International Standard

ISO 19847

Ships and marine technology — Shipboard data servers for sharing field data at sea

Navires et technologie maritime — Serveurs de données embarqués pour partager les données de terrain en mer

Second edition
2024-02

Reference number
ISO 19847:2024(en)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

ISO draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents. ISO shall not be held responsible for identifying any or all such patent rights.

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 8, *Ships and marine technology*, Subcommittee SC 6, *Navigation and ship operations*.

This second edition cancels and replaces the first edition (ISO 19847:2018), which has been technically revised.

The main changes are as follows:

- In Clause 7, a specific security requirement on the shipboard data server has been added.
- In Clause 8, a test standard in a tabular arrangement of test objectives, conditions, methods, and test criteria has been added.
- In Annex H, implementation requirements for the calculation function have been added.
- In Clause 5, additional examples of an output statement for reporting status have been added.
- In Clause 6, an additional output function with JSON data has been added.
- In Annex C, additional query parameters to designate date and time, search for partial matches of Local IDs and obtain down sampling data have been added.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

Shipboard computer applications to ensure ships operate safely and efficiently are becoming increasingly popular.

These applications require access to data which is provided by shipboard machinery and equipment.

Navigational instruments can use the IEC 61162 series of standards when exchanging data, but access to other shipboard machinery and systems to obtain data has not yet been standardized.

For the purpose of sharing field data at sea, including non-standardized machinery data, this document specifies requirements for performance, function, service and safety for the shipboard data server that stores data from shipboard machinery and equipment, and sends stored data off the ship.

The shipboard data server is connected to an information network that is specified in ISO 16425. The requirements for cyber security on the shipboard data server are specified.

Ships and marine technology — Shipboard data servers for sharing field data at sea

1 Scope

This document specifies requirements for shipboard data servers that are used to collect data from other shipboard machinery and systems, and to further share the collected data in a safe and efficient manner.

This document specifies communication protocols with reference to the data structure of ISO 19848.

This document is intended for users and developers of shipboard data servers, as well as users and developers of systems that record data on, or retrieve data from, shipboard data servers.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 8601-1, *Date and time — Representations for information interchange — Part 1: Basic rules*

ISO 16425, *Ships and marine technology — Guidelines for the installation of ship communication networks for shipboard equipment and systems*

ISO 19848:2024, *Ships and marine technology — Standard data for shipboard machinery and equipment*

IEC 60092-504:2016, *Electrical installations in ships — Part 504: Special features — Control and instrumentation*

IEC 60945, *Maritime navigation and radiocommunication equipment and systems — General requirements — Methods of testing and required test results*

IEC 61162-1, *Maritime navigation and radiocommunication equipment and systems — Digital interfaces — Part 1: Single talker and multiple listeners*

IEC 61162-450:2018, *Maritime navigation and radiocommunication equipment and systems — Digital interfaces — Part 450: Multiple talkers and multiple listeners — Ethernet interconnection*

IEC 62923-1, *Maritime navigation and radiocommunication equipment and systems — Bridge alert management — Part 1: Operational and performance requirements, methods of testing and required test results*

IEC 62923-2, *Maritime navigation and radiocommunication equipment and systems — Bridge alert management — Part 2: Alert and cluster identifiers and other additional features*

INTERNET SOCIETY (ISOC) RFC 3986, *Uniform Resource Identifier (URI): Generic Syntax [online]. Edited by T. Berners-Lee, W3C/MIT, R. Fielding, Day Software, L. Masinter and Adobe Systems. January* 2005 *[viewed 2023-05-13]. Available at* https://datatracker.ietf.org/doc/html/rfc3986

IACS Rec.166, *Recommendation on Cyber Resilience*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

- ISO Online browsing platform: available at https://www.iso.org/obp
- IEC Electropedia: available at https://www.electropedia.org/

3.1
actual recorded data
actual (sensor) data acquired from *data providers* (3.10) and recorded to the *shipboard data server* (3.38)

3.2
Alias ID
symbol to refer to one or more *Local IDs* (3.24) with different names

3.3
Alias List
list defining a list of virtual *Data Channel IDs*

Note 1 to entry: The Data Channel ID is the identifier for the *Data Channel* (3.7) that identifies Data Channel universally and on-board a ship. There are three types of Data Channel ID: Universal ID, *Local ID* (3.24) and Short ID.

