GUIDANCE NOTES
GD24-2021

CHINA CLASSIFICATION SOCIETY

Guideline for Verification of Digital Systems of Ships and Offshore Installations

2021

Effective from 1 October 2021

Beijing

Contents

Chapter 1 General

Section 1 General Provisions

1.1.1 Scope

1.1.1.1 The guideline is applicable to the inspection and verification of the digital systems and data activities of ships and offshore units and their ancillary equipment.

1.1.1.2 Data identification, acquisition, integration, model and application are the core elements of the digitalization of ships and offshore units and their ancillary equipment. This guideline takes these core elements as the smallest unit to verify the requirements of technical standards, and takes the model as the object for verifying the application capabilities of the digital systems.

1.1.1.3 The guideline is used to verification and validation the technical standards requirements, functional integrity, model verifiability, software and hardware facilities reliability, network and data security, etc. of the digital systems from the aspects of data identification, acquisition, integration, model and application, etc.

1.1.1.4 The data in this guideline includes but is not limited to equipment data, structured data, status data, motion data, posture data, maintenance data, production data, personnel data, etc.

1.1.2 General requirements

1.1.2.1 The digital system in this guideline refers to the system that uses data to digitally represent specific physical entities and reflect the specific life cycle process of physical entities.

1.1.2.2 The digital system should label the data according to the requirements of Chapter 2 of this guideline, and it is recommended to carry out classified and hierarchical management according to Chapter 2 of the “Guidelines for Quality Assessment of Ship Data”.

1.1.2.3 The relevant hardware and software of the digital system involved in this guideline should meet the applicable requirements of Part 7, Chapter 2 and Section 6 of the *Rules for Classification of Sea-going Steel Ships* of China Classification Society (hereinafter referred to as “CCS”), and should pass the drawing review and inspection of CCS.

1.1.3 Certificate

1.1.3.1 The applicant applies for inspection and verification of the digital system of ships and offshore installations according to the technical provisions listed in this guideline. After qualified verification, CCS may issue relevant compliance certificates and/or reports, which are divided into two categories: type A and type B, among them:
(1) Type A certificate may be issued after the integrated operation requirements in Chapters 1-4 and 7 of this guideline are satisfied and the verification of application ability assessment of the digital system is qualified according to the requirements of Chapter 9;
(2) Type B certificate may be issued after the requirements in Chapters 1-4 and the integrated operation requirement of Chapter 7 of this guideline are satisfied and the inspection and verification are qualified.

1.1.3.2 The validity period of the certificate should generally not exceed 5 years.

1.1.3.3 The certificate of compliance should be invalidated, suspended and resumed according to the provisions of Part 1, Chapter 3 and Section 1 of the Rules for Classification of Sea-going Steel Ships of CCS.

1.1.4 Application and expenses

1.1.4.1 For ships and offshore installations applying for the certificate mentioned in 1.1.3, a written application should be submitted to CCS, and an evaluation service contract and/or agreement may be signed when necessary. For specific requirements, please refer to Part 1, Chapter 2 and Section 4 of the *Rules for Classification of Sea-going Steel Ships*.

1.1.5 Normative references

1.1.5.1 The clauses in relevant documents will become the clauses of this guideline after being taken as a reference by this guideline. For undated references, the latest edition of the referenced document applies to this guideline.

1.1.6 Terms

1.1.6.1 Unless expressly provided otherwise, for the purpose of the guideline:
(1) Physical entity: refers to the physical equipment and systems;
(2) Model: A formal representation after the physical entity is abstracted in digital space;
(3) Confidence: the probability that the overall parameter value falls within a certain interval of the sample statistical value;
(4) Confidence interval: the error range between the sample statistical value and the overall parameter value under a certain confidence level;
(5) Data-driven model: a model generated by applying an appropriate training algorithm to the data set.

1.1.7 Data provision and confidentiality

1.1.7.1 CCS shall comply with the information disclosure requirements of paragraph 2.12.2, Section 12, Chapter 2, Part 1 of the *Rules for Classification of Sea-going Steel Ships* with respect to the data and information submitted by the applicant.

1.1.8 Exemption clause

1.1.8.1 The digital technology is constantly evolving. This guideline aims to adapt and promote the application of digital technology on ships and offshore installations. however, the contents of this guideline cannot replace the analysis and/or recommendations of qualified professionals on the application of digital systems. It is the user's responsibility to evaluate and obtain professional advice on their own.

1.1.8.2 Some information contained in this guideline may become invalid due to changes in laws, regulations, standards, methods, etc., and users are fully responsible for the compliance.

1.1.9 Personnel requirements

1.1.9.1 The shipowners and ship management companies should develop the management methods, training plans, operating procedures, etc. related to the digital system to clarify the responsibilities,

qualifications, training and other requirements of relevant operators and users of the digital system.

1.1.9.2 Relevant personnel should be trained and qualified before taking the job, and be familiar with the operation of the digital system.

1.1.10 Change management

1.1.10.1 For the digital systems that have been inspected and verified by CCS, inspections shall be carried out according to the specific conditions after the equipment and systems related to the digital system are changed or repaired to confirm that they meet the relevant technical requirements.

Section 2 System Reliability

1.2.1 Hardware reliability

1.2.1.1 Factors to be considered for the hardware reliability of the system:

(1) Service conditions;

(2) Performance parameters and allowable limits;

(3) Redundancy design (such as bypass, etc.);

(4) Common cause failure, i.e., system failure due to a common cause;

(5) Associated failure, i.e., the failures of each unit are often related, once one component is damaged, the other component will bear the consequences of the damaged component.

1.2.2 Software reliability

1.2.2.1 Software reliability evaluation indicators

(1) Maturity, which measures the software reliability, and such indicators as failure, fault, test and validity are mainly considered, among them:

① Failure refers to the degree to measurement software failure and resolution, which mainly includes such indicators as failure density and failure resolution rate;

② Fault refers to the degree to measure, detect and eliminate the software fault, which mainly includes such indicators as fault density, potential fault rate, and troubleshooting rate;

③ Testability refers to the degree to measure software testing, which mainly includes such indicators as test coverage and test pass rate;

④ Validity refers to the degree to measure effective operation of the software, which mainly includes such indicators as mean time between failures, effective service time rate and cumulative effective service time.

(2) Fault tolerance, which mainly involves such indicators as normal operation and resistance to maloperation rate, among them:

①Normal operation refers to the degree to measure the efforts made by the software to maintain normal operation, which mainly includes such indicators as downtime avoidance rate and failure avoidance rate;

② Resistance to maloperation rate refers to the degree to measure the efforts made by the software to avoid maloperation .

(3) Recoverability

①Restart success refers to the degree to measure the extent to which the software can be reused after downtime, which mainly includes such indicators as average downtime and average

recovery time;

② Repair success refers to the degree to measure the extent to which the software can be repaired after an abnormal condition occurs, which mainly includes such indicators as repairability and repair effectiveness.

1.2.2.2 The software reliability test process is shown in Figure 1.2.2.2.

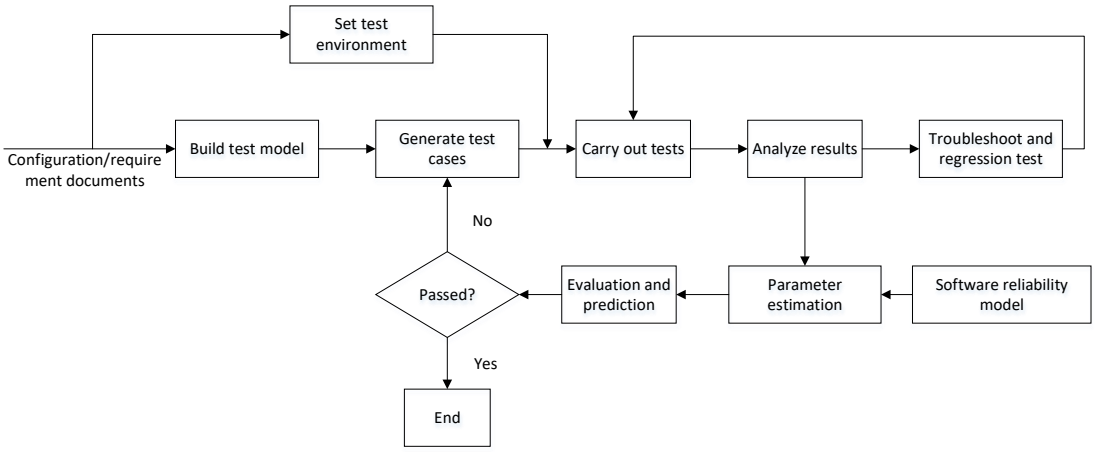

Figure 1.2.2.2 Software reliability test process

1.2.3 Network connection reliability

1.2.3.1 The network connection should meet the relevant requirements of Chapter 3 of CCS "Guidelines for Requirement and Security Assessment of Ship Cyber System".

1.2.3.2 The following factors need to be considered with respect to the connectivity of wired links:
(1) Network node hardware reliability;
(2) Accessibility of network topology;
(3) Logical connection of the network.

1.2.3.3 The following factors need to be considered with respect to the connectivity of wireless links:
(1) Node equipment reliability;
(2) The signal-to-noise ratio should meet the requirements of the receiver if the wireless links failed due to signal attenuation;
(3) The rated value (i.e., the bit error rate caused by a given co-channel interference type multi-path attenuation) or the received signal power is lower than the minimum required by the receiver because the ratio of multi-path transmission channel signal to interference and noise drops below the rated value.

Section 4 Cyber Security

1.4.1 General requirements

1.4.1.1 The digital system should meet the requirements of Chapter 4 of CCS "Guidelines for Requirement and Security Assessment of Ship Cyber System".

1.4.1.2 Data security should meet the relevant requirements in Chapter 3 of CCS "Guidelines for Requirement and Security Assessment of Ship Cyber System" Appendix 8 of CCS "Guidelines for Quality Assessment of Ship Data".

1.4.1.3 Data export should meet the relevant laws and regulations of the flag country, the country of entry and the country of departure.

1.4.1.4 The storage and transmission of digital systems should meet the relevant requirements of Chapter 3 of this guideline.

1.4.1.5 The network used to connect the digital systems and the physical entities should have timely, accurate and complete transmission capabilities to meet business needs.

Section 5 Data Quality

1.5.1 General requirements

1.5.1.1 Data quality refers to the extent to which the characteristics of data meet explicit and implicit requirements when being used under specified conditions.

1.5.1.2 Generally, some planning, execution and control activities (such as some quality management tools and/or techniques) can be adopted to ensure that the data meets the use requirements.

1.5.1.3 Data quality depends on the application scenario and the requirements of data users.

1.5.2 Data quality requirements

1.5.2.1 Data quality requirements include two aspects:
(1) Data attributes;
(2) Data activity.

1.5.2.2 The definition, requirements and assessment of data attributes should meet the requirements of Chapter 3 of CCS “Guidelines for Quality Assessment of Ship Data”.

1.5.2.3 Different data activities have different requirements for data quality. Data activities include but are not limited to the followings:
(1) Data identification
① For relevant requirements of data identification, please refer to Chapter 2 of this guideline;
② Data identification is required to easily identify the data and pay attention to the quality characteristics such as comprehensibility and traceability of data;
③ Different digital systems should meet the uniqueness requirements of data identification in the event of output or forward of general data of ships and offshore installations, such as position, heading, etc.
(2) Data collection
① Requirements of data collection refers to Chapter 3 of this guideline;
② Collection activities focus on the reception, analysis and transmission of data, and pay attention to the characteristics of data compliance, currentness, and confidentiality;
③ Data collection activities have different requirements for data quality with different application scenarios.
(3) Data storage
① Requirements of data storage refers to Chapter 3 of this guideline;
② Data storage focuses on the quality characteristics of data currentness, accuracy, portability, and recoverability;
③ Data cleaning focuses on the quality characteristics of data accuracy, compliance, timeliness, efficiency;
④ The requirements of data storage for data quality must meet the product

specification/standards and CCS inspection requirements.

