.9 as applicable.

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

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

1.4.3 Automatic safety actions shall initiate alarm at manned workstations.

1.4.4 When the safety system element stops an EUC, the EUC shall not start again automatically.

1.4.5 When a safety system element is made inoperative by a manual override, this shall be clearly indicated at the main control station.

1.4.6 When a safety system element has been activated, it shall be possible to trace the cause of the safety action at the main control station. There shall be means at the main control station to reset safety functions made inoperative in a readily accessible manner, unless stated otherwise in the Offshore Standards.

1.4.7 When two or more protective safety actions are initiated by one failure condition, these actions shall be activated at different levels, with the least drastic action activated first.

Guidance note:

For certain equipment the sequence of events for certain process parameters may be so rapid that it is no use to activate the two protective safety actions at different levels. An alarm should be activated prior to a protective safety action, except when it is regarded as not being possible due to urgency, see relevant parts of SOLAS Ch. II-1.

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

1.5 Alarms

1.5.1 Alarms shall be visual and audible and shall indicate abnormal conditions only. In areas where the audible signal may not be heard due to background noise, additional visual and audible display units shall be installed.

Guidance note:

Several suitably placed low volume audible alarm 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.

IMO resolution A.1021(26) regulation 4.18, requires that alarms and indicators on the navigation bridge should be kept at a minimum. Alarms and indicators not required for the navigation bridge should not be placed there unless permitted by the administration.

For PA/GA alarms see DNVGL-OS-A101 Ch.2 Sec.5 [6] for details.

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

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

Guidance note:

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

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

1.5.3 Audible alarms shall be readily distinguishable from signals indicating normal conditions, telephone signals, different alarm systems and noise.

Interpretation:

The audible and visual characteristics of alarm signals defined by IMO Resolution A.1021(26), code on alarms and indicators, aragraph 7 characteristics, should be used.

---e-n-d---o-f---i-n-t-e-r-p-r-e-t-a-t-i-o-n---

1.5.4 Responsibility for alarms shall not be transferred before acknowledged by the receiving location. Transfer of responsibility shall give audible warning. At each individual location, it shall be indicated when this location is in charge, if relevant.

1.5.5 Acknowledgement of alarms shall only be possible at the workstation(s) dedicated to respond to the alarm.

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

Silencing and acknowledgement of alarms shall be arranged as follows:

Silencing the audible signal:

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

Acknowledgement of an alarm:

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

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

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

Guidance note:

Flashing red indication is normally used for un-acknowledged alarm while steady red is used for active, acknowledged alarm. This applies for all operator interfaces, including standard VDU and back-up means.(e.g. CAAP)

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

Guidance note:

The individual alarms in an alarm group may be identified on a local panel.

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

1.5.6 The presentation of alarms and indicators should be clear, distinctive, unambiguous and consistent.

(See IMO A.1021(26), sec. 4.1)

Interpretation:

1) Acknowledgement of visual signals should be separate for each signal or common for a limited group of signals. Acknowledgement should only be possible when the user has visual information on the alarm condition for the signal or all signals in a group.
2) Local equipment audible alarm for equipment connected to the automation and safety system, should be suppressed when localised in the same workplace as the user interface for the automation and safety system.

---e-n-d---o-f---i-n-t-e-r-p-r-e-t-a-t-i-o-n---

1.5.7 Permanent blocking of alarm units shall not be possible. Manual blocking of separate alarms is acceptable when this is clearly indicated.

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

Interpretation:

Alarms should be time-tagged, see also Sec.3 [3.1.1].

---e-n-d---o-f---i-n-t-e-r-p-r-e-t-a-t-i-o-n---

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

1.5.10 Means should be provided to prevent normal operating conditions from causing false alarms, e.g., provision of time delays because of normal transients.

(See IMO A.1021(26) sec. 4.17)

Interpretation:

Blocking of alarm and safety functions in certain operating modes (for example during start-up) should be automatically disabled in other modes.

---e-n-d---o-f---i-n-t-e-r-p-r-e-t-a-t-i-o-n---

1.5.11 The number of alarms during abnormal conditions shall be assessed and reduced as far as practicable by alarm processing/suppression techniques in order to have operator attention on the most critical alarms that require operator actions.

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 shall be accomplished. Alarms 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, for example by standardising the scales, applying mimic diagrams, and similar.

---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 vessel/unit 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

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, for example route plan used as input to an autopilot or load plan used as input for automatic or user assisted sequence control of the loading.

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---

1.8 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.

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

2 General requirements

2.1 System operation and maintenance

2.1.1 Prior to restart after a shut-down, the situation resulting in the shut-down shall be cleared and be reset prior to restart.

2.1.2 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, where applicable.

Interpretation:

This restoration and resume of operations should include all controller units, operator stations and network/ communication link components necessary to support normal operation of the control and safety system.

---e-n-d---o-f---i-n-t-e-r-p-r-e-t-a-t-i-o-n---

2.1.3 The system shall be designed to allow testing without disrupting normal operation of the function served.

Interpretation:

Alarm- and safety functions should be possible to test during operation, and the system should not remain in test mode unintentionally.

---e-n-d---o-f---i-n-t-e-r-p-r-e-t-a-t-i-o-n---

Guidance note:

It is recommended to arrange an automatic return to operation mode or alarm.

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

2.2 Power distribution

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 DNVGL-OS-D201 Ch.2 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 are feeding both systems.

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

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.

Guidance note:

See DNVGL-OS-D201 Ch.2 Sec.2 Table 1.

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

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 work stations.

SECTION 3 ADDITIONAL REQUIREMENTS FOR COMPUTER BASED SYSTEMS

1 General requirements

1.1 Assignment of responsibility for integrated systems

The responsibility of total integrated system shall be assigned to one organisational body.

Guidance note:

This organisational body may be the yard, a major manufacturer or another body holding necessary competence and resources to enable a controlled integration process.

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

1.2 Back-up means of operation

Where the normal user interface for the below listed safety functions is an operator station in an integrated system, a back-up means of operation/user interface is required.

This applies to:

— emergency shutdown systems (ESD)
— fire and gas detection system
— activation of relevant fire-fighting systems
— other safety functions where a back-up means is required by the rules or standards.

The back-up means of operation shall be independent of the normal user interface and its communication networks.

Interpretation:

The back-up means of operation should be based on proven and reliable design and be:

— located adjacent to the normal operating position
— for all activation signals and other ESD related signals needed to ensure activation, hard-wired individually directly to the respective controller.

---e-n-d---o-f---i-n-t-e-r-p-r-e-t-a-t-i-o-n---

Guidance note:

The back-up means of operation is typically achieved by provision of a CAAP (critical alarm and action panel).

