

OFFSHORE STANDARD
DNV-OS-D202

AUTOMATION, SAFETY, AND
TELECOMMUNICATION SYSTEMS

OCTOBER 2008

DET NORSKE VERITAS

FOREWORD

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

DNV Offshore Codes consist of a three level hierarchy of documents:

- *Offshore Service Specifications*. Provide principles and procedures of DNV classification, certification, verification and consultancy services.
- *Offshore Standards*. Provide technical provisions and acceptance criteria for general use by the offshore industry as well as the technical basis for DNV offshore services.
- *Recommended Practices*. Provide proven technology and sound engineering practice as well as guidance for the higher level Offshore Service Specifications and Offshore Standards.

DNV Offshore Codes are offered within the following areas:

- A) Qualification, Quality and Safety Methodology
- B) Materials Technology
- C) Structures
- D) Systems
- E) Special Facilities
- F) Pipelines and Risers
- G) Asset Operation
- H) Marine Operations
- J) Wind Turbines
- O) Subsea Systems

Amendments and Corrections

Whenever amendments and corrections to the document are necessary, the electronic file will be updated and a new Adobe PDF file will be generated and made available from the Webshop (<http://webshop.dnv.com/global/>).

Comments may be sent by e-mail to rules@dnv.com

For subscription orders or information about subscription terms, please use distribution@dnv.com

Comprehensive information about DNV services, research and publications can be found at <http://www.dnv.com>, or can be obtained from DNV, Veritasveien 1, NO-1322 Høvik, Norway; Tel +47 67 57 99 00, Fax +47 67 57 99 11.

© Det Norske Veritas. All rights reserved. No part of this publication may be reproduced or transmitted in any form or by any means, including photocopying and recording, without the prior written consent of Det Norske Veritas.

Computer Typesetting (FM+SGML) by Det Norske Veritas.

If any person suffers loss or damage which is proved to have been caused by any negligent act or omission of Det Norske Veritas, then Det Norske Veritas shall pay compensation to such person for his proved direct loss or damage. However, the compensation shall not exceed an amount equal to ten times the fee charged for the service in question, provided that the maximum compensation shall never exceed USD 2 million.
In this provision "Det Norske Veritas" shall mean the Foundation Det Norske Veritas as well as all its subsidiaries, directors, officers, employees, agents and any other acting on behalf of Det Norske Veritas.

CHANGES

- **General**

Being class related, this document is published electronically only (as of October 2008) and a printed version is no longer available. The update scheme for this category of documents is different compared to the one relevant for other offshore documents (for which printed versions are available).

For an overview of all types of DNV offshore documents and their update status, see the “Amendments and Corrections”

document located at: <http://webshop.dnv.com/global/>, under category “Offshore Codes”.

This document supersedes the previous edition dated April 2008.

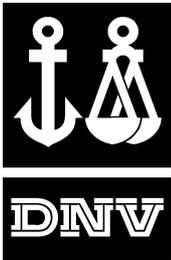
- **Main changes as of October 2008:**

- Clarification of “secondary means of operation” for the Operator Station, in particular general requirements for a CAAP.
- Chapter 2, Section 3, B100 System Software.

CONTENTS

| | |
|---|---|
| CH. 1 INTRODUCTION 7 | Sec. 3 Additional Requirements for Computer Based Systems..... 21 |
| Sec. 1 General 9 | A. General Requirements 21 |
| A. Introduction 9 | A 100 Assignment of responsibility when installing integrated systems..... 21 |
| A 100 Objectives 9 | A 200 System dependency 21 |
| A 200 Scope and application 9 | A 300 Storage devices 21 |
| A 300 Organisation of contents 9 | A 400 Computer usage 21 |
| A 400 Alterations and additions 9 | A 500 System response and capacity 21 |
| A 500 Assumptions 9 | A 600 Temperature control 21 |
| B. References 9 | A 700 System maintenance 21 |
| B 100 Normative references 9 | A 800 System access 21 |
| B 200 Offshore standards 10 | B. System Software 22 |
| C. Definitions 10 | B 100 Software requirements 22 |
| C 100 Verbal forms 10 | B 200 Software manufacturing 22 |
| C 200 General terms 10 | C. Network Systems and Communication Links 22 |
| C 300 Terms related to computer based system 11 | C 100 General 22 |
| C 400 Abbreviations 12 | C 200 Serial communication 23 |
| CH. 2 TECHNICAL PROVISIONS 13 | C 300 Network communication 23 |
| Sec. 1 Design Principles..... 15 | C 400 Network analysis 23 |
| A. System Configuration 15 | C 500 Network test and verification 24 |
| A 100 General 15 | C 600 Wireless communication 24 |
| A 200 Field instrumentation 15 | Sec. 4 Component Design and Installation 25 |
| A 300 System 15 | A. General 25 |
| A 400 Integrated systems 15 | A 100 Environmental strains 25 |
| A 500 Redundancy 15 | A 200 Materials 25 |
| B. System Availability 15 | A 300 Component design and installation 25 |
| B 100 General 15 | A 400 Maintenance 25 |
| B 200 Continuous availability (R0) 16 | A 500 Marking 25 |
| B 300 High availability (R1) 16 | A 600 Standardisation 25 |
| B 400 Manual system restoration (R2) 16 | B. Environmental Conditions, Instrumentation 25 |
| B 500 Repairable systems (R3) 16 | B 100 General 25 |
| C. Response to Failures 16 | B 200 Electric power supply 26 |
| C 100 Failure detection 16 | B 300 Pneumatic and hydraulic power supply 26 |
| C 200 Fail-safe functionality 16 | B 400 Temperature 26 |
| D. Back up Functions and Emergency Operation 16 | B 500 Humidity 26 |
| D 100 General 16 | B 600 Salt contamination 26 |
| E. User Interface 16 | B 700 Oil contamination 26 |
| E 100 General 16 | B 800 Vibrations 26 |
| F. Tests 17 | B 900 Electromagnetic compatibility 26 |
| F 100 General 17 | B 1000 Inclination 27 |
| F 200 Software module testing 17 | B 1100 Miscellaneous 28 |
| F 300 Integration testing 17 | C. Electrical and Electronic Equipment 28 |
| F 400 System testing 17 | C 100 General 28 |
| F 500 On-board testing 17 | C 200 Mechanical design, installation 28 |
| Sec. 2 System Design..... 18 | C 300 Protection provided by enclosure 28 |
| A. System Elements 18 | C 400 Cables and wires 28 |
| A 100 General 18 | C 500 Cable installation 28 |
| A 200 Automation system 18 | C 600 Power supply 28 |
| A 300 Propulsion remote control 18 | C 700 Fibre optic equipment 28 |
| A 400 Safety 18 | D. Pneumatic and Hydraulic Equipment 29 |
| A 500 Alarm philosophy 19 | D 100 Pneumatic equipment 29 |
| A 600 Alarms 19 | D 200 Hydraulic equipment 29 |
| A 700 Indication 20 | Sec. 5 User Interface 30 |
| A 800 Planning and reporting 20 | A. General 30 |
| A 900 Calculation, simulation and decision support 20 | A 100 Application 30 |
| B. General Requirements 20 | A 200 Introduction 30 |
| B 100 System operation and maintenance 20 | B. Workstation Design and Arrangement 30 |
| B 200 Power distribution 20 | B 100 Location of visual display units and user input devices 30 |
| | C. User Input Device and Visual Display Unit Design 30 |
| | C 100 User input devices 30 |
| | C 200 Visual display units 30 |
| | C 300 Colours 30 |

| | | | | |
|--|--|-----------|---|-----------|
| C 400 | Requirements for preservation of night vision (UIDs and VDUs for installation on the navigating bridge)..... | 31 | B. Design Principles | 33 |
| | | | B 100 General | 33 |
| D. Screen Based Systems | | 31 | C. System Design | 33 |
| D 100 General | | 31 | C 100 General | 33 |
| D 200 Illumination | | 31 | D. Additional Requirements for Computer Based Systems | 33 |
| D 300 Colour screens | | 31 | D 100 General | 33 |
| D 400 Computer dialogue | | 31 | E. Component Design and Installation..... | 34 |
| D 500 Application screen views | | 31 | E 100 General | 34 |
| Sec. 6 Supplementary Requirements for Drilling Units | | 32 | F. User Interface..... | 34 |
| A. General..... | | 32 | F 100 General | 34 |
| A 100 Introduction..... | | 32 | CH. 3 CERTIFICATION AND CLASSIFICATION 35 | |
| B. Design Principles | | 32 | Sec. 1 Certification and Classification - Requirements | 37 |
| B 100 General | | 32 | A. General | 37 |
| C. System Design | | 32 | A 100 Introduction..... | 37 |
| C 100 General | | 32 | A 200 Organisation of Ch.3 | 37 |
| D. Additional Requirements for Computer Based Systems | | 32 | A 300 Classification principles..... | 37 |
| D 100 General | | 32 | B. Documentation..... | 37 |
| E. Component Design and Installation | | 32 | B 100 General | 37 |
| E 100 General | | 32 | C. Certification | 41 |
| F. User Interface | | 32 | C 100 General | 41 |
| F 100 General | | 32 | D. Inspection and Testing | 42 |
| Sec. 7 Supplementary Requirements for Production and Storage Units..... | | 33 | D 100 Manufacturing survey | 42 |
| A. General..... | | 33 | D 200 On board testing | 42 |
| A 100 Introduction..... | | 33 | D 300 Renewal survey | 42 |
| | | | E. Alterations and Additions | 42 |
| | | | E 100 General | 42 |



