GUIDANCE NOTES
GD014-2026

INTERNATIONAL SHIP CLASSIFICATION

GUIDELINES FOR SURVEY OF INTELLIGENT INTEGRATION PLATFORM

2026

Effective from 1 June 2026

CONTENTS

CHAPTER 1 GENERAL

1.1 Objectives and application

1.1.1 The Guidelines are survey guidelines for intelligent integration platforms of ships, specifying technical and survey requirements for such platforms.

1.1.2 The Guidelines are supplementary to the Rules. The intelligent integration platform is, in addition to satisfying the requirements of the Guidelines, to comply with the provisions in Chapter 7 of ISC Rules for Intelligent Ships.

1.1.3 The intelligent integration platform (hereinafter referred to as "the platform") is the platform to achieve onboard data acquisition/collection, storage, sharing and management, which is open and expandable.

1.2 Class notations

1.2.1 The intelligent integration platform is divided into two categories by function: basic platform and support platform. The platform category may be expanded with the increase of functions and data application requirements.

1.2.2 The basic platform is to be provided with the following functions:

(1) data acquisition/collection;

(2) data storage;

(3) data sharing;

(4) data management.

1.2.3 The support platform is also to be provided with the following functions in addition to those specified in 1.2.2:

(1) data integration;

(2) visualization;

(3) ship-shore information exchange (if applicable).

1.2.4 The support platform is to be capable of providing support for two or more intelligent systems specified in ISC Rules for Intelligent Ships as a minimum.

1.2.5 Class notation for product

A system complying with the requirements of the Guidelines is assigned a notation of corresponding category upon satisfactory completion of type approval or unit/batch inspection, which is indicated in the column of class notation for product of the certificate.

1.2.6 Class notation for ship

After obtaining the class notation for product, the ship may be assigned a notation of corresponding category upon satisfactory completion of surveys during construction and after construction. The notation is indicated in the column of class notation for ship.

1.3 Normative references

1.3.1 The following referenced documents are indispensable for the application of the Guidelines. For undated references, the latest edition of the referenced document applies.

References **Table 1.3.1**

No.	Document No.	Document Name
1		ISC Rules for Classification of Sea-going Steel Ships
2		ISC Rules for Intelligent Ships
3		ISC Guidelines for Type Approval Test of Electric and Electronic Products
4		ISC Guidelines for Assessment of Security and Reliability of Marine Software
5		ISC Guidelines for Ship Cyber Security
6		Guidelines for Verification of Digital Systems of Ships and Offshore Installations
7	IACS UR E22	On Board Use and Application of Computer-based systems
8	IEC 60812	Analysis techniques for system reliability - Procedure for failure mode and effects analysis (FMEA)
9	IEC 61162-450	Maritime navigation and radiocommunication equipment and systems - Digital interfaces - Part 450: Multiple talkers and multiple listeners - Ethernet interconnection
10	IEC 61162-460	Maritime navigation and radiocommunication equipment and systems - Digital interfaces - Part 460: Multiple talkers and multiple listeners - Ethernet interconnection - Safety and security
11	IEC 61508	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems
12	IEC 62940	Maritime navigation and radiocommunication equipment and systems - Integrated communication system (ICS) - Operational and performance requirements, methods of testing and required test results
13	ISO 9241-210	Ergonomics of human-system interaction -- Part 210: Human-centred design for interactive systems
14	ISO 16425	Ships and marine technology -- Guidelines for the installation of ship communication networks for shipboard equipment and systems
15	ISO 18028-2	Information technology -- Security techniques -- IT network security -- Part 2: Network security architecture

1.4 Definitions and abbreviations

1.4.1 Definitions

(1) System: a set of elements which interact according to a design, which may include hardware, software and human interaction.

(2) Stakeholders: a person or an organization that can affect, or is affected or is deemed being affected by decision-making or activities.

(3) Owner: the Owner is responsible for contracting the system integrator and/or suppliers to provide a hardware system including software according to the owner's specification. The Owner

could be the Ship Builder Integrator (Builder or Shipyard) during initial construction. After vessel delivery, the owner may delegate some responsibilities to the vessel operating company.

(4) System integrator: the system integrator is responsible for the integration of systems and products provided by suppliers into the system invoked by the requirements specified herein and for providing the integrated system. The system integrator may also be responsible for integration of systems in the vessel. The role of system integrator is to be taken by the yard unless an alternative organization is specifically contracted/assigned this responsibility. If there are multiple parties performing system integration at any one time a single party is to be responsible for overall system integration and coordinating the integration activities. If there are multiple stages of integration, different System Integrators may be responsible for specific stages of integration but a single party is to be responsible for defining and coordinating all of the stages of integration.

(5) Supplier: the Supplier is any contracted or subcontracted provider of system components or software under the coordination of the System Integrator or Shipyard. The supplier is responsible for providing programmable devices, sub-systems or systems to the system integrator. The supplier provides a description of the software functionality that meets the Owner's specification, applicable international and national standards, and the requirements specified herein.

(6) Human-centred design (HCD): an approach to systems design and development that aims to make interactive systems more usable by focusing on the use of the system and applying human factors/ergonomics and usability knowledge and techniques.

(7) Metadata: data that describe data.

1.4.2 Abbreviations

(1) ISC: International Ship Classification

(2) DCS: Distribution Control System

(3) ESD: Emergency Shutdown Device

(4) FAT: Factory Acceptance Test

(5) IEC: International Electrotechnical Commission

(6) IO: Input/Output

(7) ISO: International Organization for Standardization

(8) MPLS: Multi-protocol Label Switching

(9) PLC: Programmable Logic Controller

(10) VLAN: Virtual Local Area Network

(11) VPN: Virtual Private Network

CHAPTER 2 FUNCTIONAL NOTATIONS OF INTELLIGENT INTEGRATION PLATFORM

2.1 Functional notations

2.1.1 The functional notation I(x) of intelligent integration platform is defined in 7.2, Chapter 7 of ISC Rules for Intelligent Ships.

Explanations for Functional Notations of Intelligent Integration Platform Table 2.1.1

Functional notation	Meanings
I(b)	Functions of data acquisition/collection, data storage, data sharing and data management
I(s)	Functions of data integration, visualization and ship-shore information exchange (if applicable)in addition to the functions of I(b)

CHAPTER 3 SYSTEM REQUIREMENTS

3.1 General requirements

3.1.1 The platform is to support multi-terminal (PC and mobile device) access.

3.1.2 The platform is to realize multi-department and multi-user cooperative management according to company's relevant requirements for management system.

3.1.3 Where the platform has the function of transmitting control commands, it is to ensure the timeliness and accuracy of the transmission of commands.

3.1.4 Log management function of the intelligent integrated platform required by 3.9 of this Chapter is to be provided, at least including error logs, query logs, and change logs, so that users with authorization for log maintenance may carry out the maintenance of log.

3.1.5 The computer-based systems of the platform are to be categorized based on data usage, function, security risk level as well as satisfying applicable requirements of Chapter 2, PART SEVEN of ISC Rules for Classification of Sea-going Steel Ships.

3.1.6 The platform is to have scalability and complete data interface plan to facilitate access of other systems.

3.1.7 The platform is to comply with the data management function as required in 3.8 of this Chapter.

3.1.8 The data activities of the intelligent integration platform is to comply with the requirements on data quality in Section 5, Chapter 1 of ISC Guidelines for Verification of Digital Systems of Ships and Offshore Installations.

3.1.9 In the event of a failure of normal power supply, the system is to be capable of being automatically changed over to an independent standby power supply. The standby power supply may be an accumulator battery, with a capacity at least sufficient for a period of supply of 30 min. Where such systems could be adversely affected by an interruption in power supply, change-over to the standby power supply is to be achieved without a break.