(4) Data integration

① Requirements of data integration refer to Chapter 4 of this guideline;

② Data integration focuses on the quality characteristics of data accuracy, completeness, consistency and currentness;

③ Data integration should meet the needs of actual application scenarios. If necessary, a description document of data integration should be provided to CCS.

(5) Data application

① For relevant requirements of data application, please refer to Chapters 6 and 7 of this guideline;

② Data application focuses on the characteristics of data confidence level, sampling frequency, data security, etc.

(6) Data verification

① Requirements of data verification refers to Chapters 8 and 9 of this guideline;

② The data used for verification should meet the characteristics of non-tampering, easy to read, easy to operate, store, etc. to meet the relevant CCS acceptance criteria for verification.

Chapter 2 Data Identification

Section 1 General Provisions

2.1.1 Purpose

2.1.1.1 Data identification is to identify and distinguish different physical entities and virtual objects, ensure the consistency and interoperability of related data at the label semantic level, and identify the entity or object itself and its attribute data.

2.1.1.2 Identification coding is the process of assigning specific codes to the identification objects.

2.1.2 Identification objects

2.1.2.1 Physical entities, including but not limited to hull structure, mechanical equipment, electrical equipment, communication and navigation equipment, cargo, course, environment, personnel, etc.

2.1.2.2 Virtual objects, including but not limited to processes, category, scenarios, status, events, services, management, functions, etc.

2.1.3 Application scenario

2.1.3.1 Closed-loop application: data identification is only used inside the system.

2.1.3.2 Open-loop application: data identification is used inside and outside the system, and there is the scenario where data exchange exists between systems, devices, and products.

Section 2 System Requirements

2.2.1 Data identification principle

2.2.1.1 Data identification should follow the relevant principles listed in Table 2.2.1.1.

Data Identification Principle **Table 2.2.1.1**

No.	Basic Principle	Description
1	Atomicity	The smallest unit of the identification objects can be identified.
2	Uniqueness	There is a strict one-to-one correspondence between the identification code and its object.
3	Scientific rationality	The stable essential attributes or characteristics of the identification object should serve as the basis for classification.
4	Extendibility	It is to accept the new identification objects that may appear without changing the original architecture, and meanwhile have a certain expansion capacity.
5	Controllability	A controllable and determined management method should be available.
6	Openness	The interconnection of internal and external data should be considered.
7	Compatibility	Coordination is required when it comes to different coding standards.
8	Comprehensiveness	All kinds of objects should be covered.
9	Operability	It is to consider the needs of rapid identification, analysis and

		information acquisition, as well as the needs of man-machine reading, initial initialization, and later operation and maintenance.
10	Normativity	In the same coding standard, the type, structure and writing format of the code should be uniform.

2.2.2 Data identification coding method

2.2.2.1 The coding method of data identification should be based on the predetermined application requirements and the nature of the coding object, and appropriate code structure should be selected. Sequence code, abbreviation code, layer code or combination code can be used;

(1) Sequence code: it is to identify the code of the coded objects by the sequence of Arabic numerals or English letters, coding can be made according to the sequence of time, spatial arrangement, name character sequence, serial number, etc.;

(2) Abbreviation code: it is to abbreviate the name of the coded objects according to a unified method, and it is a code generated from one or more characters in the name of the coded objects;

(3) Layer code: it is to divide the coded objects into continuous and increasing groups (classes) based on the hierarchical classification in the set of coded objects, and coding can be made according to the hierarchical relation of systems, equipment, components, parts, etc.;

(4) Combination code: it is to use a combination of two or three of the sequence code, abbreviation code and layer code, as shown in Table 2.2.2.1(4).

Example of Combination Code **Table 2.2.2.1(4)**

Identification code	http://data.shipdatacenter.cn/imo1234567/ccs_cls/MainEngine/Cylinder1/ExhaustGas/Outlet/Temp
Named entity	data.shipdatacenter.cn
Identification number	imo1234567
Naming rule	ccs_cls
Local identification	MainEngine/Cylinder1/ExhaustGas/Outlet/Temp

2.2.3 Data identification code standard

2.2.3.1 Data identification coding can be subject to the proprietary standards and general standards, as follows:

(1) Proprietary standards: the identification coding system structure customized based on specific needs, which should meet the requirements of paragraphs 2.2.1 and 2.2.2;

(2) General standards: ISO, IEC standards or equivalent general standards.

2.2.3.2 The data identification coding standards should at least include the scope of application, coding method, coding structure (including code composition and representation) and coding rules.

2.2.4 Data identification code management

2.2.4.1 Each assigned identification code should be registered in an appropriate manner to ensure no re-issuance.

2.2.4.2 For the identification codes that are transmitted multiple times between media, the integrity of the code should be verified through a format check or check code.

2.2.4.3 The identification code can only be registered, changed and deleted by the authorized party or the related party approved by CCS. Meanwhile, the registration, change or deletion of the codes

should be recorded and the code table should be updated in a timely manner.

Section 3 Verification Requirements

2.3.1 Verification method

2.3.1.1 The verification method is divided into document review, test and verification. The specific requirements are shown in Table 2.3.1.1.

Verification Requirements **Table 2.3.1.1**

Scope of Use	Closed-loop Application	Open-loop Application
Proprietary standards	Document review: Identification code scheme Code table	Document review: Identification code scheme Code table Heterogeneous standards coordination plan (if applicable) Coding rules and coding structure metadata
	Test and verification: Document conformance test (spot check of 10%) Identity resolution test	Test and verification: Document conformance test (spot check of 20%) Identity resolution test Heterogeneous standards conversion test (if applicable)
General standards	Document review: Code table	Document review: Code table Heterogeneous standards coordination plan (if applicable)
	Test and verification: Document conformance test (spot check of 5%) Identity resolution test	Test and verification: Document conformance test (spot check of 10%) Identity resolution test Heterogeneous standards conversion test (if applicable)

2.3.1.2 Conformance spot check test requirements, it is considered that the test is passed when above 90% of the spot check items are qualified; when the spot check items of 70%-90% are qualified, the second spot check shall be carried out according to Table 2.3.1.1; The test is passed when above 90% of the second spot check items are qualified; it is failed under other conditions.

2.3.2 Documents

2.3.2.1 Corresponding documents should be submitted according to the requirements of Table 2.3.1.1:

(1) Identification code scheme: including but not limited to the coding standards adopted, identification scope and code management;

(2) Code table: including all identification code object sets and code element sets and their corresponding relations;

(3) Heterogeneous standards coordination scheme: including but not limited to the standards and compatibility/conversion schemes involved;

(4) Coding structure metadata: data that defines and interprets the coding structure;

(5) Coding rule metadata: data that defines and interprets the coding rules.

Chapter 3 Data Collection

Section 1 General Provisions

3.1.1 Scope of application

3.1.1.1 The data collection of ships and offshore installations refers to the process of acquiring data through collection of sensor and other equipment, system generation and knowledge entry, etc., and transmitting and storing them in the data server of ships and offshore installations (hereinafter referred to as "shipboard data server") or remote data server.
(1) Sensor collection, which includes data generated during the operation of various systems of ships and offshore installations through temperature sensors, pressure sensor, camera, global navigation satellite system, radar, and other sensor equipments;
(2) System generation, which includes business data collected and generated during the operation of other systems of ships and offshore installations as well as the operation and maintenance and log data generated during the operation of various systems, programs, and services, etc.;
(3) Knowledge entry, which includes email subscription, expert knowledge entry data, systematic reasoning data, as well as migration data of other ships and offshore installations or systems, etc.

3.1.2 General requirements

3.1.2.1 It is required to define aliases for data sources, and mark the basic attributes, locations, use range of all installations or systems, as well as the information correlation model between equipment, etc.

3.1.2.2 The data collection infrastructure should meet the use of data volume of the digital system.

3.1.2.3 Data collection should ensure the availability, integrity, and confidentiality of data.

3.1.2.4 If the data is filtered and compressed, the description of the compression algorithm and the description of the node location for compression execution should be provided.

3.1.2.5 It is required to mark the data according to the data quality status coding rules and transmit them to the data server of ships and offshore installations. The mark should at least indicate the validity status of the data.

3.1.2.6 The internal status error of data collection should not affect the normal operation of the data source.

3.1.2.7 The data collection infrastructure and systems should have access control.

3.1.2.8 The data server and relay components should be directly powered by the uninterrupted power supply of the ships and offshore installations.

3.1.2.9 During data collection, it is important to carry out consistency check, delete the duplicate data and correct the errors, and initially supplement the data.

3.1.2.10 Quality assessment of the collected data should be carried out on a regular basis.

3.1.2.11 In the case of consistency check of the data, the following conditions should at least be dealt with:

(1) Null value;

(2) Data length;

(3) Data type;

(4) Incomplete data;

(5) Duplicate data.

3.1.2.12 The data security of data collection shall meet the requirements of Appendix 8 of CCS "Guidelines for Quality Assessment of Ship Data", and the data security of data storage shall meet the requirements of Section 3.5 of CCS "Guidelines for Requirement and Security Assessment of Ship Cyber System".

Section 2 Collection Architecture

3.2.1 Data collection architecture

3.2.1.1 The data collection architecture refers to the deployment methods used to complete data collection to storage through data source, sensor and other equipment, shipboard data server, data relay components, and remote data server, where:

(1) Data relay components refer to such devices as switch, gateway, firewall, router, wireless transmitter and receiver in the data transmission path from the data source to the shipboard data server, and from the shipboard data server to the remote data server;

(2) The shipboard data server can be used as the data source for other data collection architectures;

(3) The data flow in the collection architecture generally flows from the data source to the shipboard or remote data server through the data acquisition equipment and data relay components.

3.2.1.2 The diagram of the data collection architecture is shown in Figure 3.2.1.2. The figure only indicates the data flow direction, and should not be used as a network topology requirement for data collection. Data can be connected to the data server through the three methods shown in the figure:

(1) Direct transmission to the remote data server through the network security equipment;

(2) Direct transmission to the shipboard data server;

(3) Transmission to the shipboard data server through relay devices such as router/switch.

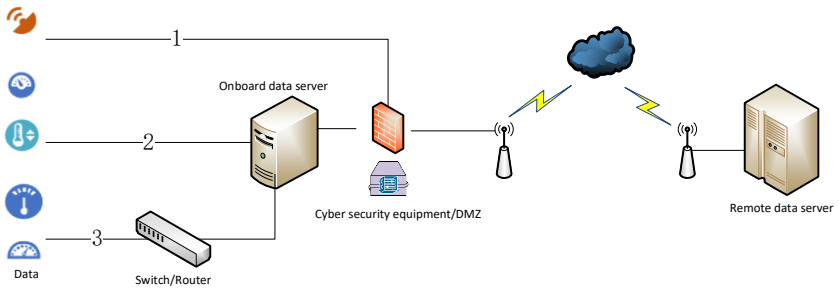

Figure 3.2.1.2 Example of Collection Architecture

3.2.1.3 The data collection architecture can be deployed based on proprietary solutions and/or general solutions. Proprietary solutions refer to the system that adopts proprietary data storage, collection and transmission protocols according to specific data collection requirements; General solutions refer to the system that adopts standardized storage, collection and transmission protocols.

3.2.1.4 The data collection system should monitor the availability and fault diagnosis information

of each module or component in the collection architecture.

3.2.2 Data collection infrastructure

3.2.2.1The data collection infrastructure involves the components of the collection, transmission and storage process, including:
(1) Shipboard data server;
(2) Data relay components, which mainly include data transmission equipment, network security equipment, etc.;
(3) Remote data server.

3.2.2.2 Shipboard data server
(1) Data can be obtained and sent to the remote data server, other shipboard data servers, or systems installed on the ships and offshore installations (hereinafter referred to as “shipboard systems”) through the data relay components;
(2) The capacity of the shipboard data server should meet the business needs;
(3) The shipboard data server should support the interface protocol used by the collection equipment;
(4) The shipboard data server should meet the relevant requirements of shipboard data server of ISO 19847.

3.2.2.3 Data relay components
(1) It should provide stable data transmission function;
(2) The bandwidth should meet the expected data throughput requirements to support peak data transmission;
(3) When the data user and the shipboard data server are not in the same controlled network, the data forwarded through the data relay components should be encrypted.

