RULES FOR
CLASSIFICATION OF

SHIPS / HIGH SPEED, LIGHT CRAFT AND NAVAL SURFACE CRAFT

NEWBUILDINGS

SPECIAL EQUIPMENT AND SYSTEMS
ADDITIONAL CLASS

PART 6 CHAPTER 5

INTEGRATED COMPUTER SYSTEMS (ICS)

JANUARY 2003
This booklet includes the relevant amendments and corrections shown in the January 2004 version of Pt.0 Ch.1 Sec.3.

CONTENTS PAGE

Sec. 1 General Requirements 5
Sec. 2 System Design 8

DET NORSKE VERITAS

Veritasveien 1, NO-1322 Høvik, Norway Tel.: +47 67 57 99 00 Fax: +47 67 57 99 11

CHANGES IN THE RULES

General

This booklet is a reprint of the previous edition and apart from clarifications of text and the inclusion of amendments and corrections, published in the July 2002 edition of Pt.0 Ch.1 Sec.3, no other changes have been made.

This chapter is valid until superseded by a revised chapter. Supplements will not be issued except for an updated list of minor amendments and corrections presented in Pt.0 Ch.1 Sec.3. Pt.0 Ch.1 is normally revised in January and July each year.

Revised chapters will be forwarded to all subscribers to the rules. Buyers of reprints are advised to check the updated list of rule chapters printed in Pt.0 Ch.1 Sec.1 to ensure that the chapter is current.

Comments to the rules 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 and the Society's services is found at the Web site http://www.dnv.com

Computer Typesetting (FM+SGML) by Det Norske Veritas
Printed in Norway

CONTENTS

SEC. 1 GENERAL REQUIREMENTS 5

A. Classification 5
A 100 Application 5
A 200 Class notation 5

B. Definitions 5
B 100 Terms 5

C. The Integration Process 6
C 100 Assignment of responsibility 6

D. Documentation 6
D 100 Plans and particulars 6

E. Testing at Manufacturer 7
E 100 Extent of testing 7

F. Testing Onboard 7
F 100 Extent of testing 7

SEC. 2 SYSTEM DESIGN 8

A. Design Principles 8
A 100 Cross reference 8
A 200 Integration principles 8
A 300 Safety actions 8
A 400 Fail-safe principles 8
A 500 System maintenance 8
A 600 Testability 8

B. Data Communication Network 8
B 100 Extent of system communication 8
B 200 Failure tolerance 8
B 300 Redundancy in data communication links 8
B 400 Cable routing of data communication links 9
B 500 Monitoring 9

C. Work Stations 9
C 100 Arrangement of work station 9

D. Data Communication Protocol 9
D 100 Standardisation and capacity 9

SECTION 1
GENERAL REQUIREMENTS

A. Classification

A 100 Application

101 The rules in this chapter apply to vessels where control and monitoring systems serving main functions are integrated, or connected via communication network, forming an integrated computer system. Further, the rules also apply where such control and monitoring systems are integrated or connected to the vessels administrative applications.

Guidance note:

The term 'integrated computer system' means a system that contains control and monitoring functions for two (or more) systems that are normally implemented in separate units. This may consist of a common computer system where all the relevant control and monitoring functions are implemented, or two (or more) individual systems interfaced via communication networks, and where functions in either system may influence the performance of the other.

Navigational- and radio communication systems are in general not subject to the requirements in these rules as the systems are regulated by the IMO "Performance Standards for Shipborne Radio communications and Navigational Equipment".

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

102 The requirements in Pt.4 Ch.9 including Sec.6 are to be complied with.

A 200 Class notation

201 Vessels implementing integrated computer based systems, in accordance with Sec.1 and Sec.2 and as described in 101, may be given the additional class notation **ICS**. However, the integrated computer systems shall be designed, built and tested in compliance with the requirements of this chapter and other referenced requirements.

202 The notation **ICS** may only be given to vessels that have at least one of the following additional class notations:

a) If integrating machinery systems, class notation **E0** or **ECO**.

b) If integrating navigational systems, class notation **NAUT-OC** or **NAUT-AW**.

c) If integrating cargo systems, class notation **CCO**.

d) If integrating positioning systems, **DYNPOS-AUTS, DYNPOS-AUT, DYNPOS-AUTR, DYNPOS-AUTRO**, **POSMOOR-ATA**.