3.4
calculation function
functions to provide calculated data (e.g. min, max and average)

Note 1 to entry: The calculated data provided is in accordance with the calculation data structures specified in ISO 19848.

3.5
calculation list
list which defines the *calculation function* (3.4) that executes calculations, and the input and output parameters given to the calculation element

3.6
comma-separated value
CSV
method of storing tabular data in plain text in a file in which each row of the file forms a data record and in which fields within one data record are separated by a comma character

3.7
Data Channel
virtual channel for data transmission from shipboard machinery and equipment to the *shipboard data server* (3.38), defining static properties of data

[SOURCE: ISO 19848:2024, 3.5]

3.8
Data Channel List
list of definitions for the *Data Channel* (3.7) that define the Data Channel ID and the Data Channel Property, and is shared through the *shipboard data server* (3.38)

Note 1 to entry: The Data Channel Property shows attributes of the *Data Channel* (3.7), such as units, ranges and others.

[SOURCE: ISO 19848:2024, 3.7]

3.9
Data Channel Type
identification of the types of *Data Channels* (3.7), such as row numeric value, average value, alarms and status

Note 1 to entry: See ISO 19848:2024, 5.2 a).

3.10
data provider
equipment that provides (sends) data to the *shipboard data server* (3.38) and has interfaces for providing data

3.11
Data Source Information
description of communication protocols and formats in which a *data provider* (3.10) sends data

3.12
data sample
measurement datum that has a timestamp

3.13
eXtensible markup language
XML
text-based data description language used for exchanging data on the Internet

[SOURCE: ISO 19848:2024, 3.10]

3.14
file transfer protocol
FTP
protocol for transferring files between a server and clients

3.15
file transfer protocol over SSL/TLS
FTPS
protocol that encrypts data transmitted and received by *file transfer protocol* (3.14) with a secure sockets layer (SSL) or transport layer security (TLS)

3.16
Function ID
identification for the calculation function with which the *shipboard data server* (3.38) performs the calculation

3.17
hypertext transfer protocol
HTTP
communication protocol used to exchange hypertext markup language (HTML) or other contents on the internet

3.18
hypertext transfer protocol over SSL/TLS
HTTPS
protocol in which web servers and clients encrypt data transmissions

3.19
internet control message protocol
ICMP
protocol consisting of communication rules that are used for purposes such as notifications of errors in the processing of datagrams, and notifications of information relating to communication

Note 1 to entry: This protocol is according to RFC 792.

3.20
internet group management protocol
IGMP
protocol which is used on IPv4 networks to report multicast group memberships

Note 1 to entry: This protocol is according to RFC 1112, RFC 2236 and RFC 4604.

3.21
input parameter
variable which gives information to the calculation function which is needed to perform the calculation

3.22
java script object notation
JSON
open and text-based exchange format

Note 1 to entry: Data transmitted in JSON formats make it easy to read and write (for humans), parse and generate (for computers).

Note 2 to entry: It is similar to *eXtensible markup language* (3.13).

3.23
Local Data Name
identifier for *Data Channels* (3.7), which is named in accordance with a *Naming Rule* (3.28)

Note 1 to entry: The syntax of the identification string shall be disclosed and precisely defined using the augmented Backus-Naur form (ABNF).

Note 2 to entry: See ISO 19848:2024, 5.1.3 b).

3.24
Local ID
identification of an on-board *Data Channel* (3.7) locally, consisting of a *Naming Rule* (3.28) and a *Local Data Name* (3.23)

3.25
management data
catalogues that allow access to, and interpretation of, recorded data

EXAMPLE Timestamped *Data Source Information* (3.11), *Data Channel List* (3.8) and *Alias List* (3.3).

3.26
malware
malicious code
software used or created to disrupt computer operation

[SOURCE: IEC 61162-460:2018, 3.23]

3.27
message queuing telemetry transport protocol
MQTT protocol
protocol for machine-to-machine (M2M)/Internet of Things (IoT) connectivity designed as an extremely lightweight publish/subscribe messaging transport; it is also one of the streaming protocols

Note 1 to entry: It is standardized by the Advancing Open Standards for the Information Society (OASIS).