3.2.2.4 Remote data server
(1) It should be able to receive data from multiple shipboard data servers, and each data source and shipboard data server should have a unique ID;
(2) The remote data server may also be responsible for providing remote data to users. The data center or other shipboard systems can also be regarded as the data recipient;
(3) Sufficient storage capacity should be provided to meet the data storage and backup requirements of the connected shipboard data server;
(4) Cache data recovery mechanism should be available to avoid data loss;
(5) The remote data server should support the protocol used by the connected shipboard data server and meet the relevant requirements of Data server of ISO 19847.

3.2.2.4 The data collection infrastructure should provide a timestamp including Coordinated Universal Time (UTC) and time zone at the time of data collection.

3.2.2.5 When the shipboard system is used as a data server, it should meet the relevant requirements of the shipboard data server in 3.2.2.2 of this Chapter.

3.2.2.6 The data source involved in edge computing should have certain data storage capabilities on the computing side to meet necessary data replay requirements.

3.2.3 Data interface protocol requirements

3.2.3.1 The standard interface protocol or special interface protocol should be determined for the remote data server, shipboard data server, mechanical equipment and systems (including hull, safety equipment and systems).

3.2.3.2 Detailed documentation should be provided for the data input/output interface of the remote data server, shipboard data server, mechanical equipment and systems.

3.2.3.3 The data interface protocol of the navigation and communication system should meet the technical requirements of IEC 61162-1.

3.2.4 Data transmission protocol requirements

3.2.4.1 Data transmission between the shipboard data server and the shipboard equipment and between the shipboard equipment that adopts the standard data transmission protocol should meet the following requirements:

(1) Fieldbus transmission should follow the relevant requirements of IEC 61158 and IEC 61784;

(2) The industrial data transmission protocol should support standard protocols such as OPC UA/DA;

(3) Ethernet transmission should follow the communication standard protocols such as TCP/IP protocol.

3.2.4.2 Protocol documentation should be provided for data transmission between the data server and the onboard equipment and between the onboard equipment that adopts the dedicated data transmission protocol.

3.2.4.3 The data transmission protocol of the navigation and communication system of ships and offshore installations should meet the following requirements:

(1) The serial port transmission protocol should comply with IEC 61162-1 and IEC 61162-2;

(2) The network transmission protocol should comply with IEC 61162-450.

3.2.4.4 The data transmitted via Ethernet should follow relevant standard protocols and be provided with documentation or configuration files.

3.2.5 Data exchange format

3.2.5.1 The type, content, structure, and other attributes of data can be described in XML, JSON, CSV, string, etc.

3.2.6 Communication requirements

3.2.6.1 Data communication should meet the business needs and expected goals, and such factors as transmission rate, signal attenuation, and interference should be considered especially when the digital systems and the physical entities are deployed in different locations or across network segments.

3.2.6.2 The communication of the collection architecture includes wired communication and wireless communication, among which wireless communication includes local wireless communication and remote wireless communication.

3.2.6.3 The encryption strategy of corresponding strength should be adopted according to the impact of the communication contents on security, and meanwhile the communication delay caused by the encryption and decryption process should be considered.

3.2.6.4 Data transmission should be verified.

3.2.6.5 The multi-input and multi-output communication links should be able to identify multiple sources and sinks, and monitor the use status of the channel, as well as the status of the source and sink, such as whether it is online, etc.

3.2.6.6 The communication link for which multiple devices work together should have a clock synchronization mechanism and meet the following requirements:

(1) It should support at least one clock synchronization protocol to realize the synchronization of the internal time reference with the clock information of the clock synchronization equipment or terminal equipment at all levels; the Network Time Protocol (NTP)/Simple Network Time Protocol (SNTP) can be used when the clock error range is required to be millisecond class, and the Precision Time Synchronization Protocol (PTP) or IRIG-B time code can be used when the error range is required to be microsecond class;

(2) It should support the output of the required time synchronization signal when required by the terminal equipment, which includes pulse signal, IRIG-B time code and other coded signals, serial port time message and network time message.

3.2.6.7 When transmitting large volume of data (such as AIS data, audio, and video data, etc.), appropriate coding techniques can be used for compression according to the business needs to save

3.2.6.8 The ships and offshore installations as well as telecommunication system should be provided with sufficient bandwidth and transmission rate according to the business requirements of the system. The bandwidth should be designed based on system requirements, buffer size and data recovery requirements. If the bandwidth is shared, any other communications that may need to use the bandwidth should also include in the calculation. Bandwidth calculation should be continuously updated based on the addition or deletion of the actual equipment or systems.

3.2.6.9 The communication link should be provided with communication management and monitoring, including the followings:

(1) Priority should be considered in communication, and communication security can be divided into 3 levels based on the impact and urgency of communication contents on personal safety, safety of ships and offshore installations, and environmental safety, as shown in Table 3.2.6.9;

(2) It is required to provide the application programmers interface (API) for system status, alarms, and performance logs (TX/RX data rate and data transmission delay).

Communication Security Classification **Table 3.2.6.9**

Level	Impact	Typical Data
1	Immediately affect personal safety, safety of ships and offshore installations, and environmental safety	Emergency control instructions, remote control instructions
2	Eventually affect personal safety, safety of ships and offshore installations, and environmental safety	Status perception data, alarm, and monitoring information, etc. of ships and offshore installations
3	Not affect personal safety, safety of ships and offshore installations, and environmental safety	Information monitoring data, maintenance data, etc.

3.2.6.10 The communication link of the control equipment should be separated from other links.

3.2.6.11 For the communication links of data at levels 1 and 2 in Table 3.2.6.9, redundancy design

may be considered from the perspective of reliability, and it should be tested whether it meets the business requirements.

3.2.6.12 The communication link should have a recovery mechanism, which should be used to re-establish the communication link after it is disconnected and identify the transmitted data and the data to be transmitted.

3.2.6.13 The recovery time of the communication link for the local real-time control of ships and offshore installations, and the communication link for the data collection and monitoring system data should be less than the time required by the system.

3.2.6.14 The data transmission delay should meet the requirements of the application scenario, and the data transmission delay from the data source to the sink should be tested and explained.

3.2.6.15 For the communication link of the local control system, the transmission delay from the control end command to the execution end should generally not exceed 0.5s.

3.2.6.16 The local wireless communication link deployment and technical specifications of ships and offshore installations should indicate the standards that they followed.

3.2.6.17 The local wireless communication links between ships and offshore installations should be as follows:

(1) For the communication link with a communication security level of 1, wireless communication should not be adopted, except for special considerations by CCS, please refer to the relevant contents of paragraph 2.6.6.2, Section 6, Chapter 2, Part 7 of CCS “Rules for Classification of Sea-Going Steel Ships” for the consideration factors;

(2) Appropriate wireless communication standards should be selected according to the business scenario requirements, the type of communication signal (switching value, analog quantity, etc.), communication interface (RS485, etc.), etc.;

(3) It is required to select an appropriate communication network topology and explain the maximum number of field devices supported by the topology network according to the location and number of collection nodes;

(4) It is required to evaluate and test the impact of field obstacles on the communication links;

(5) It is required to indicate the transmission distance and transmission rate of the communication link in the presence and absence of obstacles;

(6) It is required to indicate the refresh rate of wireless field devices and consider the impact of refresh rate on the number of supported devices;

(7) It is required to evaluate and test the impact of outdoor site wind speed and other environmental factors on the communication link.

3.2.6.18 The wireless communication link should also meet the security requirements of the wireless network in the CCS “Guidelines for Requirement and Security Assessment of Ship Cyber System”.

3.2.6.19 In addition to meeting the requirements of Section 2, Chapter 1, Part 4 of CCS “Rules for Classification of Sea-going Steel Ships”, the installation and service environment requirements of the communication equipment should also be considered with respect to the communication hardware equipment.

3.2.6.20 Auxiliary electrical equipment such as communication cables should meet the requirements of Section 5, Chapter 3, Part 4 of CCS “Rules for Classification of Sea-going Steel Ships”, and

should also meet the requirements of navigation and communication systems for cables.

3.2.6.21 The equipment and cables should have necessary electromagnetic compatibility and electrostatic protection characteristics.

3.2.6.22 Signal interference should be considered for the communication network cables, if necessary, isolated communication should be adopted to reduce or avoid the signal interference.

Section 3 Data Storage Requirements

3.3.1 Technical requirements

3.3.1.1 The data storage facilities should meet the expected data processing and storage requirements of the business.

3.3.1.2 It is required to develop the data backup strategy and recovery strategy, backup procedures and backup plans, and carry out data recovery test based on the backup results to ensure that the backup data can work normally.

3.3.1.3 Data backup and recovery test should be arranged regularly.

Section 4 Verification Requirements

3.4.1 Documents

3.4.1.1 In the event of applying for data collection, inspection, verification and assessment, the materials listed in Table 3.4.1.1 shall be submitted to CCS for future reference.

Documents **Table 3.4.1.1**

Item	File Type	Details
Data collection infrastructure	Test program file	Test documents related to the function and safety of the product or system.
	System topology diagram	Description of the relationship, interface specification, physical location (if applicable) of the source system, relay components, data server, and digital system, etc.
	Function description	Description of the function, performance and working environment of the facility, such as the maximum number of devices that can be connected, device identification, etc.
	Data format	Including all data interface protocols, transmission protocols, data storage and conversion formats, and data encryption and decryption instructions.
	Power supply system description	Main power line and specifications, battery specifications.
	Software change management file	-
	Equipment list	List of components included in the data collection architecture.
	List of control points or monitoring points	Mark all data input and output points.
	Installation and operation manual	Documents to guide equipment installation and operation.

	Documents of compliance	Product certificate or type approval certificate.
	Data storage capacity estimation book	Estimate the data storage capacity based on the data collection frequency and applicable business requirements.
	Data collection protocol specification	Including data collection interface protocol, transmission protocol and exchange format description, as well as detailed description of the proprietary protocol.
	Data backup and recovery strategy specification	-

3.4.2 Verification and test

3.4.2.1 The verification and test of the data collection infrastructure shall include but not limited to:

(1) The integrity of data collection should be verified based on the system requirements;

(2) Test the function and security according to the approved test plan, and see Sections 1 and 2 of this Chapter for the requirements;

(3) Verify whether the connected source system and data collection infrastructure can receive and transmit data according to the established protocol;

(4) For the documents to be submitted on board, please refer to the requirements of 3.4.1.

3.4.2.2 Data storage verification

(1) Check whether a backup and recovery exercise plan is established and whether the backup and recovery task is executed according to the plan;

(2) Check the change records of the digital system, and check the update status of the missing measure rate and the importance assessment if necessary.

Chapter 4 Data Integration

Section 1 General Provisions

4.1.1 Scope of application

4.1.1.1 The technical requirements for data integration of the digital system is prescribed in this chapter, including the technical requirements for such processing processes as calibration, sharing, fusion, and distribution.

4.1.2 General requirements

4.1.2.1 Data integration is used to form a unified data sharing and analysis mechanism for ships and offshore installations. And it also can be used to provide a unified data management system and technical standards for different data providers and users, and promote the interconnection and intercommunication of data.

4.1.2.2 Data integration is divided into two levels, among which:
(1) Physical data integration stores data centrally;
(2) Virtual data integration or distributed data storage uses virtual views and other methods to achieve data integration.

4.1.2.3 The basic functions of data integration include data calibration, data sharing and data dissemination. In addition to the basic functions, data fusion can also be provided.

4.1.2.4 Data quality assessment should be evaluated on a regular basis to confirm that it meets the business system requirements.