3.2 Data collection/acquisition

3.2.1 Normalized data standards are to be established for acquired/collected data, including standards relating to data definition, data description, data quality, data transmission and data processing, so as to realize data traceability.

3.2.2 Validation check is to be carried out during data acquisition by removing duplicate data and erroneous data, initially completing missing data and giving effective reminding of error data.

3.2.3 Data input in the platform is to comply with the internationally recognized data formats.

3.2.4 Data acquired by the platform is to be uniquely identified. For data identification, reference may be made to Chapter 2 of ISC Guidelines for Verification of Digital Systems of Ships and Offshore Installations.

3.2.5 The communication protocol for data acquisition is to comply with the requirements in 3.2.3 and 3.2.4, Chapter 3 of ISC Guidelines for Verification of Digital Systems of Ships and Offshore Installations.

3.2.6 Data acquisition is to have fault-tolerant mechanism.

3.3 Data storage

3.3.1 A redundant design is to be used for data storage devices to ensure the availability of platform functions.

3.3.2 Data stored is to satisfy the expected application demands and quality requirements.

3.3.3 Periodical evaluation is to be carried out for collected data to ensure the accuracy, integrity and availability of data.

3.4 Data sharing

3.4.1 The platform is to provide an external data transfer interface and have the ability to share data with relevant parties.

3.4.2 The platform is to be able to ensure the integrity and reliability of data during the sharing process:

(1) It is to have a data integrity check and automatic retransmission mechanism to ensure that the data transmission content has not been tampered with or damaged;

(2) It is to support transmission identity verification functions to ensure that the data sharing objects are trustworthy and the data sharing function is traceable.

3.5 Data integration

3.5.1 The platform is to be capable of integrating multi-source heterogeneous data to support data applications and decision-making.

3.5.2 In different interaction scenarios, the platform is to conduct reasonable resource scheduling to meet the business requirements of different intelligent systems.

3.5.3 The platform is to be capable of integrating the information resources from existing intelligent systems on board, and the data acquired by intelligent systems may be stored in the platform database or an effective call relationship may be established with them.

3.5.4 When the platform is used to integrate newly added systems (such as integrated navigation system(INS), etc.) in accordance with conventions, regulations, rules, and company management and operational needs, the data acquired by these newly added systems may be stored in the intelligent integration platform database or an effective call relationship may be established with them.

3.6 Ship-shore information exchange

3.6.1 Stable and reliable communication protocols and data transmission mechanism is to be adopted for communication between ship and shore.

3.7 Visualization

3.7.1 The platform is to be able to provide the results of data analysis as request by the user and display in proper form.

3.8 Data management

3.8.1 Data source management

3.8.1.1 The platform is to support authorized users to query the data source directory.

3.8.1.2 The platform is to support authorized users to create aliases for data sources and describe basic attributes, locations, usage scopes, and information association models for all facilities or systems.

3.8.1.3 The platform is to regularly test the connectivity of data sources and generate alerts for link interruptions or data source losses.

3.8.1.4 Querying of data source directory is to support record auditing.

3.8.2 Metadata management

3.8.2.1 The platform is to support the maintenance of metadata and establishment of a synchronization mechanism for metadata with the connected systems.

3.8.2.2 The platform is to support authorized users to query metadata information based on expected data application requirements.

3.8.2.3 Query and modification of metadata information are to support record auditing.

3.8.3 Clock management

3.8.3.1 The clock of the platform system is at least to be synchronized with UTC.

3.8.3.2 The platform is to be able to identify the loss of system time synchronization and issue timely alerts.

3.9 Log management

3.9.1 The platform is to be capable of generating security-related auditable records, with the following requirements:

(1) Event types

① Attempts to access the intelligent integration platform management interface and administration authentication requests;

② operations on all configurations of the platform, including but not limited to adding/deleting accounts, modifying authentication information, data input and output, modifying metadata information, important configurations, user permission, etc.;

③ backup of log information, etc.;

④ important security events;

⑤ records of data queries and exports;

⑥ other event information that need to be recorded.

(2) Management

① Audit information such as logs is to be protected to prevent unauthorized access and tampering;

② tools for viewing logs are to be provided, with the ability to search for audit events based on conditions such as time, date, subject identifier, object identifier, etc.;

③ it is to support categorization of system events recorded in logs;

④ log records are to be retained for at least one survey cycle.

3.10 Requirements for software and supporting hardware

3.10.1 Organizations in charge of software modifications are to be clearly declared by Owner to ISC. A System integrator is to be designated by the Owner and is to fulfil requirements of ISC Guidelines for Assessment of Security and Reliability of Marine Software. Limited life cycle steps may be considered for modifications already considered and accepted in the scope of initial approval. The software modification effect analysis record and test report are to be submitted to

ISC for information. It is the responsibility of the owner to manage traceability of these modifications. The achievement of this responsibility is to be supported by system integrators updating the software registry.

3.10.2 The owner is to ensure that necessary procedures for software and hardware change management exist on board, and that any software modification/upgrade are performed according to the procedure. All changes to computer-based systems in the operational phase are to be recorded and be traceable.

3.10.3 The owner, system integrator and suppliers are to adopt physical and logical security policies and include these in their quality systems and procedures. to prevent unauthorized or unintentional modification regardless whether the system is physical or remotely-controlled. Prior to installation, all artefacts, software code, executables and the physical medium used for installation on the vessel are to be scanned for viruses and malware. Results of the scan are to be documented and properly kept.

CHAPTER 4 DATA SECURITY

4.1 General requirements

4.1.1 The following questions need to be addressed at the stage of demand analysis and design:

(1) What kind of information needs to be protected?

(2) what are the security risks, and what kind of protection is needed to manage these risk?

(3) what are the distinct types of network activities that need to be protected?

(4) What are the distinct types of network equipment and facility groupings that need to be protected?

4.1.2 A risk assessment is preferably to be conducted to prioritize the protection requirements and help to determine the appropriate security measures for security architecture.

4.1.3 A multifaceted Reference Architecture in ISO 18028-2 is recommended by the Guidelines. The principles described by the multifaceted Reference Architecture can be applied to a wide variety of networks independent of the network's technology or location in the protocol stack. Here are the additional requirements.

4.2 Access Control Security Dimension

The Access Control Security Dimension provides authorization for the use of the network resources. Access control ensures that only authorized personnel or devices are allowed access to network elements, stored information, information flows, services and applications. For example, Role-Based Access Control (RBAC) provides different access levels to guarantee that individuals and device can only gain access to and perform operations on network elements, stored information, and information flows for which they are authorized.

In general, some configuration parameters are preset by the designer while others are frequently changed by the operating and maintenance personnel in the pre-defined limit. The value of default parameters and the permissible scope of change (operators and engineers are usually different) have been determined subject to appropriate analysis, in order to establish and maintain safe and reliable operation of equipment and ship.

The maintenance of security data is to be designed in the system. The common type of protection is authorization at different levels, which is realized through the password protection of the user interface. For a ship with shore-based connection, as the vulnerability point of security data is changed, any circumvention of the normal user interface control mechanism is to be identified and mitigation measures are to be taken.

The access permit is to be examined on an irregular basis.

4.3 Authentication Security Dimension

The Authentication Security Dimension serves to confirm the identities or other authorizing attributes of communicating entities. Authentication ensures the validity of the claimed identities when used by authorization or Access Control of the entities participating in communication (e.g. person, device, service or application) and provides assurance that an entity is not attempting a masquerade or unauthorized replay of a previous communication. Authentication methods that employ techniques based on user identification and password pair, two-factor authentication (e.g. token), biometrics are among widely used methods.