CHAPTER 1

INTRODUCTION

| CONTENTS | PAGE |
|----------------------|------|
| Sec. 1 General | 9 |

SECTION 1 GENERAL

A. Introduction

A 100 Objectives

101 The objectives of this standard are to:

- 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.

Guidance note:

Additional requirements for specific applications will be given in the DNV Offshore Standard covering those applications.

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

A 200 Scope and application

201 The requirements of this standard, shall apply to all safety, automation, and telecommunication systems required by the DNV Offshore Standards.

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

203 The requirements of this standard are considered to meet the regulations of the “1989 MODU Code”, with regard to safety, automation, and telecommunication systems.

204 For telecommunication only relevant parts are applicable. For specific requirement to telecommunication equipment reference is made to DNV-OS-A101 Sec.6 F.

A 300 Organisation of contents

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

302 Ch.2 Sec.6 gives supplementary requirements to Drilling Units.

Guidance note:

It should be noted that separate automation and safety requirements related to DRILLING PLANT is described in DNV-OS-E101.

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

303 Ch.2 Sec.7 gives supplementary requirements to Oil and Gas Production and Storage Units

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

A 400 Alterations and additions

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

402 When an alteration or addition to the approved system(s) is proposed, plans shall be submitted for approval. The alterations or additions shall be presented under inspection, and the installation and testing shall be to the inspecting party's satisfaction.

403 Details of proposed hardware and software modifications shall be submitted for evaluation. Where the modification may affect compliance with the offshore standard, proposals for verification and validation shall also be submitted.

404 Software versions shall be identifiable as required in Ch.2 Sec.3.

405 If remote software maintenance is arranged for onboard, the installation of new software versions submitted from software suppliers requires the below items and or actions to be fulfilled:

- a) no modification shall be possible without the acceptance and acknowledgement by the vessel/ unit's responsible
- b) the objective or reason for updating a software module shall be documented in the vessel/unit systems/software maintenance log
- c) any revision which may affect compliance with the standard shall be approved by the Approval centre and evidence of such shall be available onboard
- d) an installation procedure and required pre-requisites for installation of the software module shall be available
- e) the security of the installation process and integrity of the new software shall be verified (especially when software has been transferred using open lines like the Internet)
- f) a test program for verification of correct installation and correct functioning of the functions shall be available
- g) in the case that the new software module has not been successfully installed, the previous version of the system shall be available for re-installation and re-testing (as a roll back function).

A 500 Assumptions

501 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.

B. References

B 100 Normative references

101 The standards listed in Table B1 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 B1 Normative references | |
|-------------------------------|--|
| Reference | Title |
| 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 |
| Classification Note 45.1 | Electromagnetic Compatibility |
| IMO Resolution A.830.19 | Code on alarms and indicators. |

B 200 Offshore standards

201 The latest revision of the DNV Offshore standards listed in table B2 applies.

| Standard | Title |
|-------------|--|
| DNV-OSS-101 | Rules for Classification of Offshore Drilling and Support Units |
| DNV-OSS-102 | Rules for Classification of Floating Production, Storage and Loading Units |
| DNV-OS-A101 | Safety Principles and Arrangement |
| DNV-OS-D101 | Marine Machinery Systems and Equipment |
| DNV-OS-D201 | Electrical Installations |
| DNV-OS-D301 | Fire Protection |
| DNV-OS-E101 | Drilling Plant |
| DNV-OS-E201 | Oil and Gas processing systems |
| DNV-OS-E301 | Position Mooring. |

| Standard | Title |
|----------------------------|---|
| Certification Note No. 1.2 | Type Approval |
| Certification Note No. 2.4 | Environmental Test Specification for Instrumentation and Automation Equipment |
| 1989 MODU Code (IMO) | Code for the Construction and Equipment of Mobile Offshore Drilling Units, 1989, as amended |
| IMO FSS Code | International code for fire systems. |

C. Definitions

C 100 Verbal forms

101 *Shall*: Indicates requirements strictly to be followed in order to conform to this standard and from which no deviation is permitted.

102 *Should*: Indicates that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others, or that a certain course of action is preferred but not necessarily required. Other possibilities have to be agreed upon.

103 *May*: Verbal form used to indicate a course of action permissible within the limits of the standard.

104 *Agreement, agreed or by agreement*: Unless otherwise indicated, agreed in writing between contractor and purchaser.

C 200 General terms

201 *Automation system*: A system that is able to control, and/or monitor fully or partly, the operation of equipment under control (EUC).

202 *Monitoring system*: A system that is able to monitor and issue alarms relating to the operation of an equipment under control (EUC).

203 *Safety system*: A system able to detect the need for and perform safety actions, - such as shut-down of an equipment under control (EUC).

204 *Telecommunication system*: A system providing internal communication within the unit (e.g. telephones, public address, general alarm) or externally to the unit (e.g. radio).

205 *Alarm*: A 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.

206 *Safety shutdown*: A 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.

207 *System*: A 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.

208 *An essential safety, automation or telecommunication system* (hereafter called an *essential system* or *essential function*): A 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 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---of---G-u-i-d-a-n-c-e---n-o-t-e---

209 *An important safety, automation or telecommunication system* (hereafter called an *important system* or *function*): A system supporting functions in order to perform in accordance to class requirement, unless specified otherwise in other DNV Offshore standards.

210 *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 Offshore Standards.

211 *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.

212 Process segment: A collection of mechanical equipment with its related field instrumentation, e.g. a machinery or a piping system. Process segments belonging to essential systems are referred to as essential.

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

214 User: Any human being that will use a system or device, e.g. captain, navigator, engineer, radio operator, stock-keeper, etc.

215 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.

216 System availability: The time the system is available.

217 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.

218 Process: The result of the action performed by the EUC.

219 Indications: The visual presentation of values for the EUC or system status to a user (lamps, dials, VDU displays, etc.).

220 Uninterruptible power supply (UPS): A device supplying output power in some limited time period after loss of input power with no interruption of the output power.

221 Interdependency: 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. Redundancy may provide the necessary independence.

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.

222 Redundancy: A system with redundancy is one with duplication which prevents failure of the entire system in the event of failure of a single component.

223 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.

224 Back-up control system: Comprises all hardware and software necessary to maintain control when main control systems have failed, malfunctioned or are being maintained.

225 Safety and automation system: 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), Safety and Automation System (SAS), Safety and Instrumentation System (SIS).

The term is also commonly used on stand alone system not integrated with other systems.

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

226 Separated: Terms used on cables, networks nodes, etc. to indicated 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---of---G-u-i-d-a-n-c-e---n-o-t-e---

227 Warning: An indication of equipment under control (EUC) or system state that needs attention.

228 Approval centre: The body that is performing the verification of the design and/or fabrication surveys.

229 Fire panel: A stand alone system for presenting of fire alarms and system failure.

230 A normally energised (NE) circuit: A circuit where energy is present when the circuit is not activated by the activating function.

231 A normally de-energised (NDE) circuit: A circuit where energy is present when the circuit is activated by the activating function.

C 300 Terms related to computer based system

301 Complex system: A 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.

302 Computer: A computer includes any programmable electronic system, including main-frame, mini-computer or micro-computer (PLC).

303 Visual display unit (VDU): Any area where information is displayed including indicator lamps or panels, instruments, mimic diagrams, and computer display monitors.

304 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.

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

306 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 controlled or monitored.

307 Software module: A small self-contained program which carries out a clearly defined task and is intended to operate within a larger program.