4.1.2.5 Data storage should meet the relevant requirements of “Section 3 Data Storage Requirements”.

4.1.2.6 The data integration activity should ensure the confidentiality, integrity and availability of data.

Section 2 System Requirements

4.2.1 Data integration

4.2.1.1 The data integration process can follow the process shown in Figure 4.2.1.1.

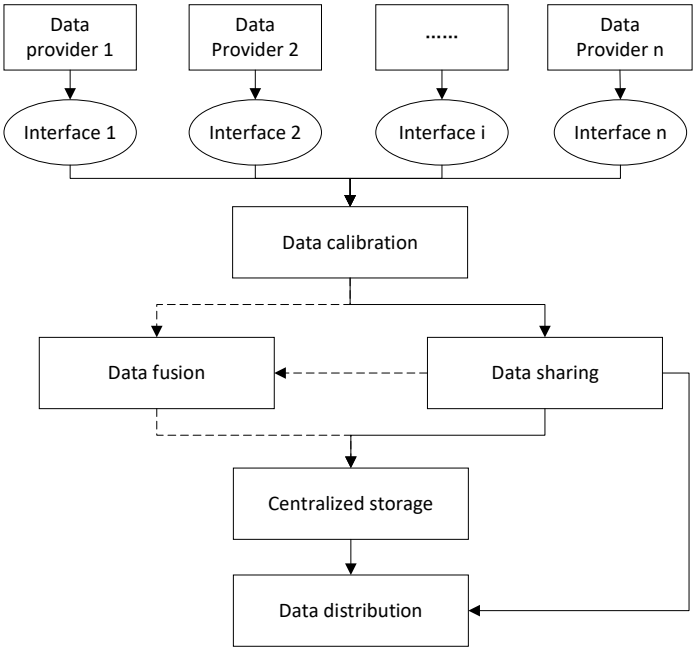

Figure 4.2.1.1 Data Integration Process

4.2.1.2 The digital system should provide data interface to different data providers, and should have the data interface management function. The data interface list should be managed in the server, and the list should be registered, modified, deleted and referenced through the data input and output functions.

4.2.2 Data calibration

4.2.2.1 The process of data processing and fusion s focused on the data. Before data fusion, the system should judge the quality of the data to ensure that the fusion results are reliable, certain and authentic.

4.2.2.2 Data calibration should meet the following requirements:

(1) The data provision system shall be responsible for the reliability, authenticity, certainty, completeness, correctness and timeliness of the data;

(2) Different data interfaces should be provided for the different data provider systems to complete the transmission from data providers to centralized data calibration processing services. Different data interfaces should include the data providers, data items, collection values, and measurement units;

(3) The unified measurement unit should be provided for different data items according to the model, and perform measurement unit conversion for the data items provided by different data providers before data processing;

(4) Time calibration and spatial calibration should be performed on the data from different sources, and the data values at the same time and space should be obtained for the same measurement object;

①To ensure the validity of time calibration, the calibration data server should provide time services, and the data server system clock should be synchronized with UTC;

②When the UTC synchronization of the ship-side data server fails, the system should give an alarm in a timely manner, and record the synchronization failure time.

(5) The system can automatically judge based on data from multiple sources, find and record the data with quality;

(6) If the quality of data and data sources is poor, the system should avoid them from getting

involved in data sharing and fusion by re-collection, discarding, etc., and record the processing results of the problematic data.

4.2.3 Data sharing

4.2.3.1 Data sharing is to provide access to multiple sinks, which should have the following functions:
(1) A data sharing directory should be provided. The directory should be constructed with reference to the data model to provide the information resource pointing functions. The information in the shared directory should include the name of the data set, the attribute name contained, whether the attribute is non-empty, the attribute type and description;
(2) A description document should be provided to explain the source of data, calling method, storage method, data type, etc.;

①For a single data storage method, the physical data warehouse and data virtual view are included;

②The data calling method includes direct reading, data interface, etc.

(3) It can query and update data sources of different organization types, including but not limited to structured database, structured data, semi-structured data and files, etc.;
(4) The system should be provided with both online and offline data dissemination functions, and support multithread processing.

4.2.3.2 The data format of data sharing input and output shall meet the requirements of Section 3.2.3 Data interface protocol of this guideline.
(1) Data sharing should have a cache data recovery mechanism to avoid data loss;
(2) The remote data server shall support the protocol used by the connected onboard data server and meet the relevant requirements of data server in ISO 19847.

4.2.3.3 The data collection infrastructure shall provide time stamps including Coordinated Universal Time (UTC) and time zones at the time of data collection.

4.2.3.4 When the ship system is used as a data server, it shall meet the relevant requirements of the ship data server in the 3.2.2.1 of this chapter.

4.2.3.5 The data sources participating in edge computing should have a certain data storage capacity at the computing end and be able to meet the necessary data backtracking requirements.

4.2.3.6 Data interface protocol requirements.

4.2.4 Data fusion requirements

4.2.4.1 Data fusion is to provide a reliable, accurate and complete description of the measured objects on the digital system. It is to analyze and process the measurement information from multiple sensors through data fusion to obtain data description of the measured objects.

4.2.4.2 The following requirements should be satisfied during the data fusion process:
(1) The input of data fusion is multi-source data from different sensors, and one or more imperfect data sources can be used to improve the data;

(2) The data fusion algorithms should take into account the completeness, correctness and timeliness of data;
(3) The data fusion system is responsible for the fused data quality;
(4) The data fusion system stores the data separately after fusion, and can distinguish the data before and after the fusion through identification;
(5) The data storage carrier shall meet the relevant requirements for data servers in Section 3.2.2 of this guideline;
(6) The system resources should be configured and managed according to current network status, system load conditions, etc.;
(7) The system should record the data fusion process log and keep it for more than 12 months, which shall include but not limited to the fusion algorithm name, fusion timestamp, and data source name.

4.2.4.3 The quality verification report should be provided for the data fusion system, and the scope of verification should cover all data types (such as digit, images, etc.) involved in the system, and the report should include:
(1) Data fusion purpose;
(2) Principle description of data fusion algorithm;
(3) Application scope of data fusion system;
(4) The local quality indicators of different types of data and the quality transfer function used to describe the relationship between the output quality, input information and quality of each data processing module;
(5) The description of the test data set of different types of data, including the data volume of the test data set, the quality indicators of different data sets, the input data and its quality description, and the actual data description corresponding to the input;
(6) Comparative analysis of the data and actual data before and after fusion;
(7) In the case of verifying the effectiveness of the fusion, the application of data after fusion should be considered, and the fusion time should meet the time requirements of the application system.

4.2.4.4 The data fusion system can verify the fusion results.

4.2.5 Data dissemination requirements

4.2.5.1 The data dissemination service is used for the discovery, extraction and transmission of data. The format and interface of data dissemination service should be unified and published within the scope of the ships and offshore installations. The data dissemination service or interface list should be provided during the review. The specific information includes but are not limited to the service or interface ID, name, specific data item name, data type, length, description, etc.

4.2.5.2 The data dissemination service should be able to adapt to the requirements of the physical data warehouse, data virtual views, hybrid data storage, etc.
Section 3 Verification Requirements

4.3.1 Documents

4.3.1.1 The data security strategy includes but is not limited to:

(1) Data integration scope: it specifies the data provider that can modify the data and the data dissemination object;
(2) Data security strategy: it develops appropriate strategies to ensure the authenticity, integrity and reliability of data;
(3) Risk assessment report: the ways, consequences and countermeasures of data loss or damage.

4.3.1.2 Data sharing description should include the relationship between different data sources and data models.

4.3.1.3 The data interface list should include the data list identification, name, purpose, and corresponding information system.

4.3.1.4 The data source list may include the identification, name, type, etc.

4.3.1.5 For details of the data quality assessment report, please refer to the data fusion requirements part of system requirements in this chapter.

4.3.1.6 The document should at least consider the followings:
(1) The data cleaning plan and data evaluation report should be complete and meet the requirements;
(2) The estimated amount of data storage should be checked, and the relationship between the estimated amount and the actual storage of the data server should be checked;
(3) The completion of data backup strategy and the recovery strategy should be checked, and the performance of backup procedures, backup plans and backup recovery drill plans should be checked;
(4) The integrity of the data security strategy, data sharing descriptions, data interfaces, and sensor descriptions should be checked

4.3.2 Verification test

4.3.2.1 It is to verify the process of integration according to the approved test outline, which mainly includes the followings:
(1) Data integration scope verification;
(2) Data integrity verification;
(3) Data calibration verification;
(4) Data fusion verification;
(5) Data sharing verification;
(6) Data dissemination verification.

Chapter 5 Model Evaluation

Section 1 General Provisions

5.1.1 General requirements

5.1.1.1 Model refers to a formal expression from the abstraction of the physical entities in digital space. Based on the scenarios of ships and offshore installations, this guideline divides the model into the following two categories:

(1) Monitoring models, which objectively reflect the operation of related systems and equipment of the ships and offshore installations;

(2) Inferential models, which are designed to predict and analyze the future operation of the systems and equipment of ships and offshore installations, and diagnose faults based on previous operating data experience.

5.1.2 Model benchmark

5.1.2.1 Model evaluation shall be based on a benchmark, which can be a parameter file.

5.1.2.2 Model parameter file refer to the data items derived from the raw or processed parameters or external observations to provide a criterion for normal behavior of the system and equipment. Model parameter files can be used alone or combined with operation monitoring, fault diagnosis and performance prediction to determine working conditions.

5.1.2.3 The model parameter file can be obtained through the following ways:

(1) Sensor (parameters)；

(2) Measured processed data;

(3) Operating parameters;

(4) Verification and validation results.

5.1.2.4 The performance of the model or application should be verified under the same benchmark (the rules for normal system behavior of the machine should be provided when one or more model parameter files are used) environment.

Section 2 Model Measurement

5.2.1 Model performance

5.2.1.1 The performance of monitoring models can be described by precision and accuracy. The precision and authenticity are used to describe how close the measured value is to the true value or the reference measured value.

(1) The accuracy grade should be determined based on several tests sufficient to calculate the standard deviation. When determining the accuracy level, the repeatability of the test should be considered;

(2) The authenticity should be recorded by the deviation from the average of the measured/calculated value and the actual value.

5.2.1.2 The performance of inferential model can be described by such indicators as MSE, RMSE, and MAE, among which:

(1) Mean Square Error (MSE）

$$MSE = \frac{1}{n}\sum_{i=1}^{n}(y_i - \hat{y}_i)^2$$

Where, n is sample size

y_i is result variable

$\hat{y}_i$ is the model predicted value of the result variable of the sample

(2) Root Mean Square Error (RMSE）

$$RMSE = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(y_i - \hat{y}_i)^2}$$

Where, n is sample size

y_i is result variable

$\hat{y}_i$ is the model predicted value of the result variable of the sample

(3) Mean Absolute Error , MAE）

$$MAE = \frac{1}{n}\sum_{i=1}^{n}|y_i - \hat{y}_i|$$

Where, n is sample size

y_i is result variable

$\hat{y}_i$ is the model predicted value of the result variable of the sample

5.2.1.3 The performance of monitoring models can be described by such indicators as accuracy, precision, recall, F1 value, P-R curve, receiver operating characteristic curve (ROC curve), etc., among which:

(1) Confusion matrix

The confusion matrix is a cross tabulation of observation and prediction categories, as shown in Table 6.2.1.3.

Example of Confusion Matrix for Binary Classification **Table 6.2.1.3**

Prediction	Observation	
	Yes	No
Yes	TP	FP
No	FN	TN

Where, False Negatives (FN): The true value of the test data is positive, and the classifier prediction it is negative.

False Positives (FP): The true value of the test data is negative, and the classifier prediction is positive.

True Negatives (TN): The true value of the test data is negative, and the classifier prediction is negative.

True Positives (TP): The true value of the test data is positive, and the classifier prediction is positive.

(2) Accuracy (A)

$$A = {}^{(TP)}\Big/_{(TP+FP)}$$

Where, TP, FP, FN, TN are shown in Table 6.2.1.3.

(3) Precision (P)

$$P = {(TP + TN)}/{(TP + FP + TN + FN)}$$

Where, TP, FP, FN, TN are shown in Table 6.2.1.3.

(4) Recall (R)

$$R = {TP}/{(TP + FN)}$$

Where, TP, FP, FN, TN are shown in Table 6.2.1.3.

(5)F1 value

$$\mathrm{F1} = {P \times R \times 2}/{(P + R)}$$

Where, P is precision, R is recall.

(6)P-R curve

P-R curve is drawn based on the current P value and R value calculated each time and by means of sorting the possibility (probability) of the test sample as a "positive example" from high to low according to the prediction results.

When the P-R curve of model A is completely enclosed by the P-R curve of another model B, it is known that the performance of B is better than that of A.