The following two important aspects need to be considered:
-- data from a remote source, e.g. shore-based facilities; and
-- time scale or order of received data.

4.4 Non-repudiation Security Dimension

The Non-repudiation Security Dimension provides technical means for preventing an individual or entity from denying having performed a particular action related to data by making available proof of various network-related actions (such as proof of obligation, intent, or commitment; proof of data origin, proof of ownership, proof of resource use). It helps to ensure the availability of evidence that can be presented to a third party as technical proof that some kind of event or action has taken place. Note, however, that non-repudiation provided by technical means does not lead to a necessary conclusion of law. Cryptographic methods are often used for providing non-repudiation.

4.5 Data Confidentiality Security Dimension

The Data Confidentiality Security Dimension protects data from unauthorized disclosure. Encryption is a method often used to ensure data confidentiality. Access control lists, and file permissions are methods that help to keep data confidential.
The management of confidentiality of decommissioned systems or components is to be considered.

4.6 Communication Flow Security Dimension

The Communication Flow Security Dimension ensures that information flows only between the authorized end points (the information is not diverted or intercepted as it flows between these end points). Security mechanisms of Communication Flow Security Dimension do not protect against modification/corruption; this is a function of Data Integrity. MPLS tunnels, VLANs, and VPNs are examples of technologies that can provide communication flow security.
Other requirements are given in Chapter 5 of the Guidelines.

4.7 Data Integrity Security Dimension

The Data Integrity Security Dimension ensures the correctness of accuracy (i.e., data are only processed by authorized processes or actions of authorized people or devices) of data. The data is protected against unauthorized modification, deletion, creation, and replication and provides an indication of these unauthorized activities. Hashed Message Authentication Code methods (e.g. MD5, SHA-1) often used for ensuring data integrity.
Data integrity needs to be managed as required by the system lifecycle, including through design and realization, at all operating stages, all operations in degraded modes and in case of any change to the system.

4.8 Availability Security Dimension

The Availability Security Dimension ensures that there is no denial of authorized access to network elements, stored information, information flows, services and applications due to events impacting the network. Disaster recovery solutions are included in this category.

For conventional and small system architecture, the communication infrastructure may lack the capability to manage the maximum load or it is very sensitive to interruption.

Data availability is very important to intelligent ships with a growing trend of accessing remote information by applying satellite communication or providing shore to ship remote control to some extent.

At the concept design stage of system development, due consideration is to be given to the demand and strategy indicating data availability, in order to control the condition where data availability is limited. Such strategy is to include structural and detailed design solutions, e.g. redundant communication channel or alternative operation method by human intervention.

The adequacy of provisions regarding the management of data integrity is to be assessed at the design stage, including the following issues:

(1) the extent to which the threat to data integrity has been determined;

(2) specific design parameters which have been included;

(3) the level of safeguard that has been applied to data preparation;

(4) data management characteristics of application programmes.

4.9 Privacy Security Dimension

The Privacy Security Dimension provides for the protection of any information (identity of a party to communications or any data—including packet headers—pertaining to any activity carried by this party) that might be derived from the observation of network activities. Example of this information include web-sites that a user has visited, a user's geographic location, and the IP addresses and DNS names of devices in a Service Provider network. Network Address Translation (NAT) and application proxies are examples of the techniques that can be used for privacy protection. Depending on the respective national privacy and data protection legislations and regulations, this Privacy Security Dimension is also to provide the appropriate protection structure and controls for collection, processing and dissemination of personal information.

CHAPTER 5 NETWORKS AND COMMUNICATION

5.1 General requirements

5.1.1 The Section focuses on the security of networks and communication infrastructure. The security and reliability of networks and software need to satisfy the requirements of Chapter 8, in addition to the following requirements:

(1) Loss of a data link is to be specifically addressed in risk assessment analysis.

(2) A single failure in data link hardware is to be automatically treated in order to restore proper working of system.

(3) Characteristics of data link is to prevent overloading in any operational condition of system.

(4) Data link is to be self-checking, detecting failures on the link itself and data communication failures on nodes connected to the link. Detected failures are to initiate an alarm.

(5) Information can only flow between authorized endpoints (information will not be diverted or intercepted when flowing between these endpoints).

5.2 Remote communication

5.2.1 Appropriate type and bandwidth of remote communication are to be selected, in order to ensure that priority is granted to business essential systems or security system when needed.

5.2.2 Appropriate operational control is to be considered to address bad communication that occurs occasionally.

CHAPTER 6 ERGONOMIC SYSTEM

6.1 Human-centred design

6.1.1 Human-centred design is necessary for system development and operation, the purpose of which is to provide a structure using human-centred methodology in order to ensure that the effect of human factor on intelligent integration platform is adequately located and relevant risk has been reduced to the lowest reasonable level. Design principles and evaluation can be carried out in accordance with ISO 9241-210.

6.1.2 Human-centred design follows the following principles:

(1) an explicit description reflecting the operational idea of intelligent integration platform

(2) early, continuous and effective personnel investment;

(3) continuous improvement, learning based on experience, attempt or prototype;

(4) providing system with persons and tasks based on user experience;

(5) a multidisciplinary team.

6.1.3 Human-centred design is to be planned and integrated into all phases of the life cycle of intelligent integration platform. Human-centred design activities are to start at the earliest stage of the project. To ensure that it is followed through on and implemented effectively, the plan for human-centred design is to be subject to the same project disciplines (e.g. responsibilities, change control) as other key activities.

6.1.4 Human-centred design aspect in the project planning is to be reviewed and revised as appropriate in the life cycle of the project. Project planning is to allocate time and resources to human-centred activities. This is to include time for iteration and the incorporation of user feedback, and for evaluating whether the design solution satisfies the user requirements. Additional time is also to be allocated to communication and reconciliation among design teams.

6.2 Ergonomic considerations

6.2.1 General requirements

(1) Reducing human data processing. Data is to be processed by equipment insofar as practicable and the result is to be presented to relevant person for decision-making.

(2) Harmonization between physical layout and monitoring interface. The control and display in the monitoring interface are to be consistent with the equipment of physical layout. The flow chart is to reflect the logical relationship between equipment.

(3) Adapted to routine operational habit. The consistency between control action and display response is to be maintained during the platform design.

(4) Consistency of images:

① the same color is to denote the same meaning in different images;

② different images are to have the same style of layout;

③ the computer display is to correspond to panel display.

(5) Effective display:

① the intelligent platform is to avoid interference or meaningless tasks;

② common or important display is to be arranged in the central visual region so that the displayed information is clear and easy to understand;

③ the alarm is not to be triggered frequently, which might affect the attention of monitoring personnel;

④ information is to be grouped so that the monitoring personnel can process a large amount of information calmly;

⑤ the priority of tasks and alarms is to be established.

(6) Convenience of monitoring

① the control device is to be close to the corresponding display and within the operational range of personnel;

② when viewed from the nominal position, the monitor:

a. is to be easy to read;

b. is located within a direct field of view;

c. has sufficient color, brightness and contrast;

d. allows the monitoring personnel to see the environmental conditions (weather conditions or day and night) out of the corner of the eye.

③ The environment of the control room is not to interfere with the visual or audible signals;

④ operation that prevents negligence is to be in place;

⑤ all control equipment is to be easily accessible and operate.