308 Function block: A 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.

309 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.

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

311 *A node in a system:* A 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).

312 *Point to point:* Link used for data communication between two dedicated nodes.

313 *Local area network:* A network used for data communication between the automation, safety and the other parts of a system, and between different systems.

314 *Instrument net:* A network used for data communication within the field instrumentation connecting instruments in a network.

315 *Multifunction VDU's and UID's:* VDU's and UID's that are used for more than one essential and / or important function for both safety and/or automation, e.g. VDU's and UID's used for integrated computer systems.

316 *Critical Alarm and Action Panel:* Panel used to present vital safety related information, and to activate vital safety related functions independent of operator stations.

317 *Operator Station* in an integrated system is a unit consisting of a user interface, i.e. UID's and VDU, and interface controller(s). An integrated operator station is one serving two or more systems.

318 *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.

319 *Network components:* All hardware devices directly connected to a communication network.

C 400 Abbreviations

401 The abbreviations given in Table C1 are used.

| Table C1 Abbreviation | |
|------------------------------|---|
| <i>Abbreviation</i> | <i>In full</i> |
| 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 |
| 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 |
| I/O | Input and/or Output |
| 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 |
| OTDR | Optical Time Domain Reflectometry |
| PCS | Process Control System |
| RPM | Rotations Per Minute |
| RP | Redundant Propulsion |
| PROM | Programmable Read Only Memory |
| UID | User Input Device |
| UPS | Uninterruptible Power System |
| VDU | Visual Display Unit. |
| VMS | Vessel Management System |



CHAPTER 2

TECHNICAL PROVISIONS

| CONTENTS | PAGE |
|---|------|
| Sec. 1 Design Principles..... | 15 |
| Sec. 2 System Design..... | 18 |
| Sec. 3 Additional Requirements for Computer Based Systems..... | 21 |
| Sec. 4 Component Design and Installation | 25 |
| Sec. 5 User Interface | 30 |
| Sec. 6 Supplementary Requirements for Drilling Units | 32 |
| Sec. 7 Supplementary Requirements for Production and Storage Units..... | 33 |

SECTION 1 DESIGN PRINCIPLES

A. System Configuration

A 100 General

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

Guidance note:

The system should be designed so that a failure in the automation function does not have any impact on the safety function. Other items are use of selective fusing of electrical distribution systems.

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

102 Failure of any safety and automation system shall initiate an audible and visual alarm at a manned control station and shall not prevent manual control.

A 200 Field instrumentation

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

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

203 When manual emergency operation of an essential process segment is required, the field instrumentation required for the manual emergency operation shall be independent of other parts of any system.

204 When traditional mechanical components are replaced by electronic components, these components shall have the same reliability as the mechanical component being replaced.

Guidance note:

Electronic governors should have power supply independent of other consumers and system availability of R0. Speed sensor cabling should be mechanically well protected.

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

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

A 300 System

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

A 400 Integrated systems

401 Essential systems, excluding common process segments, shall be independent of other systems.

402 Non-important systems or parts of non-important systems, which may affect essential or important systems shall meet the requirement for the relevant system it is connected to.

403 UID's for operation shall only be available at workstations from which operation is permitted.

404 There shall be sufficient VDU's or other panels to ensure both overview and detailed information for relevant safety systems.

Guidance note:

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 using other VDU's to obtain detailed information about the incident.

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

Guidance note:

The number of VDU's and UID's 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.

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

A 500 Redundancy

501 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/or automation system.

502 Automatic switching between two systems shall not be dependent on only one of the systems.

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

Guidance note:

Redundancy of computers should be limited to controllers with CPU's; 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 loop 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---of---G-u-i-d-a-n-c-e---n-o-t-e---

B. System Availability

B 100 General

101 The time the system is available, shall be adapted to the redundancy requirements imposed on the system served.

102 Typical system availability for the different categories are given in Table B1.

| Table B1 System availability | |
|-------------------------------------|--------------------|
| <i>System category</i> | <i>Repair time</i> |
| Continuous availability (R0) | None |
| High availability (R1) | 30 s |
| Manual system restoration (R2) | 10 minutes |
| Repairable systems (R3) | 3 hours |

B 200 Continuous availability (R0)

201 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.

202 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.

203 User interfaces of redundant systems shall allow super-

vision of both systems from the same position.

B 300 High availability (R1)

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

302 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.

303 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.

B 400 Manual system restoration (R2)

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

B 500 Repairable systems (R3)

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

C. Response to Failures

C 100 Failure detection

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

Failures detected shall initiate alarms in an assigned manned control station.

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

- power failures
- sensor and actuator failures.

and additionally for computer based systems:

- communication errors
- computer hardware failures
- software execution failures
- software logical failures.

C 200 Fail-safe functionality

201 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:

References also made to DNV-OS-A101, Sec.5 C.

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

202 If single fire or gas detectors are used for each detection area, fail safe action should be taken on instrument failure, meaning confirmed fire or gas.

Guidance note:

If shutdown logic requires no shutdown action on confirmed fire/gas detection, detector failure should also only give alarm with equal priority. Normally local HVAC should be tripped on gas detection in the inlets and then detector failure should also cause HVAC trip.

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

D. Back up Functions and Emergency Operation

D 100 General

101 For functions where back up and/or manual emergency operation is required, this shall be used to maintain a minimum functionality in case of major system failures.

Guidance note:

This implies that back-up or emergency functions should be implemented in systems that are independent of the system in control, and be equipped with the necessary minimum of readily available and simple to use operator interface.

See also Sec.3 A201.

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

E. User Interface

E 100 General

101 When designing the layout of operation and display devices, due consideration shall be given to the user interface. Attention shall be paid to the significance of human factors in the event that a critical failure or condition occurs. Graphic information systems shall contain all relevant functions for safe operation, shall be easy to understand and operate, and shall enable system overview.

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

F. Tests

F 100 General

101 All relevant tests shall be according to a test program, approved by the Approval centre.

102 Testing according to 200, 300, and 400 shall be performed at the manufacturers' works.

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

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

- tools for system set-up and configuration of the EUC
- implementation of software quality plan.

104 The tests and visual examinations shall verify that all requirements given by the applicable DNV Offshore Standards are met. The test procedures shall specify in detail how the various functions shall be tested and what is to be observed during the tests.

105 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.

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

F 200 Software module testing

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

202 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.

F 300 Integration testing

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

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

- 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 Offshore Standards. Function tests are also to include a degree of performance testing outside of the normal operating parameters.
- e) User interface tests.

Guidance note:

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

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

F 400 System testing

401 System tests includes the entire system, integrating all

hardware and software. The test may also include several systems.

402 System tests shall be performed with the software installed on the actual systems to be used on-board, interconnected to demonstrate the functions of the systems.

403 The tests shall include those tests which were not or could not be completed on hardware component or software module level.

F 500 On-board testing

501 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 the automation and safety 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.

Guidance note:

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 normal system is disabled as far as practical.

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

502 A copy of the approved test programme shall be kept on the installation, completed with final set points.

503 The test program for harbour and sea trials shall be approved prior to tests by the Approval centre.

504 Hydraulic automation and shut-down systems with on or off regulation 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.

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

SECTION 2 SYSTEM DESIGN

A. System Elements

A 100 General

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

102 System elements belong to the categories:

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

103 The safety and automation system shall be designed as mutually independent systems. The different elements must not be designed as one combined system, where safety functions are combined with automation functions.

Guidance note:

Mutual independence is required on each node such as ESD/PSD, F&G, PCS, VMS, and DCS as applicable, while Operator Stations for each node is accepted on a common redundant network provided robustness against common failures (i.e. network storm).

The exception is safety system for load reduction, i.e. for propulsion engines.

Manufactures that delivers parts of a larger system should also meet the requirements of independence between automation and safety functions.

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

A 200 Automation system

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

202 The automation system 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.

203 Automatic functions such as automatic starting and other automatic operations, when relevant, shall include provisions for manually overriding the automatic controls unless designed according to SOLAS Ch. II-1/31.1 and 31.5.1 or safe manual operation is not feasible. Failure of any part of such systems shall not prevent the use of the manual override.

204 In closed loop systems, feedback failures shall initiate an alarm, and the system shall fail to safety which normally implies either to remain in its present state or move controlled to a predefined safe state.

205 Remote control of important and essential systems shall meet the requirements described in Sec.2 and Sec.3 as applicable.

A 300 Propulsion remote control

301 At the remote command location, the user shall receive continuous information on the effects of his or her orders.

302 One command location is to be designated as the main command location. The main command location is to be independent of other command locations.