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

1.3 Storage devices

The data storage devices shall ensure satisfactory availability and performance of the function served.

Interpretation:

1) The on-line operation of essential functions should not depend on the operation of rotating bulk storage devices.
2) Software and data necessary to ensure satisfactory performance of essential and important functions should normally be stored in non-volatile memory (e.g. EPROM, EEPROM or FLASH). Exception may be given for RAM with battery backup if the following three conditions are met:
   - low battery voltage results in an alarm or visual indication detectable by routine inspections
   - battery can easily be replaced by crew personnel without danger of losing data
   - battery failure has no influence on performance as long as normal power supply is maintained.

---e-n-d---o-f---i-n-t-e-r-p-r-e-t-a-t-i-o-n---

Guidance note:

Interpretation 1) does not exclude the use of such storage devices (e.g. hard disks) for maintenance, restoration and back-up purposes.

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

1.4 Computer usage

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

1.5 System response and capacity

1.5.1 Systems used for automation and safety systems 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 offshore units:

Table 1 Typical response times

Function	*Typical response times*
Data sampling for automatic control purposes (fast changing parameters)	0.1 s
Data sampling, indications for analogue remote controls (fast changing parameters)	0.1 s
Other indications	1 s
Alarm presentations	2 s
Display of fully updated screen views	2 s
Display of fully updated screen views including start of new application	5 s
Automatic emergency actions	1 s
Gas detector response time	<10 s
Fire detector response time	<10 s

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

1.5.2 System start-up and system restoration after power failures shall take place with sufficient speed to comply with the system availability requirements for the systems. The system shall revert to a pre-defined state providing an appropriate level of safety.

1.5.3 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.

1.6 Temperature control

Wherever possible, computers shall not have forced ventilation. For systems where cooling or forced ventilation is required to keep the temperature at an acceptable level, alarm for high temperature or mal-operation of the temperature control function shall be provided at a manned control station.

1.7 System maintenance

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

1.7.2 Essential systems shall have diagnostic facilities to support finding and repair of failures.

1.8 System access

1.8.1 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 allowed to be modified under normal operation.

Guidance note:

As a minimum this should cover:

— calibration data
— alarm limit modification
— manual alarm blocking or inhibiting.

The operator should only have access to the application(s) related to the operation of the functions covered by the system according to Sec.1 [1.4.1], while access to other applications or installations of such, should be prevented. Hot keys normally giving access to other functions or program exits (Alt+Tab, Ctrl+Esc, Alt+Esc, double-clicking in background, etc.) should be disabled.

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

1.8.2 Unauthorised access to essential and important systems from a position outside the unit shall not be possible. See also [2.3.4] for remote diagnostics and maintenance.

Interpretation:

1) Systems allowing for remote connection (e.g. via Internet), for e.g. remote diagnostics or maintenance purposes, should be secured with sufficient means to prevent unauthorised access, and functions to maintain the security of the control and monitoring system. The security properties should be documented.
2) Any remote access to the control system should be authorised on-board.

---e-n-d---o-f---i-n-t-e-r-p-r-e-t-a-t-i-o-n---

Guidance note:

The system should have appropriate virus protection also related to the possibility of infection via the remote connection.

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

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

2 System software

2.1 Software requirements

Application software shall, to the extent possible, be standardised with the flexibility to provide the required functionality for an individual system by simple configuration and parameterisation (i.e. with minimal need for high level programming).

(See IEC 60092-504 10.9.2, 10.11.4)

Interpretation:

1) Application software should be realised using standard software modules (e.g. function blocks) to the greatest extent possible. The software modules should have the flexibility to provide individual application functionality by use of simple configuration and parameterisation. The use of high level programming should be minimised.
2) The application software, software modules and function blocks should encourage consistent programming of functions within the system as well as maximising the consistency of operation and consistency of presentation of information to the Operator.
3) System set-up, configuration to suit the EUC and the setting of parameters for the EUC on-board should take place without modification of program code or recompilation. Facilities should be provided to allow simple back-up and restoration of operator configured parameters.

---e-n-d---o-f---i-n-t-e-r-p-r-e-t-a-t-i-o-n---

2.2 Software development

Software shall be developed in accordance with procedures for configuration management that ensure traceability and the integrity of the software.

(See IACS UR E22 2.5, 3.7, 4.1, IEC 60092-504 10.9)

Interpretation:

All relevant actions should be taken during manufacturing of software for a complex system to ensure that the probability of errors to occur in the program code is reduced to an acceptable level.

Relevant actions should at least include actions to:

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

---e-n-d---o-f---i-n-t-e-r-p-r-e-t-a-t-i-o-n---

Guidance note:

Typical execution failures are:

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

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

2.2.1 The actions taken to comply with 2.2.1 shall be documented and implemented, and the execution of these actions shall be retraceable.

Interpretation:

1) The documentation should include a brief description of all tests that apply to the system (hardware and software), with a description of the tests that are intended to be made by sub-vendors, those to be carried out at the manufacturer's works and those to remain until installation on-board.

   When novel software is developed for essential systems, third party approval of the manufacturer may be required, either prior to or as part of the actual product development.
2) Running software versions should be uniquely identified by a version number, date or other appropriate means. This should apply for all system software (including third party software packages) and all application software. Modifications should not be made without also changing the version identifier.

---e-n-d---o-f---i-n-t-e-r-p-r-e-t-a-t-i-o-n---

2.3 Software and hardware change management

2.3.1 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.

2.3.2 System software shall be protected against unauthorised and unintended modifications by means of appropriate access control.

(See IACS UR E22 2.5, IEC 60092-504 10.3)

2.3.3 Software shall be maintained in accordance with procedures for configuration management that ensure traceability and the integrity of the software.

(See IACS UR E22 2.5, 3.7, 4.1, Appendix 1, 1.5)

Interpretation:

1) Manufacturers or system suppliers should 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.
2) Major changes or extensions in hardware or software of approved systems should 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.
3) When basic or application software is changed on an approved control system, the following requirements apply:
   - a procedure for software change handling should be available on request, describing the necessary steps and precautions related to SW handling
   - major modifications which may affect compliance with the rules should be described and submitted to the society for evaluation before the change is implemented on-board

- no modification should be done without the acceptance and acknowledgement by the offshore units responsible member of the crew
- the modified system should be tested and demonstrated for the offshore units responsible member of the crew
- the modification should be documented (including objective/reason for the change, description, authorization, test record, signatures, date, new incremented SW revision no)
- a test program for verification of correct installation and correct functioning of the applicable functions should be available
- in case the new software upgrade has not been successfully installed, the previous version of the system should be available for re-installation and re-testing.