(7) Effective images:

① effective methods are provided to show important and changed information;

② multiple displays are to be avoided to access frequently used or critical information. Critical information is to be displayed immediately;

③ cross reference between information display is to be avoided;

④ control is to be distinguishable from display;

⑤ identification is to be simple and easy to memorize;

⑥ the update of information is to be quick;

⑦ a clear and continuous automatic indication of system status is to be provided.

(8) Information search and interpretation are simplified by color coding:

① color is not to be used as the only coding mechanism to convey information, which is to be used in conjunction with other coding mechanisms;

② the use of color is not to reduce the readability of images, tags, maps, etc.;

③ it is to be easy to distinguish between used colors;

④ there are not to be more than 7 types of used colors.

6.2.2 Simple, direct, easy to input and control

(1) Providing direct manual control

The design of system interface is to be interactive, which can improve the operating speed. It is to be ensured that manual control is correctly performed through clear control entries. The automation system is to accept manual planned input and intervention.

(2) Clear identification control mode

Automatic, auxiliary and manual control modes are to be displayed clearly in the vicinity of control components.

(3) Prompt of any change of control mode

The changeover of control mode is to ensure that:

① confirmation from the operator is needed;

② the current control mode is to be indicated before the changeover takes place and a sound signal is given as a hint of changeover;

③ a clear audible and visual hint is to be given during the changeover to manual control mode.

(4) Providing guidance to human intervention in the automation system

Guidance is to be given in the following cases:

① when to take over from the automatic control;

② when or how to switch the control right from one place to another;

③ when to close the equipment or system.

(5) Providing direct and instant feedback for control action

Controls and corresponding display are to be placed together insofar as practicable.

① the operation or command of equipment is to be have corresponding display, accompanied by immediate display of feedback signal;

② in case of operation by several persons, all relevant information is to be provided to other responsible persons at the same time for task coordination;

③ information required for diagnostics or decision-making control is to be provided at the same time instead of continuously.

(6) Providing simple image display

① the menu hierarchy of image is not to exceed three levels;

② a hierarchy chart or other hinted information is to be provided, so as to help the operator find the required image conveniently.

(7) Response delay and availability of system status

The response of control system is to be recorded and the record of intermediate system response is to be available.

6.2.3 Reducing human errors

(1) Providing error prevention and tolerance

For operations that might directly endanger the ship, personnel or the environment, the software or hardware is to be provided with protective operations. An action that might cause harm is to be confirmed. In possible cases, the software is to supervise and guide the safety of personnel behavior.

(2) Considering the communication demand of tasks

The communication system is to satisfy the following requirements:

① frequent movement by operators to different positions for access to the communication equipment is to be avoided;

② consideration may be given to the use of portable, no-load equipment or fixed communication equipment.

(3) Avoiding any conflict of control

The concurrent control of system or equipment from different workstations is to be avoided. The concurrent operation of control and display of one piece of equipment conducted by two or more persons is to be avoided, i.e. the right of control of one system can only be obtained by one operator each time.

(4) Requirements for provision of operators

① the provision of personnel for all operating modes is determined based on the workload;

② considering whether the level, skill and experience of personnel can satisfy requirements for operation and failure disposal;
③ considering the provision of personnel in the worst case;
④ considering the provision of personnel in the normal case;
⑤ tasks are assigned in accordance with personnel skill and experience.

6.3 Training

6.3.1 Determination of required knowledge, skill and capability

Understand what operators need to do and provide training to complete required work tasks.

6.3.2 Identification of training demands and requirements

(1) specific training requirements are developed in terms of the intelligent platform and automation function;

(2) identify automatic function operation and intervention measures of operators. Identify automatic and manual conditions;

(3) provide training on automation control related to ship control;

(4) provide training on important tasks;

(5) provide practical training on changeover between automatic and manual control.

6.3.3 Prompt of program

(1) provide available written or on-line program to guide and record uncommon conditions, complex or safety critical operations;

(2) provide guidance to the action of operators through the program rather than the display of commands in special alarm conditions;

(3) provide programs to address uncommon or assumed conditions;

(4) provide on-line help.

6.3.4 Provision of tags and warning

Provide standardized, durable, readable and available tags for all equipment and components. Tags and marks are to be consistent in terms of:

(1) use of codes and colors;

(2) display position;

(3) language and grammar;

(4) design style.

CHAPTER 7 INFORMATION APPLICATION

7.1 Information display

7.1.1 Information categorization and display

The categorization and display of Intelligent Integration Platform information are to comply with the requirements of IMO Resolution A.1021(26).

Special attention is to be paid to the harmonization on the priority, categorization, processing, distribution and display of alarms so as to avoid adverse effects on ship's navigation or other functions related to safety and environmental protection.

7.1.2 Input and output devices

Input and output devices of computer-based systems are to be designed for ease of handling and user-friendliness and are so far as possible to follow ergonomic principles.

(1) The keyboard of a computer is to meet the following requirements:

① Where equipment operations or functions may be changed via keyboards, appropriate measures (such as setting password) are to be employed so as to limit access of such operations to authorized personnel only.

② If the operation of a key is able to cause dangerous operating conditions, measures are to be taken to prevent the instruction in question from being executed by a single action such as use of a special key lock, or use of two or more keys.

(2) The computer displays are to comply with following requirements:

① The size, color and resolution of text and graphic information displayed on a visual display unit is to be such that it may be easily read from the normal operator position under all operational lighting conditions. The brightness and contrast are to be capable of being adjusted to the prevailing ambient conditions.

② Information is to be displayed in a logical priority.

③ If alarm messages are displayed on color monitors, the distinctions in the alarm status are to be ensured even in the event of a failure of a primary color.

(3) Where a display unit is used for alarm in place of a general indicating lamp, the following requirements are to be satisfied:

① The indication of the display unit is to be clear under the bright environmental condition. Data and information shown on the display unit are to be capable of being easily read by an operator in a normal working position.

② The display unit is to be capable of clearly indicating all the alarm signals.

③ The display unit is to be capable of distinguishing the status of fault alarms, i.e., the status before and after acknowledgment; but this distinction is not to be shown by means of different colors only.

④ A storage device and an output interface are to be provided in order to record and output the faults and their time of occurrence.

⑤ For the platform, at least a standby display unit or lamp panel is to be provided, or a printer is to be provided in order to record the faults and their time of occurrence.

⑥ The display unit is to be capable of normal operation in the event of a failure of the normal power supply.

⑦ Where a display unit is common to parameter and alarm displays, the parameter display is not to interfere with the initiation of alarm signals.

7.2 Information application

7.2.1 When the intelligent integration platform is supporting intelligent systems specified in ISC Rules for Intelligent Ships, information processing and application are to comply with the requirements in ISC Rules for Intelligent Ships and the corresponding survey guidelines.

CHAPTER 8 SECURITY REQUIREMENTS

8.1 General requirements

8.1.1 The Intelligent Integration Platform is to comply with the basic requirements for automation systems in PART SEVEN of ISC Rules for Classification of Sea-going Steel Ships.

8.1.2 Software is to comply with the requirements of ISC Guidelines for Assessment of Security and Reliability of Marine Software.

8.1.3 Cybersecurity is to comply with the requirements of ISC Guidelines for Ship Cyber Security.

8.1.4 Hardware is to function in the environmental conditions specified in Section 1, Chapter 2, PART SEVEN of ISC Rules for Classification of Sea-going Steel Ships and other working conditions.

CHAPTER 9 BASIC SURVEY REQUIREMENTS

9.1 Product certification requirements

9.1.1 Certification of the intelligent integration platform system and components are to comply with relevant provisions in 1.10, Chapter 1 of ISC Rules for Intelligent Ships.