Guidance note:

The purpose of the above limitation is to ensure that the **ICS** rules are only applied to vessels that are equipped with control and monitoring systems of a certain complexity, and where integration of the systems are crucial.

The class notations **ECO**, **NAUT-OC** or **NAUT-AW**, and **CCO** are only applicable to ships.

The class notations **DYNPOS-AUTS**, **DYNPOS-AUT**, **DYNPOS-AUTR**, **DYNPOS-AUTRO** and **POSMOOR-ATA** are not applicable to HS, LC and NSC.

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

203 The class notation **ICS** mainly covers the planning, implementation and verification of the integrating process between the systems that are integrated or interconnected. Hence, the rules do not apply to internal functionality within a system; the intention with the rules is to ensure that the interaction between integrated systems is secured via a set of requirements for the integration process.

Guidance note:

The main concerns are:

— Interconnection between different systems being part of the integrated system.
— Interface between systems and/or parts of systems from different vendors. This applies to interfaces between computer based systems and between computer based systems and non-computer based systems being part of the integrated system.

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

204 The different systems being part of the total integrated system to be covered by the class notation **ICS** are to be handled according to Pt.4 Ch.9 Sec.1 A200.

B. Definitions

B 100 Terms

101 For general terms, see Pt.4 Ch.9 Sec.1 B

102 *Application rules* are requirements for a specific use.

Guidance note:

Rules found in Pt.4 Ch.9 are general and give requirements for "how to", e.g. how to configure computer based systems to ensure the required reliability and availability, how alarms are to be presented and acknowledged, etc.

The application rules (e.g. for periodically unmanned machinery spaces) gives requirements for "what to", e.g. pressures and temperatures to be monitored, alarms to be given, shut-downs to be automatically activated, etc.

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

103 *Verification level* (on board):

Level 1: Installation of equipment
Level 2: Connection of field equipment
Level 3: Calibration of field equipment
Level 4: Component / Process segment testing
Level 5: Systems integration testing
Level 6: Total system testing (sea trial)

104 The different parts of a computer based system are divided as described in 105 to 111.

105 *Field instrumentation layer:* I/O and connections from the sensors and actuators to the I/O.

Guidance note:

The sensor/actuator and I/O may be one physical unit.

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

106 *Process layer:* The process layer consists of process control nodes, data communication links and I/O. The data communication links are connected between process control nodes and or between process control nodes and I/O. The process control nodes normally perform real-time process control where no delay in the data communication link is allowed.

Guidance note:

The instrument and process layer may be one physical unit.

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

107 *System layer:* Operator stations, servers, etc. and data communication links (normally a single or redundant network) for interconnection to process control nodes from the same

manufacturer or from different manufacturers. The system nodes often perform real-time process control where delay in the data communication link is allowed. Normally, there is a person in the control loop.

Guidance note:

There may be two system layers for a single installation, one for interconnection of nodes from the same manufacturer and a second for interconnection of nodes from different manufacturers (e.g. between navigation system and main alarm system).

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

108 *Administrative layer:* Data communication links (normally a single network) for interconnection of general PC's, servers, satellite communication, etc., and the system layer.

109 *Data quality* is defined as the accuracy of the measured values combined with time stamping.

110 *Software life cycle* is defined as the totality of all activities related to a software product throughout the lifetime of the product, including specification, quality planning, development, verification, implementation, validation, acceptance, installation and subsequent modification.

111 *A total integrated system* is defined as the final resulting system from the integration of the computer based systems via the data communication link(s). The total integrated system also includes the interface between operator(s) and the various sub-systems.

C. The Integration Process

C 100 Assignment of responsibility

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

An integration plan shall be available containing relevant elements from 102.

Guidance note:

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

102 As an alternative to 101 a split of responsibilities may be accepted provided the following conditions are met:

A detailed written and signed *manufacturer's integration plan* shall be available. The integration plan shall, as a minimum, include the following information:

a) Identification of each partial system to be integrated in the total integrated system.

b) Specification of the responsible manufacturer for each of the partial systems to be integrated in the total integrated system.

c) Specification of manufacturer(s) responsible for the physical networks (field, process, system and administrative).

d) Specification of the manufacturer responsible for the interface from each partial system to the relevant physical net.

e) For each partial application utilising data from another application or system, the required data quality (see B109) is to be specified.

f) For each partial application providing data to another application the provided data, quality (see B109) is to be specified.

g) A plan for integration testing according to E101, F101 and F102.