---e-n-d---o-f---i-n-t-e-r-p-r-e-t-a-t-i-o-n---

2.3.4 If the control system is approved for remote software maintenance (i.e. from outside the vessel), the procedures and means for configuration management shall be expanded beyond the requirements of [2.3.2] to ensure that the integrity of the software is maintained.

Interpretation:

1) A particular procedure for the remote SW maintenance operation should exist.
2) No remote access or remote SW modification should be possible without the acceptance and acknowledgement by the offshore units responsible member of the crew.
3) The security of the remote connection should 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).
4) Before the updated software is put into real-time use, the integrity of the new software should be verified by appropriate means.
5) The remote session should be logged in accordance with the above procedure for remote SW maintenance.

---e-n-d---o-f---i-n-t-e-r-p-r-e-t-a-t-i-o-n---

3 Network systems and communication links

3.1 General

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

Interpretation:

The accuracy of the synchronisation should 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.

---e-n-d---o-f---i-n-t-e-r-p-r-e-t-a-t-i-o-n---

Guidance note:

If information is received from a source where time tagging is not practical, it is accepted that the time tagging is done at the receiving node in the network, at the earliest possible time.

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

3.1.2 The network shall be designed with adequate immunity to withstand the possible noise exposure in relevant areas.

Guidance note:

This implies e.g. use of fibre optical cable in areas of high noise exposure from high voltage equipment.

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

3.1.3 Systems or components not considered to be a necessary part of the automation and safety functions shall not be connected to the system.

Interpretation:

1) If the automation and safety system is connected to administrative networks, the connection principle should ensure that any function or failure in the administrative net can not harmfully affect the functionality of the automation and safety system. The administrative functions should be hosted in separate servers and should, if at all necessary, have read only access to the control network.
2) It should not be possible for unauthorized personnel to connect equipment to the SAS network, e.g. unauthorised access on network components like e.g. switches.
3) Miscellaneous office or entertainment functions should not be connected to the automation and safety system.

---e-n-d---o-f---i-n-t-e-r-p-r-e-t-a-t-i-o-n---

Guidance note:

Ad 1) 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 offshore standard.

Ad 2) and 3) it is normally not acceptable to include CCTV video streams as part of the automation and safety system.

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

3.1.4 It shall be possible to maintain emergency operation of the vessel/units main functions independent of network status. This may imply that essential nodes hosting emergency operation functionality shall be able to work autonomously, and with necessary operator interface independent of the network.

3.1.5 Any network integrating SAS shall be single point of failure-tolerant. This normally implies that the network with its necessary components and cables shall be designed with adequate redundancy.

Interpretation:

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

---e-n-d---o-f---i-n-t-e-r-p-r-e-t-a-t-i-o-n---

3.1.6 Cables and network components belonging to redundant networks shall as far as practicable be physically separated in exposed areas.

Guidance note:

Exposed areas in this context means machinery spaces category A and hazardous areas and areas where operational incidents may lead to damage of equipment.

In order to support the system fault tolerance, it is recommended to arrange redundant network components with necessary power supplies in separate cabinets, and the network cabling serving the redundant networks routed separately.

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

3.2 Network communication

3.2.1 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, intentionally or erroneously, 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 should have properties to monitor it's own communication through the network, and to be able to detect, alarm and respond in a predefined manner in case of an excessive traffic event.

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

3.2.2 The network (traffic) performance shall be continuously monitored, and alarms shall be generated if malfunctions or reduced/degraded capacity occurs. The alarm detail level shall be sufficient to clearly identify the cause of the failure and related modules shall go to fail safe condition if necessary.

3.2.3 Important inter-node signals shall reach the recipient within a pre-defined time. Any malfunctions shall be alarmed and nodes shall go to fail safe condition if necessary.

Interpretation:

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

---e-n-d---o-f---i-n-t-e-r-p-r-e-t-a-t-i-o-n---

3.2.4 When different main systems are integrated in a common network, the network topology shall be designed with physical segmentation where each main system is allocated to different segments.

(See IEC60092-54, 4.3, 4.6 and 9.5.2)

Interpretation:

1) The integrity and autonomy of each segment should be secured with appropriate network components, e.g. firewalls or routers. It should be possible to protect each segment from unnecessary traffic on the remaining network, and each segment should be able to work autonomously.
2) Virtual networks (VLAN) is not considered satisfactory to meet the requirements for network fault tolerance and segmentation as specified.

---e-n-d---o-f---i-n-t-e-r-p-r-e-t-a-t-i-o-n---

3.3 Network analysis

For complex automation and safety systems, the network with its components, connected nodes, communication links (also external interfaces) shall be subject to an analysis where all relevant failure scenarios are identified and considered.

Interpretation:

1) The requirement is basically applicable for all automation and safety containing nodes connected on a common network. However, for simpler systems, the above requirement is fulfilled by covering the most relevant failure scenarios in a test program.
2) The analysis should demonstrate robustness against network storm and other possible failure scenarios, as fail safe may not be achievable. It should 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.).
3) The main purpose of the analysis is 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.

---e-n-d---o-f---i-n-t-e-r-p-r-e-t-a-t-i-o-n---

3.4 Network test and verification

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

— the main observations/items from the analysis
— self diagnostics, alarming upon different network failures
— worst-case scenarios, network storm
— segment segregation, autonomous operation of segments
— individual controller node integrity, nodes working without network communication
— consequence of single cabinet loss.

3.5 Wireless communication

3.5.1 Wireless technologies may be used in functions that are additional or supplementary to those required by the offshore standard. Any use of wireless technology in functions required by the offshore standard shall be subject to special considerations where the requirements of this chapter is observed.

(See IACS UR E22 sec. 2.4.1)

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

(See IACS UR E22 sec. 2.4.2)

3.5.3 The wireless equipment shall not cause interference to licensed users of the ISM frequency bands in the geographical areas where the vessel/unit shall operate. The radiated power level shall be adjustable.

(See IACS UR E22, sec. 2.4.4)

Guidance note:

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

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

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

(See IACS UR E22, Sec. 2.4.4)

Guidance note:

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

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

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

Guidance note:

The type of modulation used should be of the category spread spectrum and be in compliance with the IEEE 802 series. Direct sequence spread spectrum (DSSS) and frequency hopping spread spectrum (FHSS) are recognised standards for modulation.

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

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

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

(See IACS UR E22, Sec.2.4.3d)

Guidance note:

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

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

3.5.7 In case more than one wireless system shall operate in the same area on board 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.

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

(See IACS UR E22, Sec. 2.4.3a)

Guidance note:

The protocol should be in compliance with the IEEE 802 standard and the nodes should execute at least a 32-bit cyclic redundancy check of the data packets.

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

3.5.9 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.