9.2 Plans and documents as well as tests

9.2.1 The following Table lists plans to be submitted and tests and trials to be carried out by stakeholders.

Lists of Plans to be Submitted and Tests and Trials to be Carried out Table 9.2.1

No	Requirement	Stakeholders				Classification Society				
		Supplier	System integrator	Ship designer	Owner	Type approval of product	Plan approval of ship	Unit/batch inspection	Construction survey	Survey after construction
1	System description	○	×			Ⓐ	ⓒ	ⓒ		
2	Hardware description	○	×			Ⓐ		ⓒ		
3	Wiring connection diagram	○	×	ⓒ		Ⓐ	ⓒ	ⓒ		
4	Software description	○	×			Ⓐ		ⓒ		
5	User interface description	○	×	ⓒ		Ⓐ	ⓒ	ⓒ		
6	Risk assessment report	○	×			Ⓐ (where necessary)		ⓒ		
7	Type test program (excluding functional and failure tests)	○	×			Ⓐ				
8	Test program for functional and failure tests	○	×			Ⓐ		ⓒ		
9	Operation Manuel	○	×	ⓒ	ⓒ	Ⓘ	ⓒ	ⓒ	ⓒ	ⓒ
10	Quality Plan	○	×			Ⓘ				
11	Evidence of verification of software	○	×			Ⓘ				
12	Type test report (including functional and failure tests)	○	×			ⒶⓌ				

No	Requirement	Stakeholders				Classification Society				
		Supplier	System integrator	Ship designer	Owner	Type approval of product	Plan approval of ship	Unit/batch inspection	Construction survey	Survey after construction
13	Single line diagram of onboard systems (including power supply)			×	ⓒ		Ⓐ	ⓒ	ⓒ	
14	Arrangement of onboard systems			×	ⓒ		Ⓐ	ⓒ	ⓒ	
15	Functional description of software	○	×		ⓒ			Ⓘ		
16	List and versions of software installed in system	○	×		ⓒ			Ⓘ	ⓒ	ⓒ
17	User manual including instructions during software maintenance (including necessary procedure for management of software and hardware changes)	○	×		ⓒ			Ⓘ		ⓒ
18	List of interfaces between system and other ship systems	○	×		ⓒ			Ⓘ	ⓒ	ⓒ
19	List of data transmission standards	○	×		ⓒ			Ⓘ		
20	Factory acceptance test program	○	×					Ⓐ		
21	Factory acceptance test report	○	×					ⒾⓌ		

No	Requirement	Stakeholders				Classification Society				
		Supplier	System integrator	Ship designer	Owner	Type approval of product	Plan approval of ship	Unit/batch inspection	Construction survey	Survey after construction
22	Test program for on board tests (including wireless network testing)		×	○	ⓒ				Ⓐ	ⓒ
23	System installation procedure		×	○	ⓒ				Ⓐ	
24	On board test report (acceptance test)		×	○	ⓒ				ⒶⓌ	
25	On board test report (integration test)		○	×	ⓒ				ⒶⓌ	ⒾⓌ
26	Updated Software Registry		×		○			ⓒ	Ⓘ	Ⓘ
27	Analysis record and test report of software change effects		×		○			ⓒ	Ⓘ	Ⓘ

Symbols:

1) Ⓐ submitted to ISC for approval; Ⓘ submitted to ISC for information;
Ⓦ To be witnessed by ISC surveyors;

2) ⓒ Submitting approved documents/documents for information;
× To be submitted/carried out; ○ To be submitted/carried out when necessary.

Note 1: The Table above gives general requirements for documents to be submitted by stakeholders, who may submit applicable part of the documents above according to the actual situation.

Note 2: ⓒ means submitting approved documents/documents for information. For example, for No.9 Operation Manual, system integrator or supplier submits it to ISC for information; after the Manuel is stamped with ISC stamp "For information", it needs to be provided to ship designer, owner and plan approval unit as supporting material or background material.

Note 3: ⒶⓌ means the surveyor may either check the test report or witness the test or carry out a combination of both.

Note 4: ⒾⓌ means the surveyor may either review the test report for information or witness the test or carry out a combination of both.

Note 5: For × and ○ in each line, documents are recommended to be submitted by ×, but may also be submitted by ○; submission by one party will suffice. For example, No.1 System instructions may be submitted by either system integrator or supplier.

9.3 Plans and documents

9.3.1 The following plans and documents are to be submitted to ISC for approval:

(1) System description (product technical specification) is to specify the general performance requirements as well as general design requirements for the product, covering at least applicable part of the following:

① provisions for the environmental conditions of the product: product compatibility requirements to the working conditions (including electromagnetic compatibility) specified in ISC Rules for Classification of Sea-going Steel Ships;

② detailed description of product functions: including system configuration, applicability of the product, control and monitoring functions of the product and detailed description of the realization method, detailed description of the safe status of each realized function, system characteristics in each operation condition (including emergency, failure) as well as operation guidelines of the system in normal and abnormal conditions;

③ detailed description of control changeover;

④ detailed description of redundancy setup and changeover mechanism;

⑤ detailed description of failure monitoring and identification functions (automatic and manual);

⑥ detailed description of data security, user's security level (entry restriction to functions);

⑦ list of control and testing items: list of all input/output signals of the system (service description, instrumentation, types, range and set limit of systems and signals).

(2) Hardware description

Applicable part of the following is to be included as a minimum:

① technical specification of hardware and peripheral configuration

② block diagram: showing internal connection of main components (software and hardware units, module) of system and interface with other system;

③ detailed description of main hardware configuration of the product;

④ detailed description of input and output devices;

⑤ detailed description of power supply equipment.

(3) Wiring connection diagram

Applicable part of the following is to be included as a minimum:

① power supply arrangement: showing power supply arrangement of the system and the connection of the system to the switch board, battery, transformer or UPS;

② circuit diagram of important hardware circuit, such as emergency operation and interlock, details of input and output devices, power supply condition of each circuit.

(4) Software description

Applicable part of the following is to be included as a minimum:

① description of the basic software installed in each hardware unit;

② description of the communication software installed on nodes in a network;

③ description of application software: information of system module keeping functions working and of system's dependency on other systems, relations of software modules keeping functions working, data flow and control flow among software modules;

④ software configuration, including preferred option;

⑤ changeover mechanism of redundant systems.

(5) User interface description

Applicable part of the following is to be included as a minimum:

① function distribution of each working station and operation station as well as description of control changeover among stations;

② description of the functions specified for each input device;

③ layout, dimensions and necessary physical pictures of input/output devices;

④ user input interface description, menu description.

(6) Risk assessment report: risk assessment of the system is to be undertaken to determine the risk to the system throughout the lifecycle by identifying and evaluating the hazards associated with each function of the system. The risk assessment report is generally submitted by the system integrator or the supplier, including data coming from other suppliers. Based on the risk assessment, a revised system category might need to be agreed between ISC and the system supplier. Where the risks associated with a computer-based system are well understood, it is permissible for the risk assessment to be omitted, however in such cases the supplier or the system integrator is to provide a justification for the omission. The justification is to give consideration to the known risks, the equivalence of the context of use of the current computer-based system and the computer-based system initially used to determine the risks as well as the adequacy of existing control measures in the current context of use.

(7) Type test program (excluding functional and failure tests): according to the requirements of ISC Guidelines for Type Approval Test of Electric and Electronic Products, the developed type test program is to include, as a minimum, visual inspection, insulation resistance measurement, power supply variation and failure test, marine environment test, high voltage test, enclosure test, electromagnetic compatibility test.