Guidance note:

The *manufacturer's integration plan* may be signed by the yard, a major manufacturer or collectively by all manufacturers providing partial systems to the total integrated system.

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

103 A similar written and signed plan; the *manufacturers service plan*, for assignment of responsibilities for how to service the integrated system during the operational phase, is to be available.

D. Documentation

D 100 Plans and particulars

101 For all systems being a part of the total integrated system, documentation shall be submitted according to Table D1.

Table D1 Requirements for documentation of integration

Document	*Information element*	*Rule reference*	*Purpose/Where to*
Integration plan	— Specification of the responsible manufacturer for each of the partial systems to be integrated in the total integrated system. — Specification of manufacturer(s) responsible for the physical networks (field, process, system and administrative). — Specification of the manufacturer responsible for the interface from each partial system to the relevant physical net. — For each partial application utilising data from another application or system, the required data quality (see B109) is to be specified. — For each partial application providing data to another application the provided data, quality (see B109) is to be specified. — A plan for integration testing according to E101, F101 and F102.	C101/102	Information/Approval centre
Interface description	— Specification of external signals to be communicated between integrated systems/components	Sec.2 B100	Information/Approval centre
Communication networks and links	— Topology — Failure and effect analysis — Capacity evaluation — Cable routing	Sec.2 B100	Approval/Approval centre
A list of all application software	Maintenance manual to contain: — specification of functions contained in each specific application software — specification of software version — modification index (to be continuously updated)		Information/Approval centre
Operator stations	— Outline of the stations	Sec.2 C100	Approval/ Approval centre
Software life cycle	— Quality planning for development, verification, implementation, validation, acceptance, installation and subsequent modification		Information/Available during certification
Workstation Design and Arrangement	— Location of visual display units and user input devices — Allocation of functions to screen based systems	Pt.4 Ch.9	Approval/Approval centre

E. Testing at Manufacturer

E 100 Extent of testing

101 Additional to testing as required in Pt.4 Ch.9 Sec.1, the following testing is to be performed:

— all logic loops in the program (the tests are normally not to be witnessed by the Society but records are to be available on request)
— all interfaces to other systems and or part-systems from the same manufacturers and from different manufacturers.

Guidance note:

If the tests required in 101 are not completed at the manufacturer's works in accordance with the integration plan, the remaining tests may be performed on board (for *Operational readiness* 4, see F102) if accepted by the yard and owner.

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

F. Testing Onboard

F 100 Extent of testing

101 Each computer system is to be tested after installation onboard. The tests are primarily intended to demonstrate correct functioning and communication between the computer system and the connected equipment (sensors, mechanical equipment, other computer system). The tests are to be carried out in connection with the tests for the different applications.

102 Installation and testing is normally to be conducted in the order defined for operational readiness.

— *Verification level* 1, 2, 3: records, normally not witnessed.
— *Verification level* 4, 5, 6: records, witnessed.

Guidance note:

The following recommendations are made to assist in keeping the requirement for on board testing to a minimum:

1) Installation and testing is to be based on the manufacturer's documented test records.

2) Whenever possible, internal system tests, including the I/O are not to be repeated.

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

SECTION 2
SYSTEM DESIGN

A. Design Principles

A 100 Cross reference

101 For cross reference to design principles, see Pt.4 Ch.9 Sec.2.

A 200 Integration principles

201 The integration is to be of a modular, hierarchical design, in order to minimise the consequence of any system failure and to ensure ease of testing and maintenance. The structure of the hierarchical design is to be explained and documented.

A 300 Safety actions

301 Safety shut-down is to be independent of the system layer.

302 All safety actions other than safety shut-down, e.g. slow down or controlled shut-down, are to be independent of the system layer if the time delay in the safety loop is unacceptable.

A 400 Fail-safe principles

401 Upon loss of communication between a unit giving control signals and the process units performing the control, the process units performing the control are to revert to the least critical of any possible new state (fail-safe).