303 When control is possible from several locations, only one shall be in control at a time.

304 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. The main command location shall be able to take control without acknowledgement, but an audible warning must be given at the work station that thereby lose control either partly or completely. The device for taking control shall not be integrated in the normal operating devices (e.g. levers or pushbuttons).

Guidance note:

Examples of situations where audible warning should be given:

- 1) autopilot losing control of one out of two rudders/thrusters,
- 2) autopilot losing control of a single rudder/thrusters when manual control is taken from the lever/wheel,
- 3) control panel on bridge for mechanically driven propulsion thrusters losing control of engine rpm or propeller pitch when control is taken from ECR or locally.

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

Guidance note:

There may be several main command locations on different levels. For example: for remote control of propulsion machinery, the engine control room is normally the main control station. For remote control of propulsion thrusters however, the bridge is the main work station as the propulsion control is integrated with the steering function for which the bridge is main control position.

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

305 Means shall be provided to prevent significant alteration of process equipment parameters when transferring control from one location to another or from one means or mode of operation to another. If this involves manual alignment of control levers, indicators shall show how the levers are to be set to become aligned, and it shall not be possible to bypass the alignment process.

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

307 Control system elements shall include safety interlocks when the consequence of erroneous user actions may lead to major damages or loss of essential or important functions.

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

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

Guidance note:

Hardwired safety interlocks should not be overridden by programmable interlocks.

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

A 400 Safety

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

For fail safe condition reference is made to DNV-OS-A101 Sec.5 C

402 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.

403 Automatic safety actions shall initiate alarm at manned workstations.

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

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

406 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.

407 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 shall be activated prior to a protective safety action, except when it is regarded as not being possible due to urgency, ref. relevant parts of SOLAS Ch. II-1.

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

A 500 Alarm philosophy

501 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 must be located accordingly for any unit. Normally ECR and Navigation bridge, according to relevant IMO regulations.

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

502 The alarm system on the vessel/ unit, alarms distributed to the entire vessel/ unit shall be as simple as possible and shall comply with relevant IMO regulations.

A 600 Alarms

601 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.

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

Guidance note:

IMO resolution A.830 (19) regulation 3.16, requires that alarms and indicators on the navigation bridge should be kept at a minimum. Alarms and indicators not required for the navigation bridge should not be placed there unless permitted by the administration.

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

Guidance note:

For PA/GA alarms see DNV-OS-A101 Sec.6 F for details.

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

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

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

604 The audible and visual characteristics of alarm signals defined by IMO Resolution A.830(19), *Code on Alarms and Indicators - Paragraph 6 Characteristics*, shall be used.

605 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.

606 Presentation and acknowledgement of alarms shall only be possible at the workstation(s) dedicated to respond to the alarm.

Guidance note:

Alarm lists may be available on any workstation.

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

607 All alarms shall initiate an audible signal and a visual indication at the workstation. The indication of an un-acknowledged alarm shall be clearly distinguishable from the indication of an acknowledged alarm. Silencing of the audible signal and acknowledgement of the alarm shall be arranged as follows:

- 1) Silencing the audible signal. Silencing will cause the audible signal to cease in addition to eventual external rotating lights etc. The visual alarm indication on the workstation remains unchanged, normally flashing.
- 2) Acknowledgement of the alarm. When the alarm is acknowledged, the visual indication on the workstation shall remain in alarm state (normally steady red indication) until the alarm condition ceases. If the audible signal is not silenced before the acknowledgement of the alarm, the acknowledgement shall include silencing. An active alarm signal shall not prevent initiation of any new alarm with its audible and visual indication. This is also valid for group - alarms.

Guidance note:

Flashing red indication is normally used for un-acknowledged alarm while steady red is used for active, acknowledged alarm.

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

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

609 Local equipment audible alarm for equipment connected to the automation and safety system, shall be suppressed when localised in the same workplace as the user interface for the automation and safety system.

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

611 Sufficient information shall be provided to ensure optimal alarm handling. Alarm text shall be easily understandable.

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

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

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

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

A 700 Indication

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

702 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.

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

A 800 Planning and reporting

801 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.

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

Guidance note:

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

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

A 900 Calculation, simulation and decision support

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

Guidance note:

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

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

B. General Requirements

B 100 System operation and maintenance

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

102 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.

103 Testing of essential systems and alarm systems shall be possible during normal operation. The system shall not remain in test mode unintentionally.

Guidance note:

Automatic return to operation mode or alarm should be arranged.

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

B 200 Power distribution

201 Requirements are given in DNV-OS-D201.

SECTION 3 ADDITIONAL REQUIREMENTS FOR COMPUTER BASED SYSTEMS

A. General Requirements

A 100 Assignment of responsibility when installing integrated systems

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

Guidance note:

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

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

A 200 System dependency

201 Where an integrated operator station is part of an essential function, back-up or emergency means of operation of the essential functions shall be provided, which to the largest extent possible shall be independent of the integrated operator station and network.

Guidance note:

Some essential systems will, as required by other parts of the standards/rules, require control from a local position independently from remote control.

The back-up means of operation is typically achieved by provision of a CAAP (Critical Alarm and Action Panel) interfaced directly to the node(s).

The back-up means of operation could be provided by additional Operator Stations, providing that they have communication to the node(s), mutually independent from the integrated Operator Station communications.

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

A 300 Storage devices

301 The on-line operation of essential functions shall not depend on the operation of rotating bulk storage devices.

Guidance note:

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

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

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

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

A 400 Computer usage

401 Computers serving essential and important functions shall only be used for purposes relevant to unit operation, taken due notice of separation between safety functions and other control/operational functions.

A 500 System response and capacity

501 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 A1 Typical response times | |
|--|-------------------------------|
| <i>Function</i> | <i>Typical response times</i> |
| 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---of---G-u-i-d-a-n-c-e---n-o-t-e---

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

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

A 600 Temperature control

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

A 700 System maintenance

701 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.

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

A 800 System access

801 Access to system set-up or configuration functions for the EUC shall be protected to avoid unauthorised modifications of the system performance. For screen based systems, tools shall be available to allow easy and unambiguous modification of configuration parameters 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 501, while access to other applications or installations of such, should be prevented. Hot keys normally giving access to other functions or program exits (Alt+Tab, Ctrl+Esc, Alt+Esc, double-clicking in background, etc.) must be disabled.

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

802 Unauthorised access to essential and important systems from a position outside the unit shall not be possible. Ref. also to Ch.1 Sec.1 A405 for remote diagnostics and maintenance.

B. System Software

B 100 Software requirements

101 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 (ie. with minimal need for high level programming).

102 Application software shall be realised using standard software modules (eg. function blocks) to the greatest extent possible. The software modules shall have the flexibility to provide individual application functionality by use of simple configuration and parameterisation. The use of high level programming shall be minimised.

103 The application software, software modules and function blocks shall 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.

104 System set-up, configuration to suit the EUC and the setting of parameters for the EUC onboard shall take place without modification of program code or recompilation. Facilities shall be provided to allow simple back-up and restoration of Operator configured parameters.

Guidance note:

When the setting of parameters is equivalent to programming then version identification of these settings shall be available. Version identification may be a check sum.

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

105 Running software versions shall be uniquely identified by number, date or other appropriate means. This shall apply for all system software (including third party software packages) and all application software. Modifications shall not be made without also changing the version identifier. A record of changes to the system since the original issue (and their identification) shall be maintained and made available to the inspection party on request

Guidance note:

For integrated systems, identification should be available in the system overview.

For any screen based system, identification should be readily available on the VDU during normal operation.

PROMs should be labelled.

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

B 200 Software manufacturing

201 All relevant actions shall 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 shall 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 onboard 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.

Guidance note:

Typical execution failures are:

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

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

202 The actions taken to comply with 201 shall be documented and implemented, and the execution of these actions shall be retraceable. The documentation shall include a brief description of all tests that apply to the system (hardware and software), with a description of the tests 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 onboard.

203 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.

C. Network Systems and Communication Links

C 100 General

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

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

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

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

Guidance note:

Miscellaneous office- or entertainment functions should not be connected to the automation and safety system.

It is normally not considered acceptable to include CCTV as part of the automation and safety system.

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

104 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.

Guidance note:

Main functions are considered to be as defined in Rules for Classification of Ships, Pt.1 Ch.1 Sec.1.

To be demonstrated during commissioning/sea-trial.