(8) Test program for functional and failure tests: the process for functional and failure tests includes FMEA or similar analysis that may be required by ISC. The test procedure is to describe test configuration and simulation method in conjunction with the characteristics of specific products according to the provisions of the Guidelines. Each test is to stipulate initial state of equipment/system, test method, test result analysis and acceptance criteria. Each test is to cover normal mode and failure mode (including self-inspection of the system, simulation test of system failures, changeover of redundant devices, if any) as well as power supply and communication failure. Functional and failure tests can be demonstrated by simulation tests.

(9) Quality plan

A document based on life cycle, referred to herein as a Quality Plan, is to be produced that records how the quality management system will be applied for the specific computer-based system and that includes, as a minimum, all of the following materials.

① Relevant procedures regarding responsibilities, system documentation, configuration management and competent staff.

② Relevant procedures regarding software lifecycle and associated hardware:

- organization set in place for acquisition of related hardware and software from suppliers;
- organization set in place for software code writing and verification;
- organization set in place for system validation before integration in the vessel.

③ Minimum requirements for approval of Quality system:

- the Intelligent Integration Platform is to have a specific procedure for verification of software code at the level of systems, sub-systems and programmable devices and modules;

- the Intelligent Integration Platform is to have check points; examples of check points can be a required submittal of documentation, a test event, a technical design review meeting, or peer review meeting;
- the owner is to be informed of a specific procedure for software modification and installation on board the vessel.

(10) Type test report: the surveyor may either check the test report or witness the test or carry out a combination of both.

(11) Single line diagram of onboard systems (including power supply)

(12) Arrangement of onboard systems

(13) Factory acceptance test program:

① Intra-system integration testing is to be done between system and sub-system software modules before being integrated on board. The objective is to check that software functions are properly executed, that the software and the hardware it controls interact and function properly together and that software systems react properly in case of failures. Faults are to be simulated as realistically as possible to demonstrate appropriate system fault detection and system response. The results of any required failure analysis are to be observed.

② The requirements for functional and failure tests are tailored according to test programs for functional and failure tests.

③ The test program is developed by the supplier or the system integrator and co-confirmed by the system integrator, the owner and the classification society. In general, the test program is to include but not limited to the following: kick-off meeting (document specification, plan, etc.), check of the supplier's documents (including factory test report), check of the list of hardware and software (including version No.), mechanical check (acceptance), check of wiring and terminals, starting test, general system features (including hardware redundancy and diagnosis check), visual inspection/operation, functional and failure tests, check of advanced features and operation modes, system interface test, FAT changes, FAT closing meeting.

(14) Factory acceptance test report: the surveyor may either check the test report or witness the test or carry out a combination of both.

(15) Test program for on board tests (including wireless network testing):

① The test program for on board tests (activities and schedules) is developed by the system integrator and co-confirmed by the system integrator, the owner and the classification society. It includes acceptance and integration tests. On board tests are to check that a computer-based system in its final environment, integrated with all other systems with which it interacts is: a) performing functions it was designed for; b) reacting safely in case of failures originated internally or by devices external to the system; c) interacting safely with other systems implemented on board vessel; d) functioning properly with regard to data collection, storage, transmission, display and application; e) the functions of intelligent navigation, intelligent machinery, intelligent energy efficiency management are surveyed according to the requirements of each integration system; f) the requirements for functional and failure tests are tailored according to test programs for functional and failure tests.

② Where the test program for mooring/sea trials has already included relevant contents of the test program for on board tests, then it is not necessary to develop a separate test program for on board tests.

③ Acceptance tests: the test program is to include but not limited to the following: kick-off meeting (document specification, plan, etc.), check of the supplier and system integrator's documents (including factory test report), check of the list of hardware and software (including version No.), mechanical check (earthing system, power supply, internet connection, etc.), starting/diagnosis check (switching on power, initializing/test running the controller, carrying out diagnosis check), downloading software.

④ Integration tests: generally the test program is to include but not limited to the following: kick-off meeting (document specification, plan, etc.), check of the supplier and system integrator's documents (including factory test report), mechanical check (communication chain between systems), diagnosis check (communication between systems, baud rate, etc.), downloading software, where applicable. The test is to be carried out by the owner after the site acceptance test of each system is completed satisfactorily. The test is to test the connection of two or more independent systems. For example, when the system is integrated in the following forms, the test is to be carried out: with DCS/PLC communication analysis system using non-conventional IO signal; emergency shutdown (ESD) system; with DCS/PLC of several manufacturers; DCS integrated to network of higher structure; other connection of the system may also require the test.

(16) System installation procedure:

① The system installation procedure is developed by the system integrator and co-confirmed by the system integrator, the owner and the classification society. It includes operation environment, installation requirements and procedures of relevant devices. In particular the following are to be specified: a) environmental control requirements for computers, internet devices, sensors, actuators (e.g. temperature, humidity, salt air, vibration); b) requirements for installation, connection, electromagnetic compatibility, earthing of IT devices such as computers; c) installation requirements for sensors (e.g. routing of pipelines); d) requirements for selection of cables for sensors and actuators and for manufacturing connections; e) procedural requirements for cable laying.

(17) On board test report (acceptance test): the surveyor may either check the test report or witness the test or carry out a combination of both.

(18) On board test report (integration test): the surveyor for construction survey may either check the test report or witness the test or carry out a combination of both.

9.3.2 The following plans and technical documents are to be submitted to ISC for information:

(1) Operating manual (including trouble-shooting instructions);

It is to include system startup, function restoration, maintenance and periodical test, data security and data backup, user permissions, software reinstallation and system recovery, trouble shooting and repair, system updates, and other matters that users should pay attention to.

(2) Evidence of software verification:

① Software modules functional description and associated hardware description for programmable devices. This is to be provided by the supplier and the system integrator.

② Evidence of verification (detection and correction of software errors) for software modules, in accordance with the selected software development standard. Evidence

requirements of the selected software standard might differ depending on how critical the correct operation of the software is to the function it performs (i.e. IEC 61508 has different requirements depending on SILs, similar approaches are taken by other recognized standard). This is to be supplied by the supplier and the system integrator.

③ Evidence of functional tests for programmable devices at the software module, sub-system, and system level. This is to be supplied by the supplier via the system integrator. The functional testing is to be designed to test the provisions of features used by the software but provided by the operating system, function libraries, customized layer of software and any set of parameters.

(3) Description of software functions;

(4) List and versions of software installed in system;

(5) User manual including instructions for use during software maintenance (including necessary procedures for management of software and hardware changes);

(6) List of interfaces between system and other ship systems;

(7) List of standards used for data links;

(8) On board test report (integration test): the surveyor for survey after construction may either review the test report for information or witness the test or carry out a combination of both.

(9) Updated Software Registry:

① list and versions of software installed in system;

② scan results for viruses and malware;

③ check points of automated systems and the preset parameters of safety systems are to be included;

④ calibration log of the device is to be included, where applicable.

(10) Analysis record and test report of software change effects.

CHAPTER 10 SUPPLEMENTARY SURVEY REQUIREMENTS

10.1 Type approval of products

Type approval of products is to be carried out according to the requirements of Chapter 3, PART ONE of ISC Rules for Classification of Sea-going Steel Ships. There are following supplementary requirements:

(1) Type test is to be carried out according to type test program (not including tests of functional testing and failure testing) as well as test program of functional testing and failure testing.

(2) Approval of programmable devices integrated inside a system is to be delivered to the system integrator or supplier. Approval can be granted on case by case basis, or as part of a product type approval, so long as the documents 1-11 of Table 9.2.1 have been reviewed/approved and the document 12 has been submitted upon completion of type tests. Documentation should address the compatibility of the programmable device in the ship's application, the necessity to have on board tests during ship integration and should identify the components of system using the approved programmable devices.