(See IACS UR E22, Sec. 2.4.3c)

Guidance note:

Secure encryption schemes such as WiFi protected access (WPA) should be used to protect critical wireless data.

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

3.5.10 The data handling and final presentation of information shall comply with the offshore standard and regulations being applicable to the information category.

Guidance note:

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

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

SECTION 4 COMPONENT DESIGN AND INSTALLATION

1 General

1.1 Environmental strains

1.1.1 Safety, automation and telecommunication equipment shall be suitable for marine use, and shall be designed to operate under the environmental conditions as described in [2].

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

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

1.2 Materials

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 materials.

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, shall pipes and equipment conveying oil, water or other fluids or steam under pressure 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 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.

1.3.9 Isolation valves in essential instrument sensor piping and speed control valves in actuator control tubing shall be designed to minimise the possibility of inadvertent mal-operation. Speed control valves in essential control systems shall be locked in position after adjustment.

1.4 Maintenance

Maintenance, repair and performance tests of systems and components shall as far as practicable 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 or transducers to EUC normally in operation at sea.

Guidance note:

The installation should, as far as possible, be built up from easily replaceable components and designed for easy troubleshooting, testing, and maintenance. When a spare component is mounted, only minor adjustments or calibrations of the component 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

All equipment and test points shall be clearly and permanently marked. Transducers, controllers and actuators shall be marked with their corresponding system identification, so that they can be easily and clearly identified on plans and in instrument lists.

Guidance note:

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

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

1.6 Standardisation

Guidance related to standardisation:

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 specified in [2.2] to [2.11], including any of their combinations, represent average adverse conditions to be fulfilled, which will cover the majority of applications on board units. Where the environmental strains will exceed those specified in [2.2] to [2.11], special arrangements and special components shall be considered.

2.1.2 The different environmental parameter classes are defined in Table 1.

Table 1 Parameter class for the different locations on board

Parameter	*Class*	*Location*
Temperature	A	Machinery spaces, control rooms, accommodation, bridge
	B	Inside cabinets, desks, etc. with temperature rise of 5°C or more installed in location A
	C	Pump rooms, holds, rooms with no heating
	D	Open deck, masts and inside cabinets, desks etc. with a temperature rise of 5°C or more installed in location C
Humidity	A	Locations where special precautions are taken to avoid condensation
	B	All locations except as specified for location A
Vibration	A	On bulkheads, beams, deck, bridge
	B	On machinery such as internal combustion engines, compressors, pumps, including piping on such machinery
	C	Masts
EMC	A	All locations except as specified for bridge and open deck
	B	All locations including bridge and open deck
Components and systems designed in compliance with IEC environmental specifications for ships, Publication No. 60092-504, and for EMC, IEC Publication No. 60533, may be accepted after consideration.		

Guidance note:

See IACS UR E10.

For details on environmental conditions for instrumentation, see DNV GL class guidelineDNVGL-CG-0339

Navigation and radio equipment should comply with IEC Publication No. 60945.

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 vessel/unit and with radio-communications should comply with IEC Publication No. 60945 (2002) Clause 9 (covered by EMC class B).

---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 / −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

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

2.4 Temperature

Table 2

Class	*Ambient temperatures*	*Test temperautures*
A	0°C to +45°C	+5°C and +55°C
B	0°C to +55°C	+5°C and +70°C
C	-25°C to +45°C	-25°C and +55°C
D	-25°C to +55°C	-25°C and +70°C

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

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

2.7 Oil contamination

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 1,6 mm (peak value) below 25 Hz
— acceleration amplitude 4,0 g above 25Hz.

2.9 Electromagnetic compatibility

The minimum immunity requirements for equipment are given in Table 2, and the maximum emission requirements are given in Table 3.

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.

Table 3 Minimum immunity requirements for equipment

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

Port	Phenomenon	Basic standard	Performance criteria	Test value
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.				

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

Table 4 Maximum emission requirements for equipment

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

2.10 Inclination

The requirements in DNVGL-OS-D101 Ch.2 Sec.1 [2.2] apply.

2.11 Miscellaneous

2.11.1 In particular applications other environmental parameters may influence the equipment and should be considered, such as:

— 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.

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.

3 Electrical and electronic equipment

3.1 General

Switching of 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

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

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).

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.

Components weighing more than 10 g should not be fastened by their connecting wires only.

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

3.3 Protection provided by enclosure

Enclosures for the equipment shall be made of steel or other flame retardant material capable of providing EMC protection and satisfy the minimum requirements of Table 4. The required degree of protection is defined in IEC 60529.

Table 5 Minimum requirements for enclosures

Class	*Location*	*Degree of protection*
A	Control rooms, accommodation, bridge, local equipment rooms, central equipment room	IP 20
B	Machinery spaces	IP 44
C	Open deck, masts, below floor plates in machinery spaces	IP 56
D	Submerged application	IP 68

More detailed requirements for ingress protection of enclosure types related to location are given in DNVGL-OS-D201 Ch.2 Sec.10 Table 1.

Guidance note:

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

3.4 Cables and wires

Cables and wires shall comply with the requirements in DNVGL-OS-D201.

3.5 Cable installation

Cable installations shall comply with the requirements in DNVGL-OS-D201.

3.6 Power supply

Electrical power supply shall meet requirements described in DNVGL-OS-D201.

3.7 Fibre optic equipment

3.7.1 Fabrication and installation of fibre optic cables shall comply with the requirements of the relevant DNV GL standard for electrical systems and equipment, DNVGL-OS-D201.

Guidance note:

The construction of fibre optic devices should comply with relevant specifications of International Electrotechnical Commission's (IEC) Publications.

---e-n-d---o-f---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 components
— select components to obtain a safe reliable transmission system
— 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.

Guidance note:

Power budget calculations to be available upon request.

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

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. interlock the power to the light sources with the covers, possible to disconnect or lock parts of the system under service, screen laser beams. The safe distance between the light source or fibre end and the eye of the operator may be determined by applying the formula:

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

Safe distance: L (cm); Pn: Nominal power (mW).

---e-n-d---o-f---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.

4 Pneumatic and hydraulic equipment

4.1 Pneumatic equipment

4.1.1 System components and arrangement shall satisfy the requirements in DNVGL-OS-D101 Ch.2 Sec.4 [9.2].

4.1.2 For air supply, the redundancy requirement of DNVGL-OS-D101 Ch.2 Sec.4 [2.1] applies for compressors, pressure reduction units, filters and air treatment units (lubricator or oil mist injector and dehumidifier).

4.1.3 Piping, tubing and components in systems required to operate in a fire scenario shall have adequate fire resistance properties to ensure correct system operation. This is particularly important for systems where pneumatic energy is required to operate or maintain control over the system.