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

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

Guidance note:

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

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

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

Guidance note:

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

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

107 It shall not be possible for unauthorised personnel to connect equipment to the ICSS network or otherwise have access to such network.

Guidance note:

This pertain to both communication onboard the unit / installation (e.g. that there should be no connectors available for unauthorised access on network components like e.g. switches) as well as remotely via external communication.

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

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

C 200 Serial communication

201 Failure in a node shall not have any effect on the remaining part of the data communication link and vice versa.

202 Data communication links shall be automatically initialised on power on. After a power interruption, the links shall regain normal operation without manual intervention.

203 The capacity of the data communication link shall be sufficient to prevent overload at any time.

204 The data communication link shall be self-checking, detecting failures on the link itself and data communication failures on nodes connected to the link. Detected failures shall initiate an alarm on dedicated workstations.

205 For essential and important functions, means shall be provided to prevent the acceptance of corrupted data at the receiving node.

206 When two or more essential functions are using the same data communication link, this link shall be redundant.

207 Redundant data communication links shall be routed with as much separation as practical.

C 300 Network communication

301 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 pre-defined manner in case of an excessive traffic event.

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

302 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.

303 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.

Guidance note:

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

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

304 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. The integrity and autonomy of each segment shall be secured with appropriate network components, e.g. firewalls or routers. It shall be possible to protect each segment from unnecessary traffic on the remaining network, and each segment shall be able to work autonomously.

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

Guidance note:

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

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

306 Systems allowing for remote connection (e.g. via Internet), for e.g. remote diagnostics or maintenance purposes, shall be secured with sufficient means to prevent unauthorised access, and functions to maintain the security of the control and monitoring system. The security properties shall be documented.

Guidance note:

Any remote access to the control system should be authorised onboard. 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---of---G-u-i-d-a-n-c-e---n-o-t-e---

307 Virtual networks (VLAN) is not considered satisfactory to meet the requirements for network segmentation as specified paragraph 204.

C 400 Network analysis

401 The automation and safety systems network with its components, connected nodes, communication links (also external interfaces) shall be subject to an analysis where all rel-

evant failure scenarios are identified and considered.

Guidance note:

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.)

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.

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

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

C 500 Network test and verification

501 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

C 600 Wireless communication

601 Wireless technologies may be used in monitoring functions that are additional or supplementary to those required by the offshore standard. Any use of wireless technology in control functions shall be subject to special consideration.

Guidance note:

This implies that the main class requirements should be fulfilled even in case of the wireless communication being out of service.

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

602 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.

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

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

Guidance note:

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

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

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

Guidance note:

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

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

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

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

Guidance note:

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

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

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

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

Guidance note:

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

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

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

Guidance note:

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

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

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

SECTION 4 COMPONENT DESIGN AND INSTALLATION

A. General

A 100 Environmental strains

101 Safety, automation and telecommunication equipment shall be suitable for marine use, and shall be designed to operate under the environmental conditions as described in B.

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

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

A 200 Materials

201 Explosive materials and materials, which may develop toxic gases shall not be used. Covers, termination boards, printed circuit cards, constructive elements and other parts that may contribute to spreading fire shall be of flame-retardant 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---of---G-u-i-d-a-n-c-e---n-o-t-e---

A 300 Component design and installation

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

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

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

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

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

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

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

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

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

A 400 Maintenance

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

A 500 Marking

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

A 600 Standardisation

601 Guidance related to standardisation:

Guidance note:

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

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

B. Environmental Conditions, Instrumentation

B 100 General

101 The environmental parameters specified in 200 to 1100, 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 200 to 1100, the corresponding requirements shall be modified accordingly.

102 The different environmental parameter classes are defined in table B1.

| Table B1 Parameter class for the different locations on board | | |
|---|--------------|---|
| <i>Parameter</i> | <i>Class</i> | <i>Location</i> |
| 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 (1994), and for EMC, IEC Publication No. 60533, may be accepted after consideration. | | |

Guidance note:

For details on environmental conditions for instrumentation, see Certification Note No. 2.4.

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 (1996) Clause 9 (covered by EMC class B).

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

B 200 Electric power supply

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

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

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

- combination of permanent frequency variations of $\pm 5\%$ and permanent voltage variations of $+6 / -10\%$ of nominal
- combination of frequency transients (5 s duration) $\pm 10\%$ of nominal and voltage transients (1.5 s duration) $\pm 20\%$ of nominal.

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

- voltage tolerance continuous $\pm 10\%$ of nominal
- voltage transients cyclic variation 5% of nominal
- voltage ripple 10%.

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

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

B 300 Pneumatic and hydraulic power supply

301 Nominal pressure $\pm 20\%$ (long and short time deviations).

B 400 Temperature

401 Class A: Ambient temperatures $+5^\circ\text{C}$ to $+55^\circ\text{C}$.

402 Class B: Ambient temperatures $+5^\circ\text{C}$ to $+70^\circ\text{C}$.

403 Class C: Ambient temperatures -25°C to $+55^\circ\text{C}$.

404 Class D: Ambient temperatures -5°C to $+70^\circ\text{C}$.

B 500 Humidity

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

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

B 600 Salt contamination

601 Salt-contaminated atmosphere up to 1 mg salt per m^3 of air, at all relevant temperatures and humidity conditions.

B 700 Oil contamination

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

B 800 Vibrations

801 *Class A*

- frequency range 3 to 100 Hz
- amplitude 1 mm (peak value) below 13.2 Hz
- acceleration amplitude 0.7 g above 13.2 Hz.

802 *Class B*

- frequency range 3 to 100 Hz
- amplitude 1.6 mm (peak value) below 25 Hz
- acceleration amplitude 4.0 g above 25 Hz.

803 *Class C*

- frequency range 3 to 50 Hz
- amplitude 3 mm (peak value) below 13.2 Hz
- acceleration amplitude 2.1 g above 13.2 Hz.

B 900 Electromagnetic compatibility

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

Guidance note:

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

| Table B2 Minimum immunity requirements for equipment | | | | |
|---|--|-----------------------|-----------------------------|---|
| <i>Port</i> | <i>Phenomenon</i> | <i>Basic Standard</i> | <i>Performance criteria</i> | <i>Test value</i> |
| A.C. power | Conducted low frequency interference | IEC 60945 | A | 50 - 900 Hz: 10% A.C. supply voltage 900 - 6000 Hz: 10 - 1% A.C. supply voltage 6 - 10 kHz: 1% A.C. supply voltage |
| | Electrical fast transient (Burst) | IEC 61000-4-4 | B | 2 kV ³⁾ |
| | Surge voltage | IEC 61000-4-5 | B | 0.5 kV ¹⁾ / 1 kV ²⁾ |
| | Conducted radio frequency interference | IEC 61000-4-6 | A | 3 Vrms ³⁾ ; (10 kHz) ⁶⁾ 150 kHz - 80 MHz sweep rate ≤ 1.5 x 10 ⁻³ decade/s ⁷⁾ modulation 80% AM (1 kHz) |
| D.C. power | Conducted low frequency interference | IEC 60945 | A | 50 Hz - 10 kHz : 10% D.C. Supply voltage |
| | Electrical fast transient (Burst) | IEC 61000-4-4 | B | 2 kV ³⁾ |
| | Surge voltage | IEC 61000-4-5 | B | 0.5 kV ¹⁾ / 1 kV ²⁾ |
| | Conducted radio frequency interference | IEC 61000-4-6 | A | 3 Vrms ³⁾ ; (10 kHz) ⁶⁾ 150 kHz - 80 MHz sweep rate ≤ 1.5 x 10 ⁻³ decade/s ⁷⁾ modulation 80% AM (1 kHz) |
| I/O ports, signal or control | Electrical fast transient (Burst) | IEC 61000-4-4 | B | 1 kV ⁴⁾ |
| | Conducted radio frequency interference | IEC 61000-4-6 | A | 3 Vrms ³⁾ ; (10 kHz) ⁶⁾ 150 kHz - 80 MHz sweep rate ≤ 1.5 x 10 ⁻³ decade/s ⁷⁾ modulation 80% AM (1 kHz) |
| Enclosure | Electrostatic discharge (ESD) | IEC 61000-4-2 | B | 6 kV contact/8 kV air |
| | Electromagnetic field | IEC 61000-4-3 | A | 10 V/m ⁵⁾ 80 MHz-2 GHz sweep rate ≤ 1.5 x 10 ⁻³ decade/s ⁷⁾ modulation 80% AM (1 kHz) |

1) line to line
2) line to ground
3) capacitive coupling
4) coupling clamp
5) special situations to be analysed
6) test procedure to be described in the test report
7) for equipment installed in the bridge and deck zone (EMC Class B) the test levels are to 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 is to be used enabling the coupling into the cable screen.