When the curve models of A and B are overlapped, the performance with a larger area under the curve is better.

When it is difficult to estimate the area under the curve, according to the balance point (the value when P=R), the higher the value of the balance point is, the better the performance will be.

(7) ROC curve

ROC curve is drawn with the False Positive Rate (FPR) as the horizontal ordinate and the True Positive Rate (TPR) as the vertical coordinate.

Where,

$$FPR = \frac{FP}{TN + FP}$$

$$TPR = \frac{TP}{TP + FN}$$

Where, TP, FP, FN, TN are shown in Table 6.2.1.3.

If the TPR is higher, the FPR will be lower, that is, if the ROC curve is steeper, the performance of the model will be better.

When the ROC curve of model A is completely enclosed by the ROC curve of another model B, it is known that the performance of B is better than that of A.

When the curves of A and B are overlapped, the performance with a larger area under the curve is better.

5.2.1.4 For multiple confusion matrixes, the following calculation methods can be taken as a reference:

(1) Macro average

It is to first calculate the P and R values of each confusion matrix, then calculate the average P and R values, and finally calculate the F1 value.

$$\overline{P} = \frac{1}{n}\sum_{i=1}^{n} P_i$$

$$\overline{R} = \frac{1}{n}\sum_{i=1}^{n} R_i$$

Where, n is number of confusion matrix

P_i is the P value of confusion matrix i

R_i is the R value of confusion matrix i

(2) Micro average

It is to first calculate the average TP, FP, TN, FN of the confusion matrix, then calculate the P and R values, and then calculate the F1 value.

$$\overline{P} = \frac{\overline{TP}}{\overline{TP} + \overline{FP}}$$

$$\overline{R} = \frac{\overline{TP}}{\overline{TP} + \overline{FN}}$$

5.2.2 Model confidence

5.2.2.1 The confidence level should be calculated at least by a weighted evaluation of the following error sources:

(1) Development (assessment of processes and risks related to selection during model development);

(2) Performance evaluation and accuracy;

(3) Data quality of the descriptors used;

(4) Design documents of the system or module;

(5) Failure data and characteristics.

5.2.2.2 The confidence level corresponding to the empirical value (such as 95% (± 2 times the standard deviation) or 99.7% (± 3 times the standard deviation)) or other standard deviation multiple intervals can be directly used as the confidence level.

5.2.2.3 The confidence level can be adjusted according to the comparison and evaluation results of the risk of the functional failure mode.

5.2.2.4 When different types of models are combined into one, it will be considered an application model or a hybrid model. The diagnostic model can also be a main model or a combination of multiple sub-models. Such models should be decomposed to fully calculate the confidence level.

5.2.2.5 The confidence interval can be calculated according to the calculated confidence level.

5.2.2.6 The models used for diagnosis and/or prediction should have the descriptions of relevant limitations and applicable operating conditions.

Section 3 Model Verification

5.3.1 Verification of monitoring models

5.3.1.1 The model can reflect the running condition of the physical entity.

5.3.1.2 The model data should meet the functional integrity requirements.

5.3.1.3 The validity of the data used in model verification should be guaranteed.

5.3.1.4 The verification indicators applicable to the model should be selected according to the model.

5.3.1.5 The quality of data used for the model should be evaluated as qualified.

5.3.1.6 The working conditions of steady state and transition state of the model should be verified.

5.3.1.7 The following verification details should be determined based on the use and functions of the model:

(1) Parameter verification;
(2) Data integrity verification;
(3) Model indicator verification;
(4) Data quality assessment;
(5) Data storage period verification.

5.3.2 Verification of inferential models

5.3.2.1 Inferential data refers to the data calculated by the digital system based on historical operating data or empirical data on the current or future trend of the operating process of the system.

5.3.2.2 Inferential data includes the data used for diagnosis, prediction, and decision-making.

5.3.2.3 Inferential data must be obtained after one or more operating cycles including the start and stop of the digital system.

5.3.2.4 The verification indicators applicable to the model should be selected according to the model.

5.3.2.5 The verification and validation of the inferential model shall be based on the dependent digital system, as well as the algorithm adopted, the data used and the conclusions generated. In addition, the following aspects shall be considered.

(1) Integrity assessment of the digital system;

(2) Data quality assessment of data retained in the digital system;

(3) Models used for diagnosis and prediction of the digital system.

5.3.2.5 The working conditions of steady state and transition state of the model should be verified.

5.3.2.6 The following verification details should be determined based on the use and functions of the model:

(1) Verification of the confidence of the model;

(2) Verification of the model based on the indicators listed in paragraphs 5.2.1.2 to 5.2.1.4 of this guideline.

5.3.3 Verification of model results

5.3.3.1 It is to compare the actual operating data and the model data of the verified item to obtain the comparison results based on the indicators selected in paragraphs 5.2.1.2 to 5.2.1.4 of this guideline (or select more applicable indicators by negotiation with CCS).

5.3.3.2 The model confidence level that meets CCS requirements.

Chapter 6 Data Application

Section 1 General Provisions

6.1.1 General requirements

6.1.1.1 Data application takes the digital system as the carrier. Data application refers to the services provided by the digital system to people, organizations or systems, and the function of which refers to the range of capabilities that the digital system can achieve.

6.1.1.2 The digital system application is divided into four functions: monitoring, diagnosis, prediction and decision-making.

6.1.2 System requirements

6.1.2.1 The digital system shall meet the applicable technical requirements for data identification and data activities.

6.1.2.2 The digital system, according to its application business requirements, shall meet the applicable international conventions, flag state requirements, IACS requirements, CCS rules and guidelines, technical standards, etc.

6.1.2.3 The digital system can build the equipment and systems for operation of the ships and offshore installations through models, and the models built should be verifiable.

6.1.2.4 The digital system reliability, integrity, change management, network security, data quality and data security should meet the relevant requirements of Chapter 1 of this guideline.

6.1.2.5 The digital system shall identify the data according to the requirements of Chapter 2 of this guideline, and it is recommended to carry out classified and graded management according to Chapter 2 of the “Guidelines for Quality Assessment of Ship Data”.

6.1.2.6 The data quality should be monitored according to the “Guidelines for Quality Assessment of Ship Data” based on the business requirements. When the data quality fails to meet the design requirements, the system should be able to identify, record and report relevant information.

6.1.2.7 The digital system itself must be able to ensure the stability of the services, and detect or recover in a timely manner when an abnormality occurs in itself.

6.1.2.8 The digital system should have self-inspection capabilities and be able to generate self-inspection report, including but not limited to:
(1) Whether data collection meets the requirements;
(2) Whether network connection is normal;
(3) Whether related hardware is in normal working condition;
(4) Whether the status of each component of the digital system is normal.

6.1.2.9 For abnormal output, wrong results, obvious deviations, untimely response, etc. found during operation of the digital system, the operator shall record and provide feedback to the operation and maintenance personnel in a timely manner to make timely corrections.

6.1.2.10 Data collection of the digital system shall meet the relevant requirements of Chapter 3 of

this guideline according to the specific scheme adopted.

6.1.2.11 Data integration of the digital system shall meet the relevant requirements of Chapter 4 of this guideline according to the specific scheme adopted.

6.1.2.12 The digital system should have friendly human-computer interaction and be easy to use. It is recommended that the relevant requirements of ISO 9241-210 be satisfied.

6.1.2.13 The application capability of the digital system should be achieved based on risk and reliability analysis.

Section 2 Monitoring

6.2.1 General requirements

6.2.1.1 Monitoring refers to the collection of data through automatic and system generation to achieve online monitoring of the true state based on complete digital description and expression of the physical entities.

6.2.2 Technical requirements

6.2.2.1 The digital system monitoring should have the following functions:
(1) Describe and display the status and statistical information of the monitored object;
(2) Monitor key nodes of the physical entities;
(3) Describe the true status of the system and report the status, events and alarms;
(4) Query and provide information about the current and historical status.

6.2.2.2 Data monitoring range
(1) The monitoring range and process of the digital system should meet the business requirements;
(2) Data entered by other means shall be confirmed in an appropriate manner.

6.2.2.3 The model of the digital system should meet the requirements of the monitoring models.

6.2.2.4 The data storage capacity of the digital system should meet business requirements, and periodic storage or event storage can be used, which are shown as follows:
(1) Periodic storage: the storage duration should meet the design voyage time of the ship, the inspection period of the ships and offshore installations, and the requirements of the regression algorithm (if applicable);
(2) Event storage: when the status of monitored object is abnormal or performance degradation event occurs, the system can store all relevant data covering the entire event time period.

6.2.2.5 The monitoring performance of the digital system should meet the design business and scenario requirements, and the system performance level should be guaranteed through appropriate methods.

Section 3 Diagnosis

6.3.1 General requirements

6.3.1.1 Diagnosis refers to the analysis and judgment of faults, failures or performance degradation that have occurred based on the information obtained from status monitoring, with the combination

of known structural characteristics and parameters, as well as environmental conditions and historical data to determine the nature, category, degree, cause and location.

6.3.1.2 If the digital system application capability is based on the monitoring capability, the relevant requirements of Chapter 6, Section 2 of this guideline should also be satisfied.

6.3.2 Technical requirements

6.3.2.1 The digital system should have the following functions:
(1) Identify the faults, failures and operation modes of the physical entity in a timely manner;
(2) Locate the fault/failure location and scope of the physical entity;
(3) Determine the cause of fault, failure or performance degradation;
(4) Provide diagnostic information, including health or status indicators;
(5) Generate samples for confirmed faults/failures;
(6) Support users in trouble shooting and removal.

6.3.2.2 The diagnostic application range and process of the digital system should meet the application business requirements.

6.3.2.3 The model of the digital system should meet the requirements of the inferential model.

6.3.2.4 Complete diagnosis records should be stored. It is recommended to have a certain playback capability. The records include but are not limited to basic information, nature, category, degree, reason, location, phenomenon, related conditions, time of occurrence, any state abnormality or not before the occurrence, the diagnosis methods adopted and the final diagnosis results.

6.3.2.5 The diagnostic performance of the digital system should meet the design business and scenario requirements, and the performance level of the system should be guaranteed through appropriate methods.

Section 4 Prediction

6.4.1 General requirements

6.4.1.1 Prediction refers to the fact that the digital system predicts the future state and trend of the corresponding physical entity based on the historical and real-time data and according to the objective development trend and variation regularity, with the combination of experience and knowledge.

6.4.1.2 If the digital system application capability is established based on the monitoring and diagnosis capabilities, the relevant requirements of Section 2 and Section 3 of Chapter 6 of this guideline shall also be satisfied.

6.4.2 Technical requirements

6.4.2.1 The prediction capability of the digital system should have the following functions:
(1) Predict the future state, performance, trend, or failure time of the physical entity;
(2) Improve the prediction ability through historical data;
(3) Predict certain results with algorithms;
(4) Send out early warning information when the early warning conditions are reached (if applicable).

6.4.2.2 The prediction application range and process of the digital system should meet the application business requirements.

6.4.2.3 When the prerequisites of prediction fail to meet the requirements, relevant information should be recorded, identified and reported.

6.4.2.4 The digital model should meet the requirements of the inferential model.

6.4.2.5 The prediction results should be stable, repeatable and meet the confidence level.

6.4.2.6 Complete prediction records should be stored. It is recommended to have a certain playback capability, including basic information, prediction conditions or assumptions, prediction use data, and prediction results.

6.4.2.7 The predictive performance of the digital system should meet the design business and scenario requirements, and the performance level of the system should be guaranteed through appropriate methods.

Section 5 Decision-making

6.5.1 General requirements

6.5.1.1 Decision-making refers to the fact that the digital system proposes a feasible plan for achieving a specific goal based on the digital description and expression of the physical entity or system, combined with the diagnosis results and the future state and trend, selects the best plan after comparison, analysis and evaluation, and puts the best solutions into the process of implementation and monitoring.

6.5.1.2 If the digital system application capability is based on the monitoring, diagnosis, and prediction capabilities, the relevant requirements of Chapter 6, Section 2, Section 3, and Section 4 of this guideline should also be satisfied.