A 500 System maintenance

501 Testing and maintenance of the data communication links are to be possible without total loss of communication.

502 Control of the main functions is not to be possible from outside of the vessel.

503 The system behaviour is not to be altered from outside of the vessel.

Guidance note:

Software and/or configuration files may be downloaded from outside of the vessel. Installation is to be controlled by responsible person(s) on board the vessel.

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

504 Adequate software for virus detection is to be installed and operative on the administrative net (layer) if based on a general purpose operating system.

A 600 Testability

601 Means are to be available to the extent necessary to ensure that a fault occurring in any part of the total integrated system can be detected, found and repaired without affecting the operation of any other function supported by the total integrated system, except the function directly affected by the fault.

Guidance note:

This may be accomplished by e.g. adding continuously running network monitoring equipment and processes in combination with implementing self test and self diagnostic utilities for the individual functions.

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

602 Full, independent re-test of partial systems supporting essential services is to be possible without affecting the operation of any other essential or important service.

B. Data Communication Network

B 100 Extent of system communication

101 The following systems may be connected in the system and or process layers:

- engine room automation as specified by the class notation **E0** or **ECO**
- bridge (navigation) systems as specified by the class notation **NAUT-OC** or **NAUT-AW**
- systems as specified for the class notations: **DYNPOS-AUTS**, **DYNPOS-AUT**, **DYNPOS-AUTR**, **DYNPOS-AUTRO** and **POSMOOR-ATA** or **CCO**
- fire and gas systems
- fire extinction systems
- emergency shut-down systems
- voyage recorder, if installed
- other systems related to the safe operation of main functions as defined in Pt.1 Ch.1 Sec.2 of the Rules for Classification of Ships.

Guidance note:

The class notations: **ECO**, **NAUT-OC** or **NAUT-AW**, and **CCO** are only applicable to ships.
The class notations: **DYNPOS-AUTS**, **DYNPOS-AUT**, **DYNPOS-AUTR**, **DYNPOS-AUTRO** and **POSMOOR-ATA** are not applicable to HS, LC and NSC.

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

102 The following functions in the administration layer may be interfaced to the system layer, provided that failures in the administration layer are not propagated into the system layer:

- external communication
- planned maintenance and systematic testing of machinery or instrumentation or automation
- condition monitoring
- stock inventory (spare parts)
- training facilities
- administrative routines
- other systems related to ship operation.

Guidance note:

To avoid failures propagating into the system layer, the administrative layer should be on a separate network and interfaced to the system layer through a device providing electrical and logical isolation (e.g. gateway or router).

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

B 200 Failure tolerance

201 Computer system architecture is to be so arranged that the different sub-systems will continue to operate independently in case of a communication failure between any workstation or computer and other parts of the computer system.

B 300 Redundancy in data communication links

301 In the event of failure in the primary communication link between the different units in the process layer and between the process layer and the system layer, then communication shall be automatically or manually reinstated by utilising designed levels of redundancy in the communication links.

302 When communication between the different units in the system layer is dependent upon other units, then communication shall be automatically or manually reinstated by utilising designed levels of redundancy in the communication links.

303 For those parts of the system that contain essential functions; type 1 redundancy is required. Otherwise, type 2 redundancy is required.

B 400 Cable routing of data communication links

401 Built in redundant data communication links are to be routed as far apart from each other as possible. The links are to be installed on separate cable trays or in separate pipes. The links are not to be routed through areas of high fire risk.

To the extent possible an accident in a single compartment, e.g. fire or flooding, is not to affect more than one link.

402 The communication links are to be installed so they are well protected against mechanical damage and electromagnetic interference (EMI).

Guidance note:

See Classification Note No. 45.1.

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

B 500 Monitoring

501 The primary network and any other network that are so arranged as to form part of the designed redundancy, are to be automatically monitored, and any failure shall initiate an alarm.

C. Work Stations

C 100 Arrangement of work station

101 At least two display units are to be installed at each mandatory workstation.

Guidance note:

One display unit normally consists of a computer unit and a VDU.

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

D. Data Communication Protocol

D 100 Standardisation and capacity

101 The protocol is to be capable of handling all data traffic, which may occur during all operational modes, without subjecting the system or the operator to unacceptable delays. This includes emergency operation and modes with high load demands.