3.28
Naming Rule
set of requirements that define a naming scheme (or an identification scheme) for components and systems on-board the ship

Note 1 to entry: See ISO 19848:2024, 5.1.3 a).

3.29
network file system
NFS
distributed file system and a protocol for distributed file systems and other protocol specifications

Note 1 to entry: This system is defined by RFC 1094, RFC 1813 and RFC 3530.

3.30
owner
specified person who can restrict editors and users

3.31
output parameter
variable which gives destinations to the calculation function to which calculation results are output

3.32
removable external data source
REDS
user removable non-network data source

EXAMPLE Compact Disc (CD), USB memory stick, Bluetooth®[1] devices

[SOURCE: IEC 61162-460:2018, 3.32]

3.33
REST API
program invocation convention for using web systems from outside, developed in accordance with the architectural style called representational state transfer (REST)

Note 1 to entry: Resource operations are designated by *HTTP* (3.17) sources. Results are sent back in *XML* (3.13), *JSON* (3.22) and other formats.

3.34
secure file transfer protocol
SFTP
protocol that uses the *SSH* (3.35) protocol to securely transfer files between computers

3.35
secure shell
SSH
cryptographic protocol that allows secure communications over an unsecured network

3.36
session
stateful or stateless dialogue established to exchange data between a *shipboard data server* (3.38) and shipboard equipment or systems

3.37
server message block
SMB
protocol for sharing files and printers among several Windows®[2] computers in networks

3.38
shipboard data server
information hub of a ship that stores data from shipboard machinery and equipment, shares data at sea including machine data, and sends stored data outboard

[SOURCE: ISO 19848:2024, 3.18]

3.39
syslog
standard for message logging

[1] Bluetooth® is the trademark of products supplied by Bluetooth Special Interest Group. This information is given for the convenience of users of this document and does not constitute an endorsement by ISO of the product named. Equivalent products may be used if they can be shown to lead to the same results.

[2] Windows® is the trademark of products supplied by the Microsoft Corporation. This information is given for the convenience of users of this document and does not constitute an endorsement by ISO of the product named. Equivalent products may be used if they can be shown to lead to the same results.

4 Abbreviated terms

AMS	alarm monitoring system
BWMS	ballast water management system
CSV	comma-separated value
ECDIS	electronic chart display and information system
FTP	file transfer protocol
FTPS	file transfer protocol over SSL/TLS
GNSS	global navigation satellite system
HTML	hypertext markup language
HTTP	hypertext transfer protocol
HTTPS	hypertext transfer protocol over SSL/TLS
IT	Information technology
JSON	java script object notation
M/E	main engine
MQTT	message queuing telemetry transport
NFS	network file system
OPC UA	open platform communications unified architecture
OT	operational technology
REDS	removable external data source
RFC	request for comments
SFTP	secure file transfer protocol
SMB	server message block
SSH	secure shell
SSL	secure sockets layer
TCP	transmission control protocol
TLS	transport layer security
UDP	user datagram protocol
URI	uniform resource identifier
UTC	coordinated universal time
UTM	unified threat management
VDR	voyage data recorder
XML	eXtensible markup language

5 General requirements for the shipboard data server

5.1 Function and performance of the shipboard data server

5.1.1 Processing performance

5.1.1.1 General

Manufacturers supplying the shipboard data server shall specify how much data their products can process. If the product exceeds the amount of data that can be processed, it is necessary to notify the requesting party by returning the status code.

5.1.1.2 Input data processing performance

The shipboard data server using the request-response transport service shall process input data from a set of 30 data samples per session, within one second, from at least five simultaneous sessions (e.g. VDR, GNSS, alarm and monitoring systems, ballast systems and cargo systems). See Figure 1.