6.5.2 Technical requirements

6.5.2.1 The decision-making capability of the digital system should have the following characteristics:
(1) Provide mandatory or suggestive action plans based on available prediction results;
(2) Evaluate the effectiveness of each option and how to optimize future actions without affecting other priorities.

6.5.2.2 The decision-making application range, process and result of the digital system should meet the application business requirements.

6.5.2.3 When the decision-making prerequisites fail to meet the requirements, relevant information should be recorded, identified and reported.

6.5.2.4 The digital model should meet the requirements of the inferential model.

6.5.2.5 The decision-making results should be stable, repeatable and meet the confidence level.

6.5.2.6 Complete decision-making records should be stored. It is recommended to have a certain playback capability, including basic information, decision-making conditions or assumptions, decision-making use data, decision-making options, and optimization results.

6.5.2.7 The decision-making performance of the digital system should meet the design business and scenario requirements, and the system performance level should be guaranteed through appropriate methods.

6.5.2.8 For the condition-based maintenance system, the recommended maintenance scheme should be based on the degree of danger of the mechanical equipment or components, operating costs, maintenance costs, availability of spare parts and other factors.

6.5.2.9 The decision-making control of the digital system should meet the following requirements:
(1) The digital system should provide timely and sole optimization results. otherwise relevant information should be reported;
(2) The decision-making results should be converted into the commands executable by the control agency;
(3) The digital system should monitor the execution results and make appropriate assessment;
(4) The digital system should have the ability of human intervention.

Section 6 Data Application Capability Verification

6.6.1 Basic document requirements

6.6.1.1 For application capability verification of the digital system, the following documents should be submitted:
(1) Digital system specifications, including but not limited to the followings:
① Description of business scope and application scenarios;
② Requirements specification for network and communication security;
③ Requirements specification for required data quality;
④ Description of functions;
⑤ Description of performance;
⑥ Description of such prerequisites as boundaries and limits;
⑦ Interface description, including human-computer interaction;
⑧ Interaction protocol and other protocol lists and documents.
(2) Data model related explanatory materials and verification results;
(3) Verification documents related to digital system reliability, integrity, change management, network security, data quality and data security;
(4) System function and performance test procedures: test process, test methods, test environment, test tools, technical indicators, test schedule;
(5) Information listed in 2.3.2 of data identification;
(6) Information listed in 3.4.1 of data collection;
(7) Information listed in 4.3.1 of data integration.

6.6.2 Supplementary document requirements for monitoring capability verification

6.6.2.1 To verify the monitoring capability of the digital system, the following documents should also be submitted:
(1) Monitoring procedures, including monitoring methods/techniques, monitoring modes (online monitoring, off-line monitoring and periodic measurement, the measurement period should be indicated for periodic measurement), benchmark measurement procedures, equipment condition

monitoring procedures, etc.;
(2) Calibration procedures and plans for the monitoring devices.

6.6.3 Supplementary document requirements for diagnostic capability verification

6.6.3.1 To verify the diagnostic capability of the digital system, the following documents should also be submitted:
(1) Diagnosis and status assessment method description, including principle description, process, mechanism, example, etc.;
(2) Feature extraction and pattern recognition methods, if applicable;
(3) Diagnostic instructions, including but not limited to the followings:

① List the possibly damaged parts of the diagnostic object;

② List the faults and status related to these parts;

③ Give potential observable symptoms for each fault;

④ Name the status monitoring characterization that will be used;

⑤ Indicate the methods and parameters used to calculate the characterization.

6.6.4 Supplementary document requirements for predictive capability verification

6.6.4.1 To verify the predictive capability of the digital system, the following documents should also be submitted:
(1) Prediction method description, including principle description, process, examples, etc.;
(2) Database description required by the prediction function.

6.6.5 Supplementary document requirements for decision-making capability verification

6.6.5.1 To verify the decision-making capability of the digital system, the following documents should also be submitted:
(1) Decision-making method description, including principle description, process, examples, etc.;
(2) Database description required by the decision-making function.

6.6.6 Verification test

6.6.6.1 The system applying for digital application capability level evaluation shall be verified and tested according to the following requirements:
(1) Data identification shall be verified and tested according to the requirements of 2.3.1;
(2) Data collection shall be verified and tested according to the requirements of 3.4.2;
(3) Data integration shall be verified and tested according to the requirements of 4.3.2;
(4) The digital model verification requirements are shown in Table 6.6.6.1(4);

Digital Model Verification Requirements **Table 6.6.6.1(4)**

Application Ability Level	Digital Model Verification Requirements
Monitoring	See the requirements in Section 5.3.1 of this guideline
Diagnosis	See the requirements in Section 5.3.2 of this guideline
Prediction	See the requirements in Section 5.3.2of this guideline
Decision-making	See the requirements in Section 5.3.2of this guideline

(5) For functional integrity test in the system integrity, please refer to Table 1.3.2.1(1);
(6) For performance efficiency test, please refer to Table 1.3.2.1(2).

Chapter 7 Data Implementation

Section 1 General Provisions

7.1.1 General requirements

7.1.1.1 The digital system shall meet the technical requirements of data identification, collection, storage and integration chapters of this guideline, and have certain data application capabilities to realize one or the combination of monitoring, diagnosis, prediction and decision-making functions.

7.1.2 Scope of application

7.1.2.1 This chapter applies to the scenarios where digital systems are installed on ships and offshore installations, as well as the scenarios where digital systems are installed in shore-based data centers.

Section 2 Digital System Process Assessment

7.2.1 General requirements

7.2.1.1 The digital system process assessment specifies the general requirements for evaluating the digital system to certify that the digital system applicant is capable of developing, deploying, monitoring and maintaining a digital system.

7.2.1.2 The digital system process mainly includes the following three aspects of assessment:

(1) The digital system development process assessment;
(2) The digital system delivery process assessment;
(3) System reliability assessment of the digital system application.

7.2.1.3 Digital system process assessment is the basis for applying for type approval of the digital system.

7.2.1.4 When there are important changes made to the processes assessed in the development and delivery of the digital system, the digital system applicant shall notify CCS. For major changes to the digital system, CCS may require -re-assessment to maintain the digital system certificate.

7.2.2 Development process assessment

7.2.2.1 To assess the development process of the digital system, the following documents shall be submitted:

(1) Specifications;
(2) Process controls related documents;
(3) Technical requirements.

7.2.2.2 Specifications, including but not limited to the followings:

(1) From the functional level, the description document of the algorithm for the design and development of the following functions:

① Sensors;

② Data collection/storage/integration;

③ Data modeling;

④ Fault detection (if applicable) ;

⑤ Diagnosis (if applicable) ;

⑥ Prediction (if applicable);

⑦ Decision-making recommendations (if applicable).

(2) Alarm limits.

7.2.2.3 Process control related documents, including but not limited to the followings:

(1) The process for establishing a team of subject matter experts with the required qualification and experience;

(2) Description of personnel training and qualification requirements, such as user guidance and training manuals;

(3) Quality management system description;

(4) System version control process;

(5) System update strategy, not limited to update method, frequency, etc. ;

(6) Verification data management, including data management and data quality management, and how to submit the data to CCS (if applicable);

(7) System failure report.

7.2.2.4 Technical requirements, including but not limited to the followings:

(1) Risk assessment techniques/methods (such as FMEA/FMECA, etc.);

(2) Data representation and mapping;

(3) Test plan, including test objectives, test environment, test methods, etc.;

(4) Service reports, including operation scenarios of the digital system.

7.2.3 Delivery process assessment

7.2.3.1 To assess the delivery process of the digital system, the following documents shall be submitted:

(1) Specifications;

(2) Process controls related documents;

(3) Technical requirements.

7.2.3.2 Specifications, including but not limited to the followings:

(1) System description, including the purpose and objectives of the digital system, system block diagram, system interface, etc.;

(2) Requirements specification;

(3) Detailed description of the quality management system used in the development and delivery of the digital system.

7.2.3.3 Process control related documents, including but not limited to the followings:

(1) The process for establishing a team of subject matter experts with the required qualification and experience;

(2) Data use strategies of the digital system, for example, when and how to transmit data;

(3) Strategies related to digital system updates, such as equipment adjustments and changes in service;
(4) Digital system software upgrade and version control strategies.

7.2.3.4 Technical requirements, including but not limited to the followings:
(1) Detailed description of the implementation of the digital system, such as which model is used;
(2) Principles and/or basis of diagnosis and prediction algorithms for the digital system;
(3) The review process for the diagnosis and prediction of false positive and false negative result events, including the prediction scope of errors and how these events are maintained during the service cycle of this digital system;
(4) Verification plan for the digital system and the physical system;
(5) Samples of previously published service reports, as well as samples of service reports and recording procedures. These processes should fully reflect that the correct operation of the digital system can be verified, so that it can be checked and confirmed during periodic inspection of CCS.

7.2.4 Reliability assessment

7.2.4.1 The relevant hardware and software of the digital system involved in this guideline shall meet the requirements of Section 6, Chapter 2, Part 2 of CCS "Rules for Classification of Sea-going Steel Ships", and be subject to drawing review and inspection by CCS.

7.2.4.2 The software development of the digital system shall meet the requirements of CCS "Guide for Safety and Reliability Assessment for Shipboard Software".

7.2.4.3 The data quality of the digital system shall meet the requirements of Chapter 3 of CCS "Guidelines for Quality Assessment of Ship Data".

7.2.4.4 In addition to the submitted information involved in the relevant requirements of 7.2.4.1-7.2.4.3, the following information shall also be submitted for reliability assessment of the digital system software:
(1) Specifications;
(2) Process controls related documents;
(3) Technical requirements.

7.2.4.5 Specifications, including but not limited to the followings:
(1) Digital system software development requirements specification;
(2) Digital system network security requirements specification;
(3) Requirements specification for data quality required by the digital systems;
(4) Specification related to the digital system functions;
(5) Specification related to the digital system performance, including but not limited to the followings:
① Integrity;
② Availability;
③ Identity authentication;
④ Confidentiality;
⑤ Accessibility;

⑥ Storage.

(6) Description of the prerequisites such as boundaries and limits of the digital system.

7.2.4.6 Process control related documents, including but not limited to the followings:

(1) Digital system description and user manual;

(2) Test plan and report;

(3) Configuration management;

(4) Description of suitable development process and life cycle activities.

7.2.4.7 Technical requirements, including but not limited to the followings:

(1) The degree of compliance and/or consistency between the digital system and its use requirements in the actual operating environment;

(2) Suitability assessment for use of machine learning, artificial intelligence or non-deterministic software technology.

Section 3 Digital System Principle Approval

7.3.1 General requirements

7.3.1.1 The digital system principle approval object is a complete equipment or system to be verified, and all parts in the equipment or system are regarded as components.

7.3.1.2 The digital system principle approval is implemented according to the requirements of Section 11, Chapter 3, Part 1 of "Rules for Classification of Sea-going Steel Ships"[2], and inspections are mainly carried out from the perspectives of development and delivery process, technical solutions feasibility, risk assessment, etc.

7.3.1.3 It is necessary to meet the process assessment requirements in Section 7.2 of this guideline in the event of application for digital system principle approval.

7.3.2 Documents

7.3.2.1 In the event of applying for digital system principle approval, the following documents shall be submitted:

(1) Specifications;

(2) Process controls related documents;

(3) Technical requirements.

7.3.2.2 Specifications, including but not limited to the followings:

(1) System description of the digital system, including the purpose and objectives of the digital system, system block diagram, system interface, etc.;

(2) Operation manual, including which functions and/or information are automatic, which are the alarms and/or suggestions provided to users, and the needs or requirements related to the maintenance of the digital system, etc.;

(3) Design description of the digital system, including sensor data flow, external sensor data used and its sampling frequency requirements, detailed description of functional logic, as well as logical description of digital system service realization;

(4) If applicable, the transmission description from the ship end to the development and deployment center, including the transmission method, protocol, frequency, security requirements, etc.

7.3.2.3 Process control related documents, including but not limited to the followings:

(1) When the digital system provides alarms related to equipment failure status, the alarm list, alarm category definition, as well as the alarm generation logic, conditions and handling procedures shall be provided to CCS;

(2) Provide the experience of subject matter experts used in digital system development.