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

| Table B3 Maximum emission requirements for equipment | | | | |
|---|--|-------------------------------|---|--|
| <i>Class</i> | <i>Location</i> | <i>Port</i> | <i>Frequency Range (Hz)</i> | <i>Limits</i> |
| 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 |

B 1000 Inclination

inclination up to 15° in any direction.

1001 All systems on board column stabilised units and self elevating units shall operate satisfactorily when the unit has an

1002 The emergency generator on board column stabilised units and self elevating units shall operate satisfactorily when

the unit has an inclination up to 22.5° in any direction.

1003 On board ship shaped units installations and components shall operate satisfactorily up to the angles of inclination specified in Table B4.

| Installations, components | Angle of inclination (degrees) ¹⁾ | | | |
|--|--|---------|--------------|---------|
| | Aftships | | Fore and aft | |
| | Static | Dynamic | Static | Dynamic |
| Main and auxiliary machinery | 15 | 22.5 | 5 | 7.5 |
| Safety equipment, for example emergency power installations, emergency fire pumps and their devices, electronic appliances ²⁾ and remote control system | 22.5 | 22.5 | 10 | 10 |

1) Aftships and fore-and-aft inclinations may occur simultaneously.
2) Up to an angle of inclination of 40° no undersized switching operations or operational changes shall occur.

B 1100 Miscellaneous

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

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

C. Electrical and Electronic Equipment

C 100 General

101 Fused isolating transformers shall be fitted between the main power supply and the different equipment or systems.

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

103 Equipment requiring insulating resistance in cables and wiring higher than 200 kΩ shall normally not be used. Exceptions can be made for special cable arrangements.

C 200 Mechanical design, installation

201 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).

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

Guidance note:

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

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

Guidance note:

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

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

C 300 Protection provided by enclosure

301 Enclosures for the equipment shall be made of steel or other flame retardant material capable of providing EMC protection and satisfy the minimum requirements of Table C4. The required degree of protection is defined in IEC 60529.

| Class | Location | Degree of protection |
|-------|---|----------------------|
| A | Control rooms, accommodation, bridge, local equipment rooms, central equipment room | IP 22 |
| B | Machinery spaces | IP 44 |
| C | Open deck, masts, below floor plates in machinery spaces | IP 56 |
| D | Submerged application | IP 68 |

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

C 400 Cables and wires

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

402 Cables, wires and electrical 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 electric energy is required to operate or maintain control over the system.

C 500 Cable installation

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

C 600 Power supply

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

C 700 Fibre optic equipment

701 Fabrication and installation of fibre optic cables shall comply with the requirements of the relevant DNV standard for electrical systems and equipment, DNV-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---of---G-u-i-d-a-n-c-e---n-o-t-e---

702 Power budget calculation shall be used to:

- determine the length between I/O 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.

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

Guidance note:

It is advised to use equipment with 'built-in' safety, e.g. interlock the power to the light sources with the covers, possible to disconnect 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:

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

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

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

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

D. Pneumatic and Hydraulic Equipment

D 100 Pneumatic equipment

101 Components requiring extremely clean air shall not be used. Extremely small openings in air passages shall be avoided.

102 Main pipes shall be inclined relative to the horizontal and drainage shall be arranged.

103 Pipes and other equipment made of plastic materials may be used if they have satisfactory mechanical strength, low thermoplasticity, high oil resistance, and flame retardation. See DNV-OS-D101.

104 For air supply, the redundancy requirement of DNV-OS-D101 applies for compressors, pressure reduction units, filters and air treatment units (lubricator or oil mist injector and dehumidifier).

105 Air to instrumentation equipment shall be free from oil, moisture and other contaminations. Condensation shall not occur at relevant pressures and temperatures. For air flowing in pipes which are located entirely inside the machinery space

and accommodation, the dew point shall be more than 10°C below ambient temperature, but need normally not be lower than 5°C. The dew point of air flowing in pipes on open deck shall be below -25°C.

106 Reduction valves and filters shall be duplicated when serving more than one function (e.g. more than one control loop).

107 Piping and tubing to actuators and between actuators and local accumulators should be hydrostatically tested to 1.5 times the system design pressure for minimum 15 minutes.

108 Local accumulators used as back up air supply for essential systems shall be designed and located or protected to minimise the possibility of inadvertent isolation or mechanical damage which could prevent correct operation on demand.

109 Piping and tubing shall be cleaned and dried before connected to control systems.

110 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.

D 200 Hydraulic equipment

201 System components and arrangement shall satisfy the requirements in DNV-OS-D101.

202 Piping and tubing to actuators and between actuators and local accumulators should be hydrostatically tested to 1.5 times the system design pressure for 15 minutes.

203 Local accumulators used as back up power supply for essential systems shall be designed and located or protected to minimise the possibility of inadvertent isolation or mechanical damage which could prevent correct operation on demand.

204 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 hydraulic energy is required to operate or maintain control over the system.

205 Piping and tubing shall be flushed and cleaned before being connected to control systems.

206 Hydraulic oil return lines shall be designed with capacity to allow the maximum return flow during extreme conditions without reducing overall system performance. Care shall be taken to avoid the possibility of blockages at filters, vents or by mechanical damage or inadvertent operation of valves.

SECTION 5 USER INTERFACE

A. General

A 100 Application

101 The requirements of this section apply for all DNV Offshore Standards class vessel/units.

A 200 Introduction

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

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

B. Workstation Design and Arrangement

B 100 Location of visual display units and user input devices

101 Workstations shall be arranged to provide the user with easy access to UID's, VDU's and other facilities required for the operation.

Guidance note:

The VDU's and UID's should be arranged with due consideration of the general availability parameters as shown in figure 1 and 2.

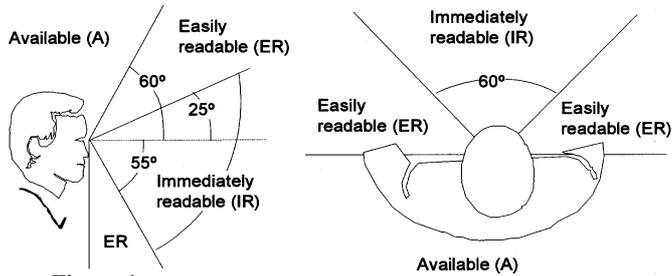


Figure 1
 VDU arrangement parameters.

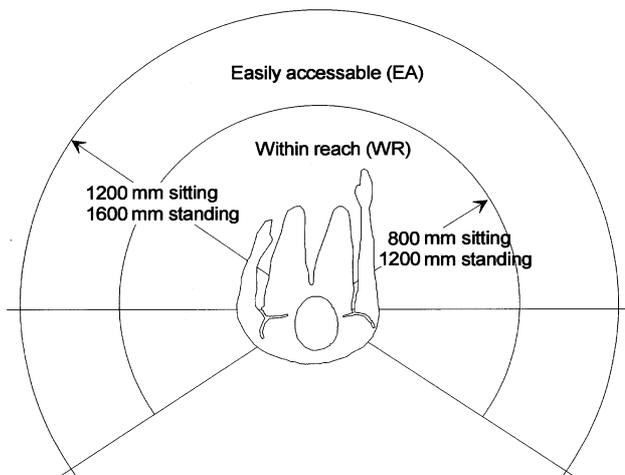


Figure 2
 UID arrangement parameters.

as possible be arranged and grouped together.

C. User Input Device and Visual Display Unit Design

C 100 User input devices

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

102 The direction of UID movements shall be consistent with the direction of associated process response and display movement.

Guidance note:

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

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

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

104 UID's or combined UID's or indicating elements shall be visually and tactually distinguishable from elements used for indication only.

Guidance note:

Rectangular buttons should be used for UID elements, and round lights for VDU elements. For screen based systems, a suitable framing method should be chosen.

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

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

C 200 Visual display units

201 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.

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

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

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

205 Back-up means of operation, ref Sec.3 A201 normally located in the CCR, shall contain the most important action functions and alarm indications related to ESD and fire detection, including activation of active fire protection devices.

Guidance note:

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
- release of ESD and ESD release confirmation indication
- lamp test, silence buzzer etc.