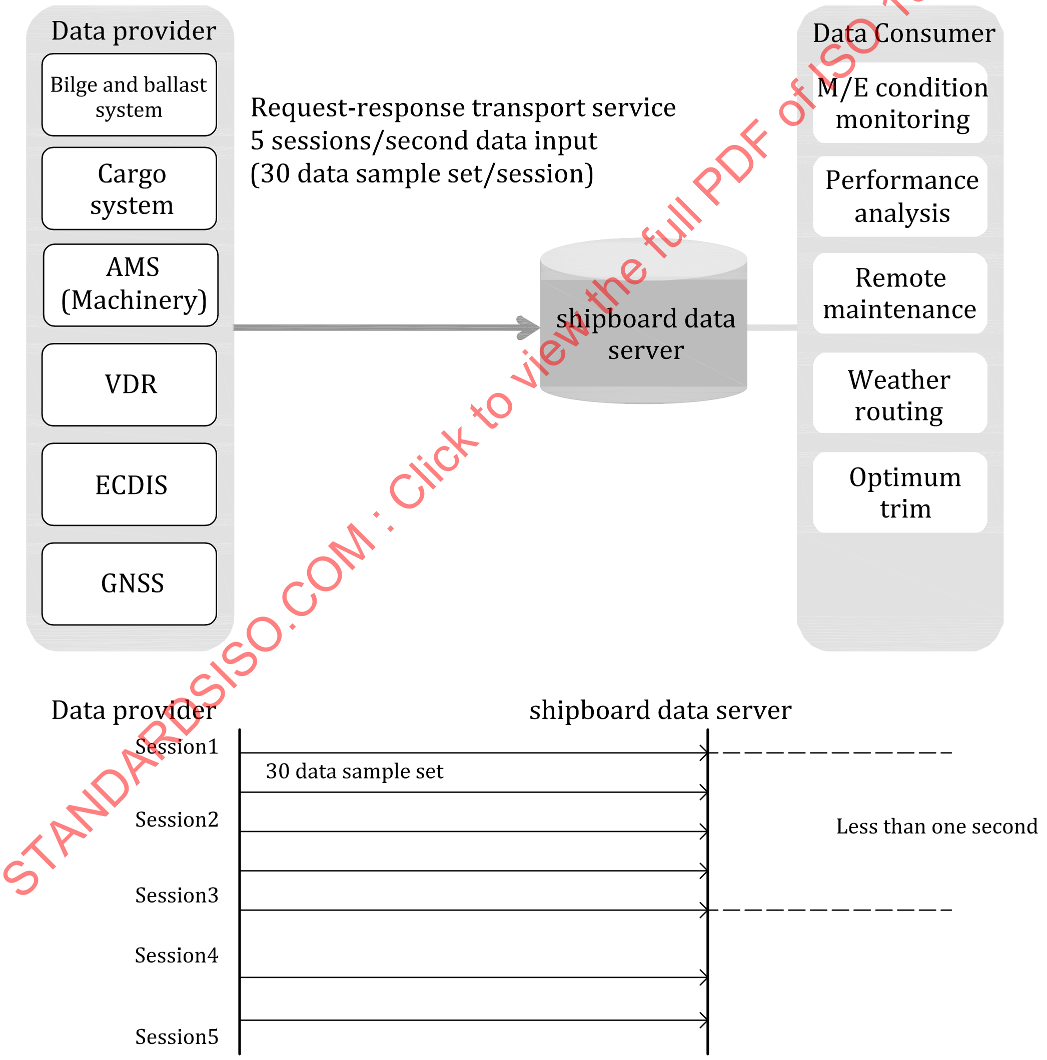


Figure 1 — Input data processing performance requirement

5.1.1.3 Output data processing performance

When the shipboard data server is using the request-response transport service:

- it shall be able to process the read request of a set of 30 data samples per session, from at least five sessions simultaneously (e.g. main engine condition monitoring, weather-routing, optimum trim, remote maintenance and performance analysis);
- the five sessions shall be processed in less than five seconds; and
- the size of the database shall meet the manufacturer’s limit.

When the shipboard data server is using the file transport service:

- it shall have a processing performance to respond to the read requests of a set of 30 data samples per session;
- at least one session shall be processed in less than five seconds; and
- the size of database shall meet the manufacturer’s limit.

See Figure 2.