7.3.2.4 Technical requirements, including but not limited to the followings:

(1) Detailed description of the principle that each component in the physical system or asset can continue to serve, and how the upper and lower limits of the working conditions are determined, how the logical functions associated with the working conditions data are defined, and how the maintenance recommendations are determined;

(2) Detailed description of the recommended actions of the digital system for possible working conditions;

(3) FMEA (FMECA or similar) analysis for each component using the applications of digital system monitoring, diagnosis, prediction, etc.;

(4) For each failure mode of the components analyzed by FMEA, the following information shall be submitted:

① Technology list of data collection and signal processing, such as filtering, signal amplification (if applicable), etc.;

② A feature list that can indicate the occurrence and severity of the failure;

③ List of fault detection algorithms;

④ List of fault diagnosis algorithms, including models for handling, evaluating and classifying faults.

(5) Detailed description of the analysis algorithm for the failure mode of each component that can be monitored by the digital system;

(6) The digital system applicant should provide a digital system diagnostic technology evaluation report, which shall clearly describe how faults of different functional levels are detected and how to evaluate the status of the equipment. In addition, the report should also include the acceptance principles for sustainable operation of the equipment.

(7) Make a detailed description of the data and processing procedures used in the development of the digital system to ensure that the data of appropriate quality and quantity are used;

(8) For the output of the digital system, a detailed description of risk and confidence should be provided;

(9) Describe how to implement/verify the risk and confidence of the digital system;

(10) Make sure that the digital system is fully tested and robust, and can be installed and deployed as a digital representation of characteristic objects or assets in the ships and offshore installations or systems;

(11) The digital system shall ensure an acceptable output of the test methods during the life cycle, such as the test and verification processes, built-in test systems, simulations, etc.;

(12) When the digital system provides decision-making suggestions, for example, in terms of the suggestions for revision of the equipment maintenance plan, samples should be provided to illustrate the process, basis and corresponding responsibilities of supporting decision-making;
(13) When major changes occur to the software, logic functions, limit conditions, etc. of the digital system, CCS shall be notified. The notification contents shall include the acceptance principle of the change, such as the data requirements used by the machine learning algorithm, so that CCS can understand the acceptance principles used in current development and services;
(14) Data loading frequency of the digital system;
(15) The handling policy/process of the digital system asset changes and changes in the services provided by the digital system applicant.

Section 4 Digital System Integration Operation

7.4.1 General requirements

7.4.1.1 The digital system integration operation is to verify that the digital system can deploy and complete specific functions or tasks in the actual operating environment.

7.4.1.2 The digital system should be installed and deployed according to the plan.

7.4.1.3 The contents of digital system test depend on the maturity and the confidence level (if any) of the digital system, as well as the degree of harm caused by failure of the digital system, etc.

7.4.1.4 When there is limited service experience of the digital system, the normal operation and maintenance requirements should be maintained until sufficient evidence shows that the business requirements of the digital system can be satisfied.

7.4.1.5 The digital system for ships and offshore installations should meet relevant requirements for principle approval.

7.4.2 Technical requirements

7.4.2.1 Review the records of all false positive results and false negative results events, and how these events are applied to the digital system, such as the retraining models, etc.

7.4.2.2 CCS will confirm the maintenance has been carried out as required by the digital system and check the maintenance records to ensure that the digital system meets the expectations. Check all anomalies/defects records, and evaluate the accuracy of the digital system's decision-making services to determine whether the digital system has the ability to continue to serve. The equipment records shall include the anomalies under the condition that the boundary limits of the digital system are exceeded, and what action was taken.

7.4.2.3 When the digital system is implemented by a shore-based data center, the data transmission records of the digital system should also be checked.

7.4.2.4 When defects in the decision-making suggestions of the digital system are found, the marine surveyor may request further review. If there are serious defects, a report can be submitted to CCS to withdraw the certificate of the digital system.

7.4.3 Documents

7.4.3.1 To verify the integration operation of the digital system, the following documents shall be submitted:

(1) Specifications;

(2) Process controls related documents;

(3) Technical requirements.

7.4.3.2 Specifications, including but not limited to the followings:

(1) System description of physical objects or entities, including functional and performance requirements;

(2) Training materials for the operators of the digital system, including manuals, training materials, etc.

7.4.3.3 Process control related documents, including but not limited to the followings:

(1) When major changes occur to the software, logic functions, limit conditions, etc. of the digital system, CCS shall be notified. The notification contents shall include the acceptance principles for change, such as the data requirements used by machine learning algorithms, so that CCS can understand the acceptance principles used in current development and services;

(2) Minimum training requirements and qualifications for the operators of the digital system, as well as the maintenance requirements for digital system output;

(3) Examples of diagnosis and prediction of the digital system to show how the digital system works;

(4) If applicable, a detailed description of equipment maintenance related information not covered by the digital system, such as maintenance items, cycles, etc.;

(5) When the digital system provides decision-making suggestions, such as suggestions for revision of the equipment maintenance plan, samples should be provided to illustrate the process, basis, and corresponding executive responsible person for supporting decision-making.

7.4.3.4 Technical requirements, including but not limited to the followings:

(1) Detailed description of all sensors used by the digital system;

(2) Models and data of expected functions of the digital system;

(3) If applicable, description of the calibration methods and frequency of the measuring equipment or sensors that provide data for the digital system;

(4) Requirements for recording equipment failures and how these records are applied to the digital system;

(5) Data loading frequency of the digital system.

7.4.4 Inspection and verification

7.4.4.1 The inspection of the digital system integration operation phase mainly includes:

(1) Documents inspection;

(2) Tests witnessed by surveyor;

(3) Sea trial (if applicable).

7.4.4.2 Documents inspection is not limited to the inspection of the documents required in paragraph 7.4.3 of this guideline.

7.4.4.3 Please refer to Section 2.3 of this guideline for the verification requirements of data identification.

7.4.4.4 Please refer to Section 3.4 of this guideline for the verification requirements of data collection.

7.4.4.5 Please refer to Section 4.3 of this guideline for the verification requirements of data integration.

7.4.4.6 Tests witnessed by surveyor include but is not limited to the following items:

(1) Presentation related test;

(2) Interface/protocol test;

(3) Function test;

(4) Performance test;

(5) Data sensitivity test;

(6) Model test;

(7) Failure mode test;

(8) Network security test;

(9) Data quality assessment.

7.4.4.7 For detailed description of equipment maintenance related information not covered by the digital system, real ship verification test includes but is not limited to the following items:

(1) Interface and protocol verification;

(2) Data reception and presentation verification;

(3) Functional compliance verification of the digital system;

(4) Handling and recording of false positive and false negative events in the actual system;

(5) Optimization process test of the digital system.

Chapter 8 Digital System Verification Methods

Section 1 General Provisions

8.1.1 General requirements

8.1.1.1 The verification methods include risk assessment, engineering assessment and direct assessment, and relevant work should be carried out based on risks in the process of test and verification.

8.1.1.2 For the test of the digital system with self-verification function, the verification methods should be tested first.

Section 2 Risk Assessment

8.2.1 Purpose of risk assessment

8.2.1.1 The purpose of risk assessment is to identify the technical risks and uncertainties related to the digital system, and record all foreseeable hazards, their causes, consequences, and consider potential risk control measures in the application and operating environment.

8.2.2 Risk assessment requirements

8.2.2.1 Before implementation, the risk assessment plan shall be approved by CCS and shall include at least the following items:

(1) Assessment scope;

(2) The knowledge and background information of the evaluator;

(3) preparation before assessment:

① Related information collection;

② Determination of risk assessment methods;

③ Assessment criteria (risk matrix, etc.).

8.2.2.2 A risk assessment report should be generated after the completion of risk assessment, including at least the following items:

(1) Assessment scope;

(2) Risk assessment assumptions and reference data;

(3) Supporting documents or information related to risk assessment;

(4) Risk item identification, cause analysis, risk consequence, frequency analysis, risk level, as well as whether measures need to be taken to reduce the risk level;

(5) Risk control measures and their effectiveness;

(6) Assessment conclusions and recommendations.

8.2.2.3 For risk assessment of the digital system based on a single data-driven model, the risk factors and/or risk items can be analyzed through analysis of the model development and deployment process. The assessment process includes at least the followings:

(1) Determine the function list of the system to be assessed based on the system description and/or other system data of the system to be assessed;
(2) Risk matrix, and the criteria for determining the probability/possibility and consequences;
(3) List of functions confirmed by the system to be assessed;
(4) Develop a risk register;
(5) Identify the risk items based on the risk register;
(6) For each risk item, estimate its probability and consequences, and calculate the risk (risk=probability×consequence);
(7) Grade these risks using the risk matrix;
(8) Define risk mitigation measures for high-risk items.

8.2.2.4 For non-single data-driven models, the data-driven models are combined with the modules based on physics and/or heuristic method or rules. For risk assessment of this type of system, the process is as follows:
(1) Develop a function list of the system to be assessed according to the system description and/or other system data of the system to be assessed;
(2) For each data-driven sub-model, the system to be assessed confirms the list of functions;
(3) Fill out the risk register according to the contents of the list;
(4) Repeat steps (2) and (3) until the risk register of all data-driven sub-models is filled in;
(5) Identify the risks after combination of the data-driven sub-models and fill in the risk register;
(6) Identify one or more adverse effects/risk items for each entry in the risk register;
(7) For each risk item, estimate its probability and consequence, and calculate the risk (risk=probability × consequence);
(8) Grade these risks using the risk matrix;
(9) Identify the unacceptable high-risk items;
(10) Define risk mitigation measures for high-risk items.

Section 3 Engineering Assessment

8.3.1 Purpose of engineering assessment

8.3.1.1 It is mainly to verify the realization of the predefined functions and performance of the digital system, as well as the security.

8.3.2 Requirements of engineering assessment

8.3.2.1 Review engineering design, by verifying the defined functions and performance of the digital system, and the compliance of the system design.

8.3.2.2 Simulate and analyze the digital system.

8.3.2.3 Verify the function and performance of the digital system through functional test, model test and prototype test. The test should be carried out in the design requirements.

8.3.2.4 Analyze the interface of the digital system and test it in the integrated system. The integrated system includes human and environment.

8.3.2.5 Verify the inference results based on the operation data of the digital system.

8.3.2.6 Verify whether the digital system can be monitored, tested and maintained.

8.3.2.7 Establish and maintain the quality certification and control procedures according to industry standards, and determine the accreditation standards for each verification stage.

Section 4 Direct Assessment

8.4.1 Purpose of direct assessment

8.4.1.1 The purpose of direct assessment is to analyze the behavior of the digital system.

8.4.2 Requirements of direct assessment

8.4.2.1 Direct assessment requires the training and test data of the model. The models and data may not be accessible due to commercial and/or technical reasons.

8.4.2.2 The model behavior can be analyzed with white box and black box methods. The white box method needs to analyze the internal parameters of the model to identify which parameters are the most important and which parameters can be ignored. However, the black box method is to use the model as it is and infer which parameters are relevant by analyzing its behavior.

8.4.2.3 In the direct assessment process, it is assumed that the actual data in the deployment environment and the training and test data in the development process should have the same statistical properties. The applicant of the digital system shall provide evidence to prove this assumption. If this assumption is not valid, the actual data in the deployment environment is" out of distribution". In this case, the applicant needs to provide evidence to prove that the behavior of the application is reasonable.

8.4.2.4 For any particular model, the appropriate level of explainability/interpretability required for the assurance that the application will operate as expected without adverse consequences and the complete risk profile depends on the intended use and importance of the application. The interpretability means that the model (white box) is easy to understand, and users with experience can understand the meaning of the model; The explainability means that the researcher makes an understandable explanation for the behavior of the black box model.

8.4.2.5 For the expected behavior of the application related to data quality and assessment, the data quality indicators (such as integrity) and assessment indicators (on known test data, such as mean square error, area under the operating characteristic curve (AUC)) can be used. The data quality indicators and assessment indicators need to be determined according to the specific application scenarios and modeling methods of the application, so that the assessment of relevant parts is relatively objective.