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

102 UID's and VDU's serving the same function shall as far

C 300 Colours

301 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 C1.

| Table C1 Colour coding | |
|--|-------------|
| Function | Colour code |
| Danger, Alarm, Emergency | Red |
| Attention, Warning, Caution, Undefined | Yellow |
| Status of normal, safe situation | Green |

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

C 400 Requirements for preservation of night vision (UID's and VDU's for installation on the navigating bridge)

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

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

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

D. Screen Based Systems

D 100 General

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

Guidance note:

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

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

102 Alarm messages for primary and emergency alarms required in DNV Offshore Standards, when initiated, are given priority over any other information presented on the VDU. The entire list of alarm messages shall be easily available.

103 Alarms shall be time tagged, see also Sec.3 C101.

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

Guidance note:

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

105 UID's shall be designed and arranged to avoid inadvertent operation.

Guidance note:

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

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

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

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

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

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

D 200 Illumination

201 Means shall be provided for adjustment of illumination of all VDU's and UID's 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.

D 300 Computer dialogue

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

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

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

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

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

306 Confirmation of a command shall only be used when the action requested may have a critical irreversible consequence.

307 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.

D 400 Application screen views

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

SECTION 6 SUPPLEMENTARY REQUIREMENTS FOR DRILLING UNITS

A. General

A 100 Introduction

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

B. Design Principles

B 100 General

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

Guidance note:

For drilling vessels the MODU code applies, and a separate fire panel should cover the entire vessel, unless a deviation from the MODU code is accepted by the flag state. The fire panel should be limited to fire detection.

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

102 Automation and safety system components that are intended to be alive after an incident shall be Ex zone 2 certified or safe by location ref. DNV-OS-A101 Sec.5 F.

103 When an incident requires relocation of the unit/installation, then safe disconnection from the well and repositioning of the unit/installation shall be supported by the systems design.

Guidance note:

On gas release, dampers and fans supplying non hazardous areas should be shut down ref. DNV-OS-D301. For non-Ex certified components located in these areas supporting position keeping, power production or other important functions, intended to be kept alive during the incident for maintaining the safety of the unit/installation, the location must be designed to support operation without normal air cooling. This will typically include separate combustion air intake and room cooling sufficient to keep components operational during the incident, for a time period sufficient to bring the unit/installation to a safe location.

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

Guidance note:

Non-Ex components located in non hazardous areas on open deck should be enclosed, or shut down on confirmed gas detection in hazardous area ref. DNV-OS-A101 Sec.5 D.

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

C. System Design

C 100 General

101 For fire detection in accommodation and engine room including marine systems, the signals shall be connected to a dedicated fire panel before being routed to the F&G node, ref. IMO FSS code requirement.

102 An alarm philosophy shall be developed for various alarm conditions. The alarms shall be distinguished by sound and colour and be given at main control stations and unit as applicable. (See also Ch.2 Sec.2 A501).

Guidance note:

For drilling units this may consist of informative alarms as lowest category, critical alarms where it is required that the operator takes actions to prevent a more critical situation to occur, and finally information actions where the safety system have taken control.

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

103 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 DNV-OS-A101 Sec.2.

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

104 Internode signals between F&G and ESD nodes shall follow the fail safe principles given in DNV-OS-A101 Sec.5, as applicable.

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

D. Additional Requirements for Computer Based Systems

D 100 General

101 No supplementary requirements.

E. Component Design and Installation

E 100 General

101 Cables 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 energy is required to operate or maintain control over the system.

F. User Interface

F 100 General

101 Back-up means of operation, ref Sec.3 A201 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 Ch.2 Sec.5 C205).

Guidance note:

This will 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 (ref. DNV-OS-E301, Ch.2 Sec.4 K509 and DNV-OS-D101, Ch.2 Sec.5 G305)
- Activation of BOP release sequence (normally located in BOP control panel).

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

SECTION 7 SUPPLEMENTARY REQUIREMENTS FOR PRODUCTION AND STORAGE UNITS

A. General

A 100 Introduction

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

B. Design Principles

B 100 General

101 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 DNV-OS-E201 for details, however it is accepted that blow down valves are equipped with remote reset.

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

102 Power to the relevant parts of the safety system shall not be tripped by the ESD system.

103 Automation and safety system components that are intended to be alive after an incident shall be Ex zone 2 certified or safe by location ref. DNV-OS-A101 Sec.5 F.

104 When an incident requires relocation of the unit/installation, then safe disconnection from the well(s) and repositioning of the unit/installation shall be supported by the systems design.

Guidance note:

On gas release, dampers and fans supplying non hazardous areas should be shut down ref. DNV-OS-D301. For non-Ex certified components located in these areas supporting position keeping, power production or other important functions, intended to be kept alive during the incident for maintaining the safety of the unit/installation, the location must be designed to support operation without normal air cooling. This will typically include separate combustion air intake and room cooling sufficient to keep components operational during the incident, for a time period sufficient to bring the unit/installation to a safe location.

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

Guidance note:

Non-Ex components located in non hazardous areas on open deck should preferably be located in an enclosed non ventilated room, or shut down on confirmed gas detection in hazardous area ref. DNV-OS-A101 Sec.5 D.

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

C. System Design

C 100 General

101 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 Loads are described in DNV-OS-A101 Sec.2.

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

102 An alarm philosophy shall be developed for various alarm conditions. The alarms shall be distinguished by sound and colour and be given at main control stations and unit as applicable. (See also Ch.2 Sec.2 A501)

Guidance note:

For an FPSO's PCS alarms would be the lowest level, PSD/ESD, and F&G as the most critical level.

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

103 For the process plant, the redundancy requirement shall apply for the F&G node(s), ref. Sec.1 A503.

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

104 Internode signals between F&G and ESD/PSD nodes shall follow the fail safe principles given in DNV-OS-A101 Sec.5.

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

D. Additional Requirements for Computer Based Systems

D 100 General

101 ESD/PSD, F&G, and PCS nodes shall be segregated both in cabinets and in topology.

Guidance note:

PSD is the lowest ESD level. PSD is a local shutdown as opposed to ESD levels that are global shutdown.

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

E. Component Design and Installation

E 100 General

101 Cables and components in systems required to operate in a fire scenario shall have adequate fire resistance sufficient to ensure correct system operation during an incident for an acceptable time period (defined by accident scenario).

Guidance note:

This is particularly important for systems where energy is required to operate or maintain control over the system.

Cabinets of the distributed parts of the automation and safety system should withstand the Design Accidental Loads.

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

F. User Interface

F 100 General

101 There shall be sufficient VDU's or other panels to ensure overview and detailed information for relevant safety systems (Ref. Sec.1 A404).

Guidance note:

Sufficient overall status should be provided without browsing between screen pictures, including all shutdown valves within the process plant.

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

102 Back-up means of operation, ref Sec.3 A201, 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 Ch.2 Sec.5 C205).

Guidance note:

This will 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 (ref. DNV-OS-D101, Ch.2 Sec.5 G305).

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



CHAPTER 3

CERTIFICATION AND CLASSIFICATION

| CONTENTS | PAGE |
|--|------|
| Sec. 1 Certification and Classification - Requirements | 37 |

SECTION 1 CERTIFICATION AND CLASSIFICATION - REQUIREMENTS

A. General

A 100 Introduction

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

102 A complete description of principles, procedures, applicable class notations and technical basis for offshore classification is given by the offshore service specifications, see Table A1.

| Table A1 Offshore Service Specifications | |
|--|--|
| No. | Title |
| DNV-OSS-101 | Rules for Classification of Offshore Drilling and Support Units |
| DNV-OSS-102 | Rules for Classification of Floating Production, Storage and Loading Units |

A 200 Organisation of Ch.3

201 Ch.3 identifies the specific documentation, certification and surveying requirements to be applied when using this standard for certification and classification purposes.

A 300 Classification principles

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

- document evaluation (see B)
- certification requirements (see C)
- on-board inspection (visual inspection and functional testing).

Guidance note:

The approval may be either case-by-case approval for each system, or type approval as specified in Certification Notes No. 1.2 and 2.4.

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

B. Documentation

B 100 General

101 Overview documentation as listed in Table B1 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---of---G-u-i-d-a-n-c-e---n-o-t-e---

102 Documentation listed in Table B2 is required submitted in order to adequately describe the automation and safety system.

103 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 B2) 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---of---G-u-i-d-a-n-c-e---n-o-t-e---

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

105 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.

106 For a system subject to certification, documentation listed in Table B3 shall be available for the surveyor at testing at the manufacturer.

107 For on-board inspection, documentation listed in Table B4 is required submitted to survey station.

108 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 B2) in one submittal, to the extent possible.