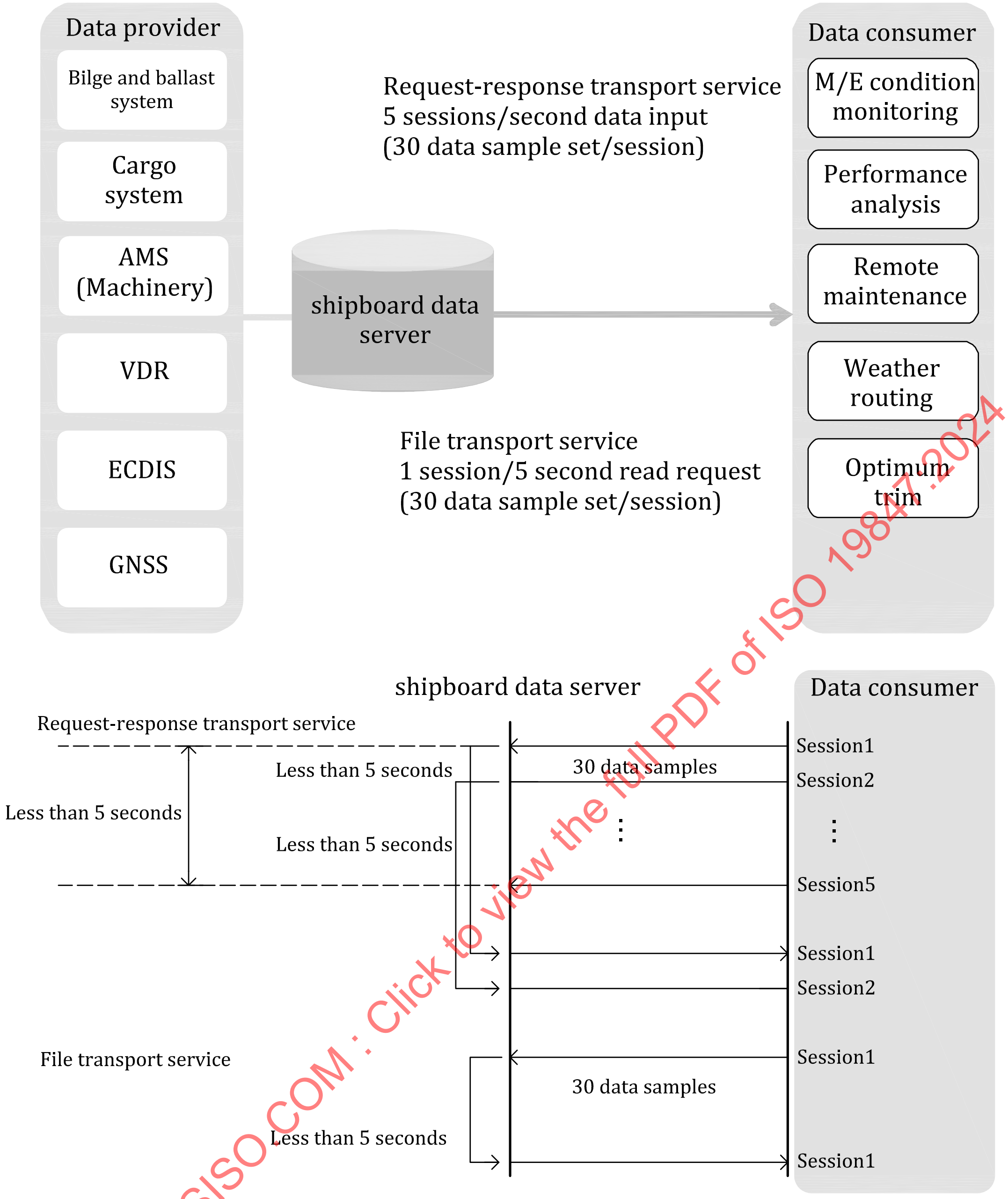


Figure 2 — Output data processing performance requirement

5.1.1.4 Streaming transport processing performance

When the shipboard data server is using the streaming transport service:

- it shall have a processing performance to input a set of 150 data samples in less than one second from at least one session; and
- it shall have a processing performance to output a set of 150 data samples in less than one second, from at least two sessions of a set of 150 input data samples (e.g. condition monitoring and performance analysis system).