(3) Sub-systems and programmable devices may be approved for limited applications with service restrictions by ISC when the ship system where they will be integrated is not known. In this case, additional drawings, details, tests reports and surveys related to the standard declared by the supplier may be required by ISC upon request. Sub-systems and programmable devices may in this case be granted with a limited approval mentioning the required checks and tests performed.

10.2 Ship plan approval

Ship plan approval is to be carried out according to the requirements of Section 5, Chapter 2, PART ONE of ISC Rules for Classification of Sea-going Steel Ships. There are following supplementary requirements:

(1) System integrators or suppliers are to submit documents 13 and 14 referred to in Table 9.2.1 for satisfactory review.

10.3 Unit/batch inspection

(1) In general, products/systems have been approved according to requirements for type approval of products mentioned above, and plan approval has been completed according to the requirements for ship plan approval mentioned above. At this point, product plan approval and inspection is carried out according to the requirements for unit/batch inspection in Section 2, Chapter 3, PART ONE of ISC Rules for Classification of Sea-going Steel Ships.

(2) If products/systems have not been approved, application for unit/batch inspection need to be carried out according to the requirements of paragraph 3.2.2.4, Section 2, Chapter 3, PART ONE of ISC Rules for Classification of Sea-going Steel Ships.

(3) Documents 15 to 20 referred to in Table 9.2.1 are to be submitted for satisfactory review.

(4) There are following supplementary requirements for factory acceptance test:

Test is to be carried out according to factory acceptance test program with detailed test steps as follows:

① Test preparation. Rack/long distance IO (to force IO by connecting simulation equipment at field end), bus interface, subsystem connection.

② Test implementation, including system property, project-related supply and examination of application contents, mainly as follows: examination testing of system property (start-up testing, including normal functional testing of hardware redundancy and diagnosis), examination of contents relating to project provided (document examination, examination of hardware and software list (including version), machinery examination (acceptance), wiring and terminal examination), pressure-resistant insulation test (if applicable), references.

③ Steps of application examination: HMI display examination, comprehensive function and interlock examination, additional function, communication testing with each subsystem, system function examination (in addition to testing of relevant application function, system property also includes system failure recovery, redundancy, alarm processing and confirmation, guaranteed system performance, e.g. refresh rate).

10.4 Construction survey

(1) Document review

① Documents 22 and 23 referred to in Table 9.2.1 are to be submitted for satisfactory review.

② Relevant work is to be carried out after satisfactory review by the construction surveyor.

③ For program and technology with approval comments, the surveyor is to check shipyard's reply to the comments and implement them during corresponding survey.

④ During review, the emphasis is to confirm whether relevant requirements of PART SEVEN of ISC Rules for Classification of Sea-going Steel Ships are met. Approval of installation technology of relevant sensors is to meet corresponding technical requirements of the manufacturer.

(2) Onboard test

① Acceptance test and integration test are to be carried out according to onboard test program.

② For the requirements of acceptance test and integration test, refer to paragraph 9.3.1(14), (15).

③ If the supplier has carried out acceptance test and integration test mentioned in ② of this sub-paragraph, the supplier's report may also be accepted after audit. Satisfactory audit result can be treated as equivalent replacement to items 24 and 25 in Table 9.2.1, and the report is to be signed with record.

10.5 Survey after construction

(1) Following items are to be checked during annual, intermediate and special surveys:

① Previous operation records of intelligent integration platform are to be checked to confirm good operation of intelligent integration platform.

② Normal exchange of system data between ship and shore to confirm historical record of data exchange.

③ Random examination of system backup records to confirm that effective backup has been implemented to the system.

④ Survey of intelligent navigation, intelligent machinery and intelligent energy efficiency management according to the requirements of each integration system (integration test according to onboard test program when necessary).

⑤ If the supplier has carried out the testing work mentioned in above ① to ④, the supplier's report may also be accepted after audit. If site witness is impracticable due to time or testing condition, testing report completed within nearly one year may be audited. Satisfactory audit result can be treated as equivalent replacement to ① to ④, and the report is to be signed with record.

⑥ Whether following documents examined by ISC are kept on board ship: operational manual, software list and edition No. of system installation, software maintenance and instruction manual (including necessary procedure for management of software and hardware alteration), list of interface between system and other systems of the ship, onboard test program (items 9, 16, 17, 18 and 22 in Table 9.2.1).

⑦ Documents 26 and 27 referred to in Table 9.2.1 (if applicable) are to be submitted for satisfactory audit.

(2) Ship modification or alteration is to be carried out according to relevant requirements of Chapter 5, PART ONE of ISC Rules for Classification of Sea-going Steel Ships.

ANNEX 1 SUPPLEMENTARY EXPLANATION OF TEST

Examples in this Annex are only for reference, and test items and acceptance basis are to be negotiated by the stakeholders.

The purpose of type approval test is to demonstrate capability of device with expected function under specified test condition.

Classification of environment condition is shown in paragraph 1.3.2 of ISC Guidelines for Type Approval Test of Electric and Electronic Products (hereinafter referred to as "ISC Guidelines for Test").

According to purpose and installation position, electric and electronic devices are to be subject to relevant type approval test according to the provisions of Table 1.3.3.a of ISC Guidelines for Test. Type approval test items for electric and electronic devices of different type are shown in Table 1.3.3b of ISC Guidelines for Test.

Test items of type test (not including tests of functional testing and failure testing) are illustrated as follows:

Examples of test items of type test (not including tests of functional testing and failure testing)

No.	Test items	Test requirements	Remarks
1	Visual inspection	Paragraph 2.1 of ISC Guidelines for Test	
2	Insulation resistance test	Paragraph 2.3 of ISC Guidelines for Test	
3	Power supply variation and failure test	Paragraphs 2.4 and 2.5 of ISC Guidelines for Test	
4	Marine environment test	Paragraphs 2.6 to 2.13 of ISC Guidelines for Test	
5	High voltage test	Paragraph 2.14 of ISC Guidelines for Test	
6	Enclosure test	Paragraph 2.15 of ISC Guidelines for Test	
7	Flame retardant test	Paragraph 2.16 of ISC Guidelines for Test	When applicable
8	Electromagnetic compatibility test	Chapter 3 of ISC Guidelines for Test	

For tests of functional testing and failure testing, supplements are as follows:

The process for functional and failure tests includes FMEA or similar analysis that may be required by ISC. The test procedure is to describe test configuration and simulation method in conjunction with the characteristics of specific products according to the provisions of he Guidelines. Each test is to stipulate initial state of equipment/system, test method, test result analysis and acceptance criteria. Each test is to cover normal mode and failure mode (including self-inspection of the system, simulation test of system failures, changeover of redundant devices, if any) as well as power supply and communication failure. Functional and failure tests can be demonstrated by simulation tests.

Examples of functional testing and failure testing are shown in the following Table.

For the test program for on board tests (including wireless network testing), supplements are as follows:

① The test program for on board tests (activities and schedules) is developed by the system integrator and co-confirmed by the system integrator, the owner and the classification society. It includes acceptance and integration tests. On board tests are to check that a

computer-based system in its final environment, integrated with all other systems with which it interacts is: a) performing functions it was designed for; b) reacting safely in case of failures originated internally or by devices external to the system; c) interacting safely with other systems implemented on board vessel; d) functioning properly with regard to data collection, storage, transmission, display and application; e) the functions are surveyed according to the requirements of each integration system; f) the requirements for functional and failure tests are tailored according to test programs.

② Where the test program for mooring/sea trials has already included relevant contents of the test program for on board tests, then it is not necessary to develop a separate test program for on board tests.