4.2 Hydraulic equipment

System components and arrangement shall satisfy the requirements in DNVGL-OS-D101 Ch.2 Sec.4 [8].

SECTION 5 USER INTERFACE

1 General

1.1 Application

The requirements of this section apply for all DNV GL offshore standards class vessel/units.

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 and user input devices

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

Guidance note:

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

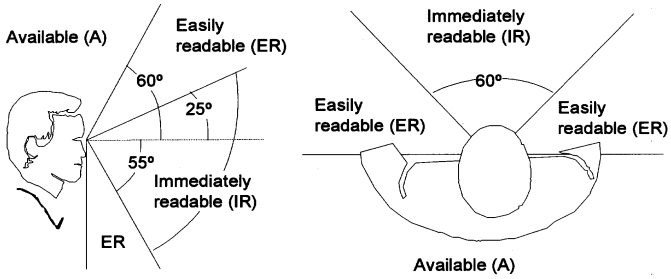

Figure 1 VDU arrangement parameters

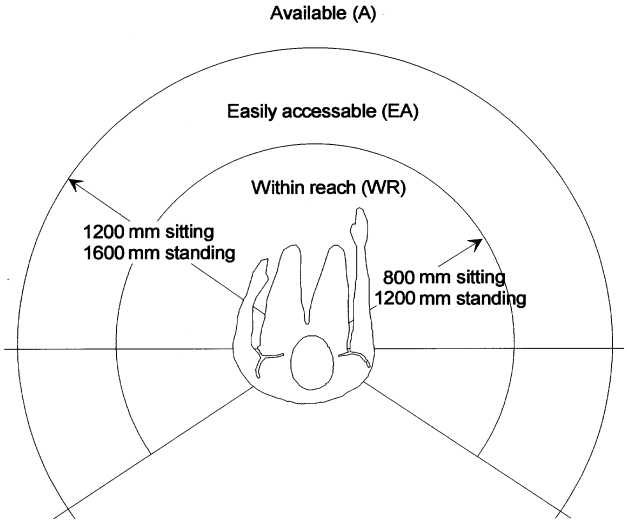

Figure 2 UID arrangement parameters

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

2.1.2 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

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.

Guidance note:

The purpose should ensure easy and understandable operation, e.g. a side thruster lever should be arranged athwart, a propulsion thruster lever should be arranged according to the vessel response. The thruster response should correspond to the lever movement.

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

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 normally 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

3.2.1 The information presented shall be clearly visible to the user and permit easy and accurate reading at a practicable distance in the light conditions normally 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 available at the location of the UID.

3.2.5 Back-up means of operation, see Sec.3 [1.2] normally located in the CCR, shall contain the most important detection and alarms related to fire and gas; activation of ESD levels and active fire protection devices.

Interpretation:

The level of detail in the presentation of fire alarms should as minimum correspond to the available active fire protection devices.

This will normally include:

— remove all inhibits/over-rides/blockings
— active inhibit/over-ride/blocking indication
— fire water pump start and pump status indication
— release of water based extinguishing systems and release confirmation indication
— fire detection status indication
— gas detection
— release of ESD and ESD release confirmation indication
— lamp test, silence buzzer etc.

---e-n-d---o-f---i-n-t-e-r-p-r-e-t-a-t-i-o-n---

3.3 Colours

The use of colours shall be consistent. Red shall be reserved to indicate danger, alarm and emergency only.

Guidance note:

Colour coding of functions and signals should be in accordance with Table 1.

Table 1 Colour coding

Function	*Colour code*
Danger, alarm, emergency	Red
Attention, warning, caution, undefined	Yellow
Status of normal, safe situation	Green

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

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 position.

3.4.2 All UIDs and VDUs shall be fitted with permanent internal or 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 which may affect night vision, upon for example start-up and mode changes.

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

4 Screen based systems

4.1 General

4.1.1 The status of all displayed objects shall be clear and unambiguous, and presentation of displays shall be consistent.

Interpretation:

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

---e-n-d---o-f---i-n-t-e-r-p-r-e-t-a-t-i-o-n---

4.1.2 Alarms shall have priority over any other information presented on the VDU. The entire list of alarm messages shall be easily available.

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

Guidance note:

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

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

4.1.4 For essential and important systems, dedicated and independent 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, switches or joysticks may be accepted after special considerations.

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

4.1.5 Symbols and their associated information in a mimic display shall have a logical relationship.

4.1.6 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 functions 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 Entry of data shall be arranged with a default value prompted by the system and permitted data interval.

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 may 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, there shall not be buffering of more than one user input. Manually initiated time-consuming operations shall be possible to cancel.

SECTION 6 SUPPLEMENTARY REQUIREMENTS FOR DRILLING UNITS

1 Introduction

In addition to the requirements given in this standard, the following requirements apply specially for drilling units.

2 Design principles

Automation and safety system components that are intended to be alive after an incident shall be suitable for ex zone 2 installation or safe by location, see DNVGL-OS-A101 Ch.2 Sec.4 [2.1.4].

3 System design

3.1 General

3.1.1 Distributed automation and safety modules with utilities necessary to operate, located in hazardous area, which is intended to be alive after an incident, shall be able to withstand the design accidental load for the actual area, for an agreed time period.

Guidance note:

Relevant design accidental loads are described in DNVGL-OS-A101 Ch.2 Sec.1.

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

3.1.2 Upon failure of the ESD system, all connected systems shall default to the safest condition for the unit or installation.

Interpretation:

1) Internode signals between F&G and ESD nodes should follow the fail safe principles given in DNVGL-OS-A101 Ch.2 Sec.4 [2.1.3] and DNVGL-OS-A101 Ch.2 Sec.6 [4.2.2].
2) When the fail safe principle is NE, single communication links are accepted, provided that communication failure activates relevant functions accordingly. When the fail safe principle is NDE, the communication link should be redundant in order to be able to activate the function in case of communication failure.

---e-n-d---o-f---i-n-t-e-r-p-r-e-t-a-t-i-o-n---

4 User interface

Back-up means of operation, see Sec.3 [1.2] shall contain the most important action functions and alarm indications related to emergency relocation (if required), gas detection, including activation of active fire protection devices. (See Sec.5 [3.2.5]).

Interpretation:

In addition to Sec.5 [3.2.5] this should typically include:

— release of foam systems and indication of foam system status, if applicable
— gas detection status indication (flammable and toxic)
— facilities for emergency relocation, if applicable
— activation of BOP release sequence (normally located in BOP control panel).

---e-n-d---o-f---i-n-t-e-r-p-r-e-t-a-t-i-o-n---

5 Enhanced system

5.1 General

5.1.1 The following requirement applies only for units with the voluntary notation **ES**.

5.1.2 Alarm philosophy - ES

An alarm philosophy shall be developed for various alarm conditions.