See Figure 3.

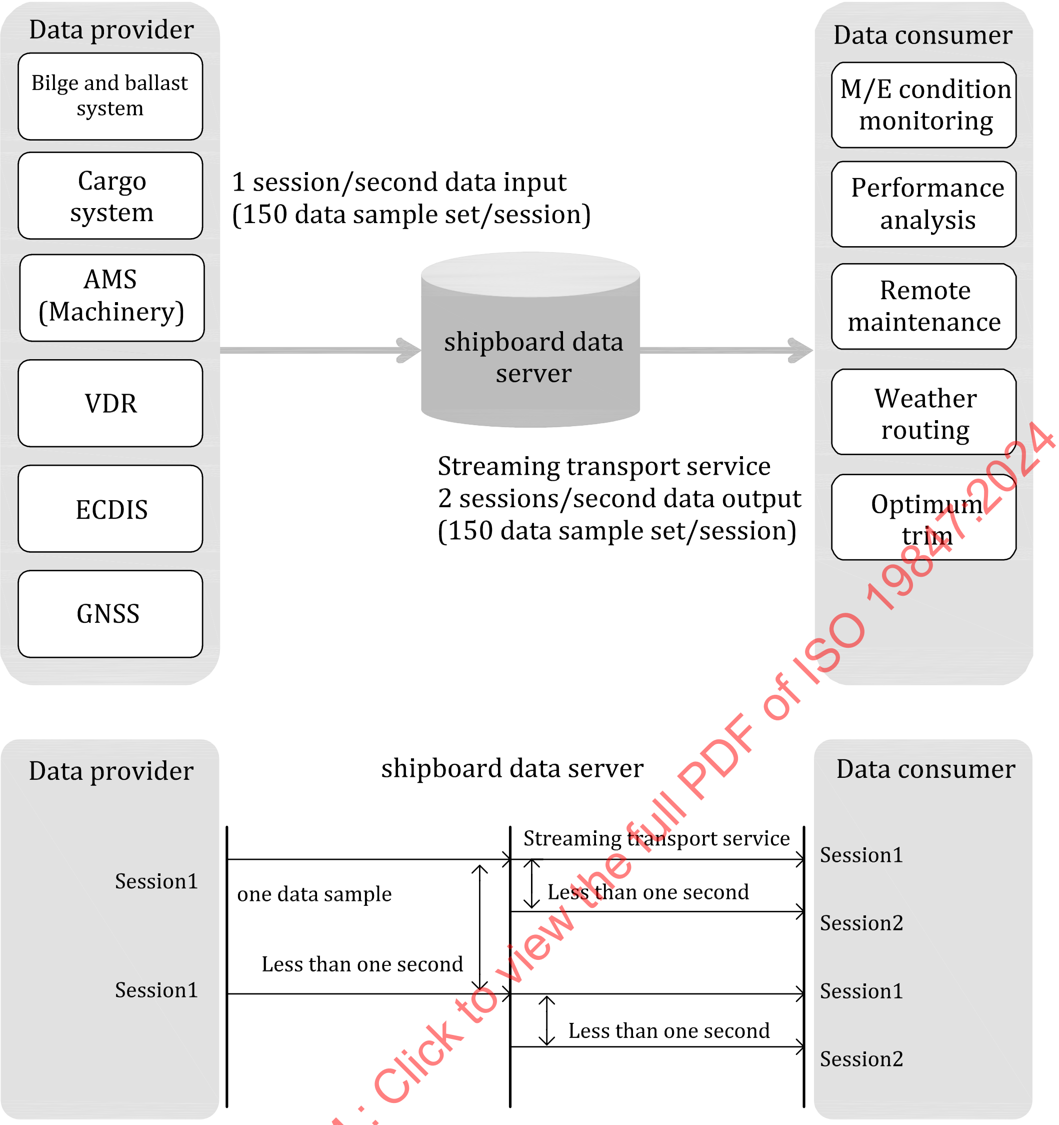


Figure 3 — Streaming transport processing performance requirements

5.1.2 Storage function

The shipboard data server shall be able to store input data (defined in 6.3.2) for at least 30 days.