8.4.2.6 The calculation of data quality should be implemented by a runtime service that monitors the quality of data input and output to the application. When the input/output data quality is low, the runtime service can detect the deviation and record this automatic check to indicate that the current model is in an in-guaranteed state, and notify the user in an appropriate way.

Section 5 Test of the Verification Methods

8.5.1 Test methods

8.5.1.1 The digital system can complete data-driven verification by collecting, processing and analyzing the system data.

8.5.1.2 Data-driven verification can be completed through the built-in programs or proxy verification system of the digital system, among which:

(1) System built-in program verification refers to that the verification method is implemented as a part of the digital system function;

(2) Proxy verification refers to the establishment of a digital representation (such as a model) based on the data of the digital system by the proxy application or system, and the verification of the digital system shall be realized according to the requirements of this guideline.

8.5.2 Test of the verification methods

8.5.2.1 Data-driven verification can be performed by the crew according to the approved test method, or realized by automated means.

8.5.2.2 The scope of data-driven verification should cover the items required for digital system verification, and provide the credibility not lower than traditional verification.

8.5.2.3 The scope of data-driven verification should be managed based on risk assessment.

8.5.2.4 The hardware and software systems based on data-driven verification shall comply with relevant CCS requirements.

8.5.2.5 The process of data-driven verification should not affect the realization of the functions of the digital system, and priority should be given to ensuring the normal functions of the digital system.

8.5.2.6 Data-driven verification shall provide relevant detailed documents to allow CCS to have sufficient knowledge of the hardware and software functions, test procedures, etc. of the data-driven verification method, so as to objectively evaluate the test data and conclusions to ensure the credibility of “black box” test.

8.5.2.7 The first verification based on data-driven verification should be completed based on the following steps:

(1) Approval of the verification plan based on the digital system and required documents;

(2) According to the plan, test the validity of the verification method in the digital system, including the verification standard and the authenticity of the conclusion, as well as the functions and performance within the declaration scope of the following verification methods:

① Verify the functions and capabilities of the digital system;

② Verify the ability of the digital system to deal with failure mode;

③ Ability to find defects in the digital system;

④ Verify the security of the digital system.

8.5.2.8 Data-driven verification should be able to collect and store the data from the digital system during test and verification and transmit them to the remote data servers for ships and offshore installations to ensure the data use and retrieval requirements. This function should not rely on any temporary or long-term communication connection.

8.5.2.9 It shall be possible to provide all test data and conclusions to CCS as the basis for test according to the requirements. The integrity and authenticity of the data provided shall be ensured.

The form and contents of provision shall be approved by CCS and serve as the part of the test process.

8.5.2.10 The verification basis should be based on the data generated by the system, and some pictures (including screenshots) and videos can be served as the verification basis.

8.5.2.11 When pictures (including screenshots) and videos are used as the basis for verification, corresponding mechanisms or procedures shall be available to ensure their authenticity.

8.5.2.12 Data-driven verification should at least provide the followings to CCS:

(1) The configuration and status of the digital system and related subsystems at the beginning of each test;

(2) The execution of the test (whether it was executed correctly according to the process);

(3) System response and performance data of the digital system;

(4) Verification standards;

(5) Personnel performing the test.

8.5.2.13 The software version and OEM service report (if any) of the main subsystems or modules of the digital system shall be verified.

8.5.2.14 The scope, functions and revision of data-driven verification shall be approved by CCS.

8.5.2.15 Data-driven verification should be able to identify a specific set of data in each test, which shall serve as the standard for assessment and verification.

8.5.2.16 The data-driven verification system or module should clearly display the test and verification status of each test item of the digital system, such as start/not start, due/not due, end/not end, etc.

8.5.2.17 The data-driven verification system or module shall be protected by a password, and be able to identify the login address of the operator, and shall have a digital mark for the digital system that has passed the test.

8.5.2.18 The data-driven verification system or module should provide a dedicated user interface for the marine surveyor to log in and complete verification related work, including status overview of the digital system, as well as subsequent planned tests and verification.

8.5.2.19 The cancellation, un-completion or failure of the test and verification shall be recorded and the reasons shall be explained.

8.5.2.20 Instructions and guidance as well as related mechanisms should be provided for the data-driven verification to ensure that the test and verification operations are correct, and the results are non-tamper and repeatable.

8.5.2.21 The data-driven verification system or module should operate in offline or online (connected with remote data server, etc.) mode.

8.5.2.22 The report generated should indicate whether CCS inspection is required.

8.5.2.23 The data-driven verification system should support CCS to generate reports in a customized manner to show the verification results and the actual status of the digital system test items, and support the shipowner’s query and records.

8.5.2.24 The data-driven verification system should support the retrieval of the historical test, verification results and processing methods.

8.5.2.25 Version change management shall be provided for the data-driven verification system.

8.5.2.26 The documents as shown in Table 8.5.2.26 shall be provided for data-driven verification.

Documents **Table 8.5.2.26**

Name	Description	Remarks
Design theory description	Describe the data-driven verification method, data interface and output form	
Function description	Describe the functions and capabilities of the data-driven verification system	
Monitoring system files	Mainly includes: 1. System topology diagram 2. User interface description	
Operation manual	Describe the operation steps and configuration methods of the data-driven verification system	
Test report	Including the test reports on the functions, security etc. of the data-driven verification system	
Process description file	Mainly includes: 1. Verification process description 2. Personnel training and qualification approval requirements 3. Test and verification scope description 4. Calibration process of the sensor and data collection equipment 5. Instructions for management and transmission of the test and verification information	
Version change management description	Record the verification scope, functions and other revisions	

Chapter 9 Verification and Validation of the Digital System

Section 1 General Provisions

9.1.1 General requirements

9.1.1.1 The object of the verification and validation is the digital system.

9.1.1.2 The inspection includes verification of the digital system and assessment of the verification methods.

9.1.1.3 The verification of the digital system involves the verification of the sensor data, status data and result data used by the digital system. Corresponding data should be provided as required to complete the verification of the digital system.

9.1.1.4 The relevant verification data submitted to CCS by the applicant shall be automatically collected, and the data collection shall not depend on the ability or intervention of the operator, and the data cannot be modified.

9.1.1.5 The format, scope and quality of the data (verification evidence) submitted to CCS should satisfy the requirements of CCS to implement effective targeted assessment and verification of the digital system.

9.1.2 Verification and validation process

9.1.2.1 The digital system of ships and offshore installations may be inspection according to the general inspection process shown in Figure 9.1.2.1.

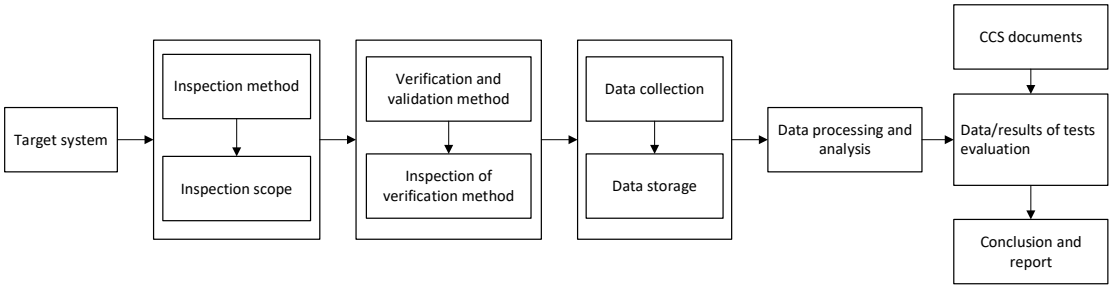

Figure 9.1.2.1 General Digital System Inspection Process

9.1.2.2 The verification and validation of the digital system should be based on engineering assessment, risk assessment and direct assessment.

9.1.2.3 The verification method shown in Figure 9.1.2.1 shall meet the requirements of Section 8.5.2 of this guideline.

9.1.2.4 The procedures of the digital system verification and validation of ships and offshore installations should be traceable.

9.1.2.5 The raw data collected during the verification process of the digital system of ships and offshore installations should be provided to CCS.

9.1.2.6 The compatibility of the digital system in the actual operating environment shall be verified.

9.1.2.7 The function and performance of the actual running digital system shall be verified.

9.1.2.8 Quantitative indicators shall be provided for the expected function and performance requirements of the digital system.

9.1.2.9 Check whether the basic assumptions of the digital system comply with the reality, such as the actual operating environment temperature, etc.

9.1.2.10 Applicant shall negotiate with CCS to determine the list of specific monitoring, test and inspection items for the digital system.

9.1.2.11 The data or models of data-driven applications shall be evaluated according to the requirements of direct assessment in Section 8.4.2 of this guideline.

9.1.2.12 During verification, the quantitative and qualitative assessment of risks should be carried out based on the actual conditions (such as completeness of information, changes in functional requirements, etc.).

9.1.2.13 As for risk assessment, it is required that the risks and uncertainties of the digital system should be identified, and the foreseeable hazards, causes, consequences and potential risk control measures should be recorded.

9.1.2.14 Risk assessment mainly involves three factors of personal safety, asset protection and environmental protection.

9.1.2.15 The system integration and operational risks shall be assessed according to the provisions of Section 8.2.2 of this guideline, and the risk management and control measures shall be specified. The main assessment items shall include:
(1) Risk assessment methods;
(2) The risks of system installation, integrated interface, commissioning, operation and shutdown, and the risks of the system associated with its operation;
(3) Update of preliminary risk assessment results and analysis of risk control measures.

9.1.2.16 The verification method of the digital system with self-verification capability shall be evaluated and approved by CCS.

9.1.3 Result verification

9.1.3.1 The operation results of the digital system should be verifiable. According to the operation of the system, the verification of the operation results can be submitted to CCS for verification in two ways:
(1) After trial operation of the system, the inspection, model, test data, and expected results shall be submitted to CCS for verification, and the results shall meet the requirements of CCS;
(2) Certain data shall be accumulated for verification based on the actual operation results of the system, and the results shall meet the requirements of CCS.

Section 2 Verification and Validation Requirements

9.2.1 Implementation of verification and validation

9.2.1.1 The digital system should have corresponding product certificate.

9.2.1.2 Trial operation should be completed before implementation of the verification and validation. The applicant shall apply to CCS for implementation of the verification and validation and submit

the report on the implementation of the trial operation.
(1) If the applicant fails to provide relevant data for digital system operation results verification such as models and test data, expected results or actual operation data, CCS shall conduct test and verification based on the digital system integration operation in Section 7.4 of the guideline;
(2) If the applicant can provide relevant information for results verification based on the operation of the digital system, CCS shall conduct verification according to the relevant contents in Section 9.1 of this chapter on the basis of the test and verification in Section 7.4 of this guideline.

9.2.1.3 The marine surveyor shall confirm that the results meet the CCS requirements, and issue different certificates according to the verification conditions.

9.2.2 Annual inspection

9.2.2.1 After implementation of the digital system, annual verification shall be performed based on the annual/intermediate inspection of ships and offshore installations where the digital system is located to ensure consistency between the digital system and the physical system.

9.2.2.2 During annual inspection, the shipowners or ship management companies should submit an annual usage report to the test unit of CCS, which should at least include:
(1) Operation and maintenance records of the digital system;
(2) Records of results of services provided by the digital system;
(3) Operation and maintenance records of the physical entity corresponding to the digital system, including all component abnormalities and failure records:
(4) Maintenance plan of the physical entity corresponding to the digital system (if applicable) .

9.2.2.3 During annual inspection, in addition to reviewing the annual report submitted by the shipowners or ship management companies, the following items should also be checked:
(1) Confirm and check the functional integrity of the digital system;
(2) Check and confirm the operating conditions of the digital system (such as sensor input conditions, model constraints, etc.);
(3) Confirm and check the self-inspection report of the digital system;
(4) Check and confirm the computer system corresponding to the digital system, and check whether it works normally;
(5) Check the performance and maintenance records of the physical entity corresponding to the digital system (if applicable);
(6) Check the detailed records of the failures of the physical entity corresponding to the digital system (if applicable);
(7) Check the maintenance records of the physical entity corresponding to the digital system (if applicable);
(8) According to the review and inspection results, the marine surveyor shall issue the corresponding review report, and the certificate of the digital system shall be kept.