They shall be distinguished by sound and colour and be given at main control stations and unit as applicable.

Guidance note:

Necessary maritime alarms should be located accordingly for any unit. Normally ECR and navigation bridge, according to relevant IMO regulations.

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

5.1.3 Relocation - ES

For units with means for emergency relocation, as required in DNVGL-OS-A101 Ch.2 Sec.6 [4.3.21] this function shall be subject for testing upon completion.

SECTION 7 SUPPLEMENTARY REQUIREMENTS FOR PRODUCTION AND STORAGE UNITS

1 Introduction

In addition to the requirements given in this standard, the following requirements apply specially for floating production and storage units.

2 Design principles

2.1 General

2.1.1 Shutdown or emergency stop commands shall not be reset automatically. Important shutdown devices shall only be reset locally after the initiating shutdown command has been reset by the operator.

Guidance note:

For ESD valves see DNVGL-OS-E201 for details, however it is accepted that blow down valves are equipped with remote reset.

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

2.1.2 Power to relevant parts of the ESD system shall not be tripped by lower ESD levels.

2.1.3 Automation and safety system components that are intended to be alive after an incident shall be suitable for ex zone 2 installation or safe by location, see DNVGL-OS-A101 Ch.2 Sec.4 [2.1.4].

3 System design

3.1 General

3.1.1 Distributed automation and safety modules, located in hazardous area, with utilities necessary to operate, which is required to be alive after an incident, shall be able to withstand the design accidental load for the actual area, for an agreed time period.

Guidance note:

Relevant design accidental aoads are described in DNVGL-OS-A101 Ch.2 Sec.1.

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

3.1.2 For the process plant, the redundancy requirement shall apply for the F&G node(s), see Sec.1 [1.4.2].

Guidance note:

Fire detection in accommodation and engine room including required marine systems the IMO MODU/SOLAS requirement is that such signals have to be routed through the fire panel before being routed to the F&G node. For the process plant it is recommended that fire and gas detectors are connected directly to the F&G node(s) and not through the fire panel.

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

3.1.3 Internode signals between F&G and ESD/PSD nodes shall follow the fail safe principles given in DNVGL-OS-A101 Ch.2 Sec.4 [2.1.3].

Guidance note:

When the fail safe principle is NE, single communication links are accepted, provided that communication failure activates relevant functions accordingly. When the fail safe principle is NDE, the communication link should be redundant in order to be able to activate the function in case of communication failure.

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

3.1.4 Alarm philosophy - ES

An alarm philosophy shall be developed for various alarm conditions.

They shall be distinguished by sound and colour and be given at main control stations and unit as applicable.

Guidance note:

Necessary maritime alarms should be located accordingly for any unit. Normally ECR and Navigation bridge, according to relevant IMO regulations.

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

4 User interface

Back-up means of operation, see Sec.3 [1.2], shall contain the most important action functions and alarm indications related to ESD and F&G detection, including activation of active fire protection devices. (See Sec.5 [3.2.5]).

Interpretation:

In addition to Sec.5 [3.2.5] this should normally include:

— release of foam systems and indication of foam system status, if applicable
— status of vessel boundary shutdown valves
— gas detection status indication (flammable and toxic)
— facilities for emergency relocation, if applicable (see DNVGL-OS-E301 Ch.2 Sec.4 [11.5.9].

---e-n-d---o-f---i-n-t-e-r-p-r-e-t-a-t-i-o-n---

CHAPTER 3 CERTIFICATION AND CLASSIFICATION

SECTION 1 REQUIREMENTS

1 General

1.1 Introduction

1.1.1 As well as representing DNV GL's recommendations on safe engineering practice for general use by the offshore industry, the offshore standards also provide the technical basis for DNV GL classification, certification and verification services.

1.1.2 This chapter identifies the specific documentation, certification and surveying requirements to be applied when using this standard for certification and classification purposes.

1.1.3 A complete description of principles, procedures, applicable class notations and technical basis for offshore classification is given by the DNV GL rules for classification, offshore units, see Table 1.

Table 1 DNV GL rules for classification: offshore units

No.	*Title*
DNVGL-RU-OU-0101	Offshore drilling and support units
DNVGL-RU-OU-0102	Floating production, storage and loading units
DNVGL-RU-OU-0103	Floating LNG/LPG production, storage and loading units
DNVGL-RU-OU-0104	Self-elevating units

1.1.4 This chapter identifies the specific documentation, certification and surveying requirements to be applied when using this standard for certification and classification purposes.

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 unit services. DNVGL-OS-D201 Ch.1 Sec.1 [4.4]

Table 2 System categories

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

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

1.2.2
Classification of automation, safety, and telecommunication systems shall generally be according to the principles of:

— type approval (see [3])
— certification of control, monitoring and safety systems (see [4])
— on-board inspection (visual inspection and functional testing).

Guidance note:

The main principle is that control system components should by type approved and that control systems shall be certified.

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

1.3 Applicable requirements

1.3.1 Requirements as covered by classification are governed by class notations. A complete description of these and their related scope can be found in the above listed rules for MOU.

1.3.2 Requirements applicable only for vessels with the voluntary notation **ES** can be found in the following Offshore Standards.

Table 3 DNV GL offshore standards including ES requirements

No.	*Title*
DNVGL-OS-A101	Safety principles and arrangements
DNVGL-OS-D101	Marine and machinery systems and equipment

No.	Title
DNVGL-OS-D202	Automation, safety and telecommunication systems
DNVGL-OS-D301	Fire protection

1.3.3 Requirements applicable only for vessels with the voluntary notation **ES** as given in this standard are on alarm philosophy as described in Ch.2 Sec.6 [3.1.2].

2 Documentation

2.1 General

2.1.1 Overview documentation as listed in Table 3 is requested submitted early in the approval work, applicable for vessel/units with automation and safety systems installed.

Guidance note:

Typically submitted by yard/manufacturer/designer based upon their detailed specification.

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

2.1.2 Documentation listed in Table 4 is required submitted in order to adequately describe the automation and safety system.

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

Guidance note:

Documentation for a specific automation and safety system should be complete (as required in Table 4) in a limited number of submittals. Priority should be given to documentation providing overall view as supposed to specific details.

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---

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

Guidance note:

ISA 5.1 or ISO 3511-1/2/3/4 are accepted standards.

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

2.1.5 The documentation type number together with identification of the automation and safety system can be used as a unique identifier for the document. The "T" indicates that the documentation type is required also for automation and safety systems where type approved components or software modules are used.

2.1.6 For a system subject to certification, documentation listed in Table 5 shall be available for the surveyor at testing at the manufacturer.