③ Acceptance tests: the test program is to include but not limited to the following: kick-off meeting (document specification, plan, etc.), check of the supplier and system integrator's documents (including factory test report), check of the list of hardware and software (including version No.), mechanical check (earthing system, power supply, internet connection, etc.), starting/diagnosis check (switching on power, initializing/test running the controller, carrying out diagnosis check), downloading software.

④ Integration tests: generally the test program is to include but not limited to the following: kick-off meeting (document specification, plan, etc.), check of the supplier and system integrator's documents (including factory test report), mechanical check (communication chain between systems), diagnosis check (communication between systems, baud rate, etc.), downloading software, where applicable. The test is to be carried out by the owner after the site acceptance test of each system is completed satisfactorily. The test is to test the connection of two or more independent systems. For example, when the system is integrated in the following forms, the test is to be carried out: with DCS/PLC communication analysis system using non-conventional IO signal; emergency shutdown (ESD) system; with DCS/PLC of several manufacturers; DCS integrated to network of higher structure; other connection of the system may also require the test.

Examples of acceptance test and integration test are shown in the following Table.

Examples of function testing and failure testing

No.	Test item	Initial condition of device/system	Test method	Test result analysis and acceptance criteria	Test result requirements
1	Document check		Checking whether all documentshave been submitted and they are issued as controlled copies		
2	General examination of software and hardware		Verifying that contents of hardware structure, quantity, size and painting are consistent with relevant documents. In addition, contents of software authorization, spare parts and consumables are also to be checked		
2.1	Hardware examination				
2.2	Software authorization, edition (including firmware) check				
2.3	Examination of spare parts, consumables and tools				
3	Examination of mechanical and electrical installation		Hardware structure and design are examined by referring to approval documents		
3.1	Cable entry method, bracket and attachment (cable fixing clamp and fixing head, etc.)				
3.2	Mark, label				
3.3	Installation of components and modules				

No.	Test item	Initial condition of device/system	Test method	Test result analysis and acceptance criteria	Test result requirements
3.4	Screw fastening connection and terminal connection				
3.5	Earthing and equal potential connection				
3.6	Protection against electric shock, warning mark				
3.7	Maintainability of cabinet fan and mechanism structure				
3.8	Spare capacity				
4	Wiring and terminal examination		Checking that wiring complies with guiding policy provided in engineering project rules, and approved hardware documents and technology comply with industrial standards		
4.1	Wiring, internal circuit wiring				
4.2	Fusing, circuit breaker				
4.3	Mark, label				
4.4	Division of cable, color, cross section, voltage and explosion-proof grade				
4.5	Cable bending examination				
4.6	Artificial cable bending and straining test				
4.7	Cable pipe load				
4.8	Wiring of I/O to terminal and connection mark				
4.9	System cable plug direction				
4.10	System voltage insulation testing				
5	Start testing and basic function of system		Survey system can start in normal condition, recover from		

No.	Test item	Initial condition of device/system	Test method	Test result analysis and acceptance criteria	Test result requirements
			power failure and upload on line. In addition, it is also to check whether the system is operated within given restriction scope.		
5.1	Restart		Using new memory card and removing spare battery of control		
5.2	Online change				
5.3	Control cycle time				
5.4	Display call time				
5.5	Numerical update time				
5.6	System load (memory capacity, storage capacity, etc.)				
5.7	Log-in policy and level				
5.8	Alarm processing policy and confirmation method				
6	System alarm testing		Report of alarm in survey system, including system-related failure, control tank alarm and system alarm		
6.1	Power failure, UPS monitoring				
6.2	Circuit breaker, fuse monitoring				
6.3	Cooling fan				
6.4	Communication, network monitoring				
6.5	Short circuit, disconnection, outrange, earthing failure				
6.6	Watchdog				
7	Hardware redundancy and diagnosis examination		Ensuring that redundant parts can operate and monitor in normal		

No.	Test item	Initial condition of device/system	Test method	Test result analysis and acceptance criteria	Test result requirements
			condition		
7.1	Redundant operation and monitoring of control				
7.2	Redundant operation and monitoring of communication and network				
7.3	Redundant operation and monitoring of power supply				
7.4	Redundant operation and monitoring of operator station				
7.5	Redundant operation and monitoring of I/O device				
7.6	Redundant operation and monitoring of all other devices not mentioned above				
8	Monitoring/operation		Verifying consistency of standard function and graphic display plan with specification		
8.1	Background color and color change				
8.2	Symbol				
8.3	Static text and dynamic change				
8.4	Picture organization (folding, conversion , subpicture)				
9	Function testing carried out according to function block diagram and function plan		Verifying consistency of system function with given document requirements		
9.1	Identification and labeling of loop/function				
9.2	Display of testing relevant I/O to picture				
9.3	Carrying out detailed function examination after putting all				

No.	Test item	Initial condition of device/system	Test method	Test result analysis and acceptance criteria	Test result requirements
	relevant interlock, alarm, message, display and trend and updating signals on graphic picture and device picture				
9.4	Bit number operation and trend collection function (internal and external)				
9.5	Priority processing of alarm				
10	Complicated function and operation mode		Checking consistency of system function with given document requirements		
10.1	Carrying out detailed function examination after putting all relevant interlock, alarm, message, display and trend and updating signals on graphic picture and device picture				
10.2	Whether the system has integrated data of intelligent systems, whether the system is open to realize ship monitoring and intelligent management as well as data exchange with shore base		Checking consistency of system function with the Guidelines		
10.3	System requirements				
10.3.1	The computer-based systems of the platform are to be categorized based on data usage, function, security risk level		Carrying out evaluation to the system according to Guidelines for Assessment of Security and Reliability of Marine Software		
10.3.2	Database of integration platform is to have valid integration process, i.e. screening necessary data according to data quality of				

No.	Test item	Initial condition of device/system	Test method	Test result analysis and acceptance criteria	Test result requirements
	each system and functional requirements for integration platform. The system supports multi-terminal (PC and mobile device) access. When necessary, the system is to provide external data transmission interface and have capability of sharing data with relevant parties				
10.4	The system is to meet the requirements for network security		Network security is to comply with the requirements of ISC Guidelines for Ship Cyber Security		
11	Sub-function integration testing		Verifying interoperability of each relevant system		
11.1	Carrying out detailed function examination after putting all relevant interlock, alarm, message, display and trend and updating signals on graphic picture and device picture				

Example of acceptance test

No.	Test items	Initial condition of device/system	Test method	Test result analysis and acceptance criteria	Test result requirements	Remarks
1	Examination of control system documents					
2	Examination of hardware specification and quantity					
3	Examination of software specification and quantity (correct software/firmware edition, etc.)					

4	Examination of mechanical and electrical installation					
4.1	Correct connection of earthing system					
4.2	Correct connection of power supply system					
4.3	Correct connection of network system					
5	Start/diagnosis examination					
5.1	Power on of relevant hardware					
5.2	Debugging/initializing relevant hardware and carrying out diagnosis examination					
6	Downloading software					

Example of integration test

No.	Test items	Initial condition of device/system	Test method	Test result analysis and acceptance criteria	Test result requirements	Remarks
1	Examination of control system documents					
2	Examination of mechanical and electrical installation					
3	Correct installation and connection among systems (serial port, Ethernet, optical fiber, etc.)					
3.1	Correct setting of communication baud rate (dial switch on the hardware, software setting, etc.)					
3.2	Verifying normal communication of system I/O signals among different systems					
4	Picture of subsystems in the system is set according to the requirements of the Rules					
4.1	Function is to comply with applicable contents of functional testing and failure testing in type approval					