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

Guidance note:

Typically submitted by manufacturers based upon their project specific specification.

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

| Table B1 Documentation requested submitted at an early stage in the approval work (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) | | |
|---|--|----------------|
| <i>Documentation type</i> | <i>Information element</i> | <i>Purpose</i> |
| System philosophy (1010) (T) | <ul style="list-style-type: none"> — 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. | Approval |
| General arrangement for the vessel/unit | General vessel/unit information. | Information |
| General arrangement for the main control stations | Main equipment layout, including main engine room, local equipment or instrument room, central equipment room and main control stations. | Information |
| Project specification /design basis for automation and safety related systems. | Automation and safety aspects of the following: <ul style="list-style-type: none"> — Propulsion and steering — Production and/or drilling plant — Turret and swivel — Position keeping — Marine systems — Cargo and offloading systems — Power production — Fire & gas detection system(s) — ESD system — Utility systems. | Information |

| Table B2 Documentation required to describe the automation and safety system (typically submitted by manufacturers based upon their project specific specification) | | |
|---|---|----------------|
| <i>Documentation type</i> | <i>Information element</i> | <i>Purpose</i> |
| Functional description (system requirement specification) (1020) (T) | <ul style="list-style-type: none"> — 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. | Information |
| System block diagrams (1030) (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 (1040) | <ul style="list-style-type: none"> — a description of the functions allocated to each work and operator station — a description of transfer of responsibility between work and operator stations. | Information |
| Power supply arrangement (1050) (T) | — electrical supply: diagram showing connection to distribution board(s), batteries, converters or UPS. Including information regarding Ex/Non Ex as applicable. | Approval |
| Functional failure analysis, for essential systems and important closed loop system (Z070) (T) | The purpose is to ensure that for single failures, essential systems will fail to safety and that systems in operation will not be lost or degraded beyond acceptable performance criteria when specified by the offshore standard. The following aspects shall be covered: <ul style="list-style-type: none"> — a description of the boundaries of the system including power supply preferably by a block diagram — a list of items which are subject to assessment with a specification of probable failure modes for each item, with references to the system documentation — a description of the system response to each of the above failure modes identified — a comment to the consequence of each of these failures. | Information |

| Table B2 Documentation required to describe the automation and safety system (Continued) (typically submitted by manufacturers based upon their project specific specification) | | |
|---|---|----------------|
| <i>Documentation type</i> | <i>Information element</i> | <i>Purpose</i> |
| Failure mode and effect analysis (FMEA) (Z071) (T) (Only when requested) | <p>A failure modes and effect analysis (FMEA) is to be carried out for the entire system. The FMEA is to be sufficiently detailed to cover all the systems' major components and is to include but not be limited to the following information:</p> <ul style="list-style-type: none"> — 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's position — the method of detecting that the failure has occurred — the effect of the failure upon the rest of the system's ability to maintain station — an analysis of possible common failure mode. <p>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.</p> <p>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.</p> <p style="text-align: center;">---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---</p> | Information |
| List of control & monitored points (I110) (T) | <p>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:</p> <ul style="list-style-type: none"> — service description — instrument tag-number — system (control, safety, alarm, indication) — type of signal (digital / analogue input / output). | Approval |
| Circuit diagrams (I150) | <ul style="list-style-type: none"> — for essential hardwired circuits (for emergency stop, shutdown, interlocking, etc.) details of input and output devices and power source for each circuit. | Approval |
| Test program for testing at the manufacturer (Z120) (T) | <p>Description of test configuration and test simulation methods. Based upon the functional description, each test shall be described specifying:</p> <ul style="list-style-type: none"> — initial condition — how to perform the test — what to observe during the test and acceptance criteria for each test. <p>The tests shall cover all normal modes as well as failure modes identified in the functional failure analysis, including power and communication failures.</p> | Examination |
| Software quality plan, based upon life cycle activities (I140) (T) (Shall be available during certification) | <p>The software life cycle activities shall minimum contain procedures for:</p> <ul style="list-style-type: none"> — 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. | Information |
| Data sheets with environmental specifications (I080) | <ul style="list-style-type: none"> — environmental conditions stipulated in Sec.4 for temperature, vibration, humidity, enclosure and EMC. | Information |
| Cause and effect diagrams | <ul style="list-style-type: none"> — 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 |
| Operation manual (Z160) (Available during certification and to be kept on board) | <p>A document intended for regular use on board, providing information as applicable about:</p> <ul style="list-style-type: none"> — 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. (Z170) (Available during certification) | <p>A document providing information about the installation procedures.</p> | Information |

| Table B2 Documentation required to describe the automation and safety system (Continued) (typically submitted by manufacturers based upon their project specific specification) | | |
|---|---|----------------|
| <i>Documentation type</i> | <i>Information element</i> | <i>Purpose</i> |
| Maintenance manual (Z180) (Available during certification and to be kept on board) | A document intended for regular use on board providing information about: <ul style="list-style-type: none"> — maintenance and periodical testing — acceptance criteria — fault identification and repair — list of the suppliers' service net — vessel/unit's systems' software - maintenance log. | Information |
| Test program for dock and sea trials (Z140) (Available during certification and to be kept on board) | <ul style="list-style-type: none"> — initial condition — what to test — how to perform the test — acceptance criteria for the test. | Examination |
| 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: <ul style="list-style-type: none"> — 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: <ul style="list-style-type: none"> — Functional Description — ISM certificate(IEEE802) from a licence authority (typical flag state) or alternatively applicable test reports — Single line drawings of the WLAN topology with power arrangements — Specification of frequency band(s), power output and power management — Specification of modulation type and data protocol — Description of integrity and authenticity measures. | Approval |

| Table B3 Documentation required available for the testing at the manufacturer | | |
|--|--|----------------|
| <i>Documentation type</i> | <i>Information element</i> | <i>Purpose</i> |
| Software quality plan, based upon life cycle activities (Available for information at testing at the manufacturer) | The software life cycle activities shall minimum contain procedures for: <ul style="list-style-type: none"> — 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. | Information |
| Operation manual (Available for information at testing at the manufacturer) | A document intended for regular use on board, providing information as applicable about: <ul style="list-style-type: none"> — 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 (Available for information at testing at the manufacturer). | A document providing information about the installation procedures. | Information |
| Maintenance manual (Available for information at testing at the manufacturer) | A document intended for regular use on board providing information about: <ul style="list-style-type: none"> — maintenance and periodical testing — acceptance criteria — fault identification and repair — list of the suppliers' service net — ship's systems' software - maintenance log. | Information |
| Test program for dock and sea trials | <ul style="list-style-type: none"> — initial condition — what to test — how to perform the test — acceptance criteria for the test. | Examination |

| Table B4 Documentation required for on-board inspection | | |
|--|--|----------------|
| <i>Documentation type</i> | <i>Information element</i> | <i>Purpose</i> |
| Test program for dock and sea trials | <ul style="list-style-type: none"> — initial condition — what to test — how to perform the test — acceptance criteria for the test | Examination |

C. Certification

- issue of a DNV product certificate.

C 100 General

101 Essential and important computer based systems shall be provided with a DNV product certificate. For DNV type approved systems, additional testing is only required for the application software programming and function, unless further testing is required in the type approval certificates. The certification procedure normally consists of:

Document evaluation

- review of documentation listed in Sec.1 B for the appropriate system.

Manufacturing survey (MS)

- survey of hardware and software
- test of project specific application software

Guidance note:

Type approval of systems includes hardware, operating system software, standard software modules and standard function blocks. If new software modules or function blocks are made, testing will be required. Application software is project specific and shall be tested before the certificate can be issued.

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

102 The certification requirement of the various instrumented systems shall follow the same certification requirement as the system they control. Reference is made to Ch.1 Sec.1 B200 for the list of relevant Offshore Standards.

103 Integrated control and safety system shall always be certified.

Guidance note:

For equipment, where failure in the automation and safety functions may lead to major incidents, the automation and safety system shall be certified, e.g. burner control for auxiliary boilers.

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

D. Inspection and Testing

D 100 Manufacturing survey

101 All test programs shall be approved by DNV.

102 Approval testing according to C100 and Ch.2 Sec.1 F100 shall be performed at the manufacturer's works.

D 200 On board testing

201 Approval testing shall be carried out as necessary to demonstrate that the overall requirements of testing described in Ch.2 Sec.1 F100 to F500 have been fulfilled.

202 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.

D 300 Renewal survey

301 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.

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

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

E. Alterations and Additions

E 100 General

101 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.