2.1.7 For on-board inspection, documentation listed in Table 6 is required submitted to survey station.

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

Guidance note:

Documentation for a specific automation and safety system should be complete (as required in Table 4) in one submittal, to the extent possible.

Typically submitted by manufacturers based upon their project specific specification.

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

Table 4 Documentation requested submitted at an early stage in the approval work

Documentation type	*Information element*	*Purpose*
System philosophy (I010) (T)	— the tasks allocated to each sub-system, divided between system tasks and manual tasks, including emergency recovery tasks — principles that will be used in the technical implementation of each system.	Information

(typically submitted by yard and/or designer and/or manufacturer based upon their detailed specification, applicable for vessels/units with the automation and safety system installed)

Table 5 Documentation required to describe the automation and safety system

Documentation type	*Information element*	*Purpose*
Functional description (system requirement specification) (I020) (T)	— clear text description of the system configuration — clear text description of scope of supply and what is controlled and monitored as well as how — clear text description of safe state(s) for each function implemented — clear text description of switching mechanisms for systems designed with redundancy R0 — P&I/hydraulic/pneumatic diagrams if relevant.	Approval
System block diagrams (I030) (T)	— a diagram showing connections between all main components (units, modules) of the system and interfaces with other systems. With details showing segregation between F&G, ESD, PSD and PCS systems as well as other systems where relevant.	Approval
User interface documentation (I040)	— a description of the functions allocated to each work and operator station — a description of transfer of responsibility between work and operator stations. — a description of the alarm philosophy	Approval
Power supply arrangement (I050) (T)	— electrical supply: diagram showing connection to distribution board(s), batteries, converters or UPS. Including information regarding Ex/Non Ex as applicable.	Approval
Failure mode description (Z070) (T)	A document describing the effects due to failures in the systems, not failures in the equipment supported by the systems. The following aspects shall be covered: — a list offailures which are subject to assessment, with references to the system documentation — a description of the system response to each of the above failure modes identified — a comment to the consequence of each of these failures.	Information

Documentation type	*Information element*	*Purpose*
Failure mode and effect analysis (FMEA) (Z071) (T) (Only when requested)	A failure modes and effect analysis (FMEA) shall be carried out for the entire system. The FMEA shall be sufficiently detailed to cover all the systems' major components and shall include, but not be limited to, the following information: — a description of all the systems' major components and a functional block diagram showing their interaction with each other — all significant failure modes — the most predictable cause associated with each failure mode — the transient effect of each failure on the vessel/unit. — the method of detecting that the failure has occurred — the effect of the failure upon the rest of the system's ability to maintain it's function — an analysis of possible common failure mode. Where parts of the system are identified as non-redundant and where redundancy is not possible, these parts shall be further studied with consideration given to their reliability and mechanical protection. The results of this further study shall be submitted for review. **Guidance note:** A project specific FMEA would normally only be expected when using new, unproven, technology or to resolve any doubt as to the reliability of the chosen system topology. ---e-n-d---o-f---g-u-i-d-a-n-c-e---n-o-t-e---	Approval
List of control & monitored points (I110) (T)	A list and or index identifying all input and output signals to the system as required in the offshore standard, containing at least the following information: — service description — instrument tag-number — system (control, safety, alarm, indication) — type of signal (digital/analogue input/output).	Approval
Circuit diagrams (I150)	— for essential hard-wired circuits (for emergency stop, shutdown, interlocking, etc.) details of input and output devices and power source for each circuit.	Approval
Test program for testing at the manufacturer (Z120) (T)	Description of test configuration and test simulation methods. Based upon the functional description, each test shall be described specifying: — initial condition — how to perform the test — what to observe during the test and acceptance criteria for each test. The tests shall cover all normal modes as well as failure modes identified in the functional failure analysis, including power and communication failures.	Approval
Data sheets with environmental specifications (I080)	— environmental conditions stipulated in Ch.2 Sec.4 for temperature, vibration, humidity, enclosure and EMC.	Information

Documentation type	*Information element*	*Purpose*
Cause and effect diagrams	— Cause and effect matrix/chart for PSD, ESD and F&G, showing the various inputs and corresponding actions to be taken by the logic, where relevant.	Approval
ESD and F&G overview mimics	A document showing the main ESD and F&G overview mimics.	Information
CAAP Panel Layout	A drawing showing layout of the CAAP panel with information showing all functions, feedbacks and alarms.	Approval
Network documentation requirements	The following information related to the network properties shall be included in the documentation submitted for approval: — topology and network details including power supply arrangement — functional description, with special focus on interfaces — identification of critical network components — qualitative reliability analysis (e.g. FMEA) Failure response test program.	Approval
Documentation of wireless communication	The following information related to the wireless communication shall be included in the documentation submitted for approval: — 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 — sescription of integrity and authenticity measures.	Approval
Software change handling procedure (I320)	Procedure describing how software changes to the system are proposed, evaluated and implemented using a standardized, systematic approach that ensures traceability, consistency and quality; and that proposed changes are evaluated in terms of their anticipated impact on the entire vessel system.	Approval

(typically submitted by manufacturers based upon their project specific specification)

Table 6 Documentation required available for the testing at the manufacturer

Documentation type	*Information element*	*Purpose*
Software quality plan, based upon life cycle activities	The software life cycle activities shall minimum contain procedures for: — software requirements specification — parameters data requirements — software function test — parameter data test — validation testing — system project files stored at the manufacturer — software change handling and revision control. — Software security policy.	Information

Documentation type	*Information element*	*Purpose*
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.	Information
Installation manual	A document providing information about the installation procedures.	Information
Maintenance manual	A document intended for regular use on board providing information about: — maintenance and periodical testing — acceptance criteria — fault identification and repair — list of the suppliers' service net — ship’s systems software, maintenance log.	Information

Table 7 Documentation required for on-board inspection

Documentation type	*Information element*	*Purpose*
Test program for dock and sea trials	— initial condition — what to test — how to perform the test — acceptance criteria for the test	Approval at local DNV GL station

3 Type approval

The main components for essential and important control, monitoring and safety systems covered by the rules of this section 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.

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

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

4 Certification

4.1 General

4.1.1 The certification requirement of the various instrumented systems shall follow the same certification requirement as the EUC. See Ch.1 Sec.1 [2.2] for the list of relevant offshore standards.

4.1.2

Essential and important control, monitoring and safety systems, as specified in the rules, shall be certifiedprovided 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 and adequately assessed during the plan approval.

The certification procedure consists of:

1) plan approval
   - assessment of manufacturer documentation in accordance with the documentation requirements in the rules
   - issuance of approval letter
2) manufacuring survey
   - visual inspection
   - verification/witness test of performance according to functional requirements based on approved test programs
   - verification/witness of failure mode behaviour
   - verification of implementation software quality plan covering life cycle activities, if applicable
3) issuance of certificate.

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

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

— remote control of vessel main functions
— main alarm system
— integrated control and monitoring system.
— safety management systems and decision support systems (where such systems interface the control, monitoring and safety systems required by the rules).

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.

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

5 Inspection and testing

5.1 Manufacturing survey

5.1.1 All test programs shall be approved by DNV GL.

5.1.2 Approval testing according to [4] and Ch.2 Sec.1 [5] shall be performed at the manufacturer's works.

5.2 On board testing

5.2.1 Approval testing shall be carried out as necessary to demonstrate that the overall requirements of testing described in Ch.2 Sec.1 [5.1] to Ch.2 Sec.1 [5.5] have been fulfilled.

5.2.2 A copy of the approved test programme and test record shall be kept on board, and shall be completed with final set points and endorsed by the inspecting party.

5.3 Renewal survey

5.3.1 Correct functioning of the following systems shall be verified, as far as applicable:

— each automation and safety system
— fire & gas system
— ESD/PSD system
— manual control of machinery
— remote control of propulsion machinery.

In connection with the latter point, the following manoeuvres are normally required to be effected:

— from stop to ahead
— from ahead to astern
— stop
— from stop to astern
— stop by operating the emergency device.

5.3.2 It shall be verified that the remote control can be transferred to standby manual control in the engine control room in case of power supply failure to the remote control system.

Guidance note:

This requirement is related to propulsion control.

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

5.3.3 When cancelling of automatic load reduction and/or automatic stop of engine are provided, these functions shall be demonstrated to the satisfaction of the surveyor.

6 Alterations and additions

When an alteration or addition to an approved system is proposed, documentation of the alteration or addition shall be submitted for approval. A survey covering testing and installation of the alteration or addition shall be performed.

CHANGES – HISTORIC

January 2017 edition

Main changes January 2017, entering into force 1 July 2017

• General

Aligment of the standard with DNV GL rules for classification: Ships, and IACS UR E22 and E10 where relevant.

• Ch.1 Sec.1 General

— Ch.1 Sec.1 Table 6: Updated definition of independency, removed some other definitions.

• Ch.2 Sec.1 Design principles

— Ch.2 Sec.1 [1.1.1]: Removed guidance note.
— Ch.2 Sec.1 [1.2]: Updated some clauses and removed guidance note.
— Ch.2 Sec.1 [1.3]: Removed former clause.
— Ch.2 Sec.1 [1.3]: Requirement related to integrated system amended and requirement for functional failure analysis added.
— Ch.2 Sec.1 [1.3]: Added clauses [1.3.1] to [1.3.3] and [1.3.6].
— Ch.2 Sec.1 Table 1: Repair time on high availability systems has been updated.
— Ch.2 Sec.1 [3.1.2]: The clause has been updated.
— Ch.2 Sec.1 [3.2]: Requirement for fail safe functionality related to fire and gas detectionhas been amended.
— Ch.2 Sec.1 [3.2.2]: Clause and guidance note have been updated and interpretation removed.
— Ch.2 Sec.1 [4]: The clause has been updated.
— Ch.2 Sec.1 [5.6.3]: The clause has been updated.

• Ch.2 Sec.2 System design

— Ch.2 Sec.2 [1.4.1]: Updated clause and added interpretation.
— Ch.2 Sec.2 [1.5]: Removed former clause [1.5.11].
— Ch.2 Sec.2 [1.5.3]: Updated former clause to interpretation.
— Ch.2 Sec.2 [1.5.5]: Added guidance note.

• Ch.2 Sec.4 Component design and installation

— Ch.2 Sec.4 [1.3.2]: The clause has been updated.
— Ch.2 Sec.4 [2.1.1]: The clause has been updated.
— Ch.2 Sec.4 [2.4]: Updated original information and included in new [Table 2].
— Ch.2 Sec.4 [2.8]: Updated various values.
— Ch.2 Sec.4 [3.1]: Previous clause [3.1.1] and [3.1.3] have been rmoved.
— Ch.2 Sec.4 [3.4]: Previous clause [3.4.2] has been removed.

• Ch.2 Sec.5 User interface

— Ch.2 Sec.5 [3.1]: A new clause Ch.2 Sec.5 [3.1.4] replace former guidance note.
— Ch.2 Sec.5 [3.2.5]: The guidance note has been removed.

• Ch.2 Sec.6 Supplementary requirements for drilling units

— Ch.2 Sec.6 [4]: The guidance note has been updated to an interpretation.
— Ch.2 Sec.6 [5.1.3]: A new clause has been added.

• Ch.2 Sec.7 Supplementary requirements for production and storage units

— Ch.2. Sec.7 [4]: Updated guidance note to interpretation.

• Ch.3 Sec.1 Requirements

— Ch.3 Sec.1 [1.2]: Rewritten content and added a description of the classification principles for control, monitoring and safety systems.
— Ch.3 Sec.1 Table 5: A software change handling procedure required for approval has been updated.
— Ch.3 Sec.1 [Table 6]: A software security policy as part of the software quality plan has been updated.
— Ch.3 Sec.1 [3]: A new clause has been added.
— Ch.3 Sec.1 [4]: Requirement for type approval of main components has been rewritten.

July 2015 edition

Main changes July 2015

• General

The revision of this document is part of the DNV GL merger, updating the previous DNV standard into a DNV GL format including updated nomenclature and document reference numbering, e.g.:

— Main class identification **1A1** becomes **1A**.
— DNV replaced by DNV GL.
— DNV-RP-A201 to DNVGL CG 0168. A complete listing with updated reference numbers can be found on DNV GL's homepage on internet.

To complete your understanding, observe that the entire DNV GL update process will be implemented sequentially. Hence, for some of the references, still the legacy DNV documents apply and are explicitly indicated as such, e.g.: Rules for Ships has become DNV Rules for Ships.

• Ch.2 Sec.1 General

— Sec.1 [3.2.2]: Interpretation on description of failure of detectors has been updated.

• Ch.2 Sec.4 Component design and installation

— Sec.4 Table 2: Removal of the 10KHz test value on conducted radio frequency interference including accompanying note

About DNV GL

DNV GL is a global quality assurance and risk management company. Driven by our purpose of safeguarding life, property and the environment, we enable our customers to advance the safety and sustainability of their business. We provide classification, technical assurance, software and independent expert advisory services to the maritime, oil & gas, power and renewables industries. We also provide certification, supply chain and data management services to customers across a wide range of industries. Operating in more than 100 countries, our experts are dedicated to helping customers make the world safer, smarter and greener.

SAFER, SMARTER, GREENER