The manufacturer shall specify, in a user or installation manual, the amount of storage space required per record. Information on the total storage capacity within the ship data server shall also be provided.

The shipboard data server shall provide the means to assist the user in estimating if the total storage capacity of the shipboard data server is sufficient for the required time period. In the manual or the help file, the manufacturer shall give instructions on how to estimate the storage capacity.

NOTE The shipboard data server can have a redundant function to protect management data and actual recorded data (e.g. redundant array of independent disks [RAID] 1, 3 and 5 systems).

5.1.3 Interface function

The shipboard data server shall be able to provide data input and output functions (see 6.3).

The shipboard data server shall have one or more ethernet interfaces where data are transmitted at 100 Mbit/s or greater.

NOTE The shipboard data server can also have other interfaces capable of serial communications or other means of inputting data.

5.1.4 Condition monitoring function

The shipboard data server shall be able to monitor the status of the following conditions:

a) system failure of shipboard data server processor;

b) failure to access storage device;

c) failure of recording interface;

d) loss of UTC synchronization; and

e) storage device that is full or has insufficient capacity to store configured records for up to 30 days.

The shipboard data server shall be able to report the above statuses to other systems on-board (see 5.1.7) and may provide local indications for these statuses.

5.1.5 Data backup and restoration functions

The shipboard data server shall have backup and restoration functions for:

- management data, and
- actual recorded data.

5.1.6 Function to protect against unauthorised access

The shipboard data server shall have protected settings, management data, actual recorded data and other items from accidental and/or unauthorised access. See Clause 7.

5.1.7 Status reporting

The shipboard data server shall be provided with an interface to provide status report to the ship's personnel. The interface shall at least consist of one relay contact output and an indicator driven by relay, capable of indicating normal/abnormal status of the shipboard data server to the ship's personnel. The relay and the indicator can be replaced by other means, as specified by the manufacturer, which allow the ship's personnel to identify a related failure of the shipboard data server.

For example, an alternate method to the relay and the indicator can be based on the provision of a specific status display at the shipboard data server or on generating alerts in the shipboard data server and reporting the alerts to other systems on-board by employing sentences ACN, ALF, ALC, ARC and HBT from IEC 61162-1.

If the shipboard data server is capable of providing the alerts to the ship's personnel by using the above sentences, it shall comply with IEC 62923-1 and IEC 62923-2.

When an alert occurs and a status report is made using the ALF statement, the following statement shown in the example below will be output. If alerts in Table 1 are provided, they shall use the priority, category, escalation and alert identifier in Table 1.

EXAMPLE $IIALF,1,1,0,223344.55,B,C,N,,3009,1,1,0, Recording failed*hh<CR><LF>

Table 1 — Alert list

Alert identifier	Alert title[a] (example)	Alert description text[a] (example)	Pri	Cat	Escal
3063	System fault	The system was stopped. Restart the system. If not recovered, schedule maintenance.	C	B	-
3009	Recording failed	No access to storage device, replace storage device to new one.	C	B	-
3003	Lost < Data Provider > [b]	Check the connection to < Data Provider > .	C	B	-
3156	Lost UTC sync	Recorded timestamp may deviate from UTC. Check the connection to the < Time Source > [c].	C	B	-
3133	Data store low	Recording will be stopped in 30 days. Backup old data and delete it until then.	C	B	-

[a] The given text (as an example) may be adjusted according to the implementation.

[b] < Data Provider > in the above list shall be changed according to the data provider’s name.

[c] < Time Source > may be GNSS or NTP server.

Key

Pri	Priority
Cat	Category
Escal	Escalation

5.2 Environmental performance of shipboard data server

5.2.1 Power-supply performance

The shipboard data server shall satisfy the test requirements of the power supply performance specified in IEC 60092-504.

Refer to IEC 60092-504:2016, Table 1, No.4 a), Electric of power supply variations, and No.4 b), Power supply failure.

The shipboard data server, management data and actual recorded data shall be protected from damage, even during temporary loss of electricity.

5.2.2 Vibration-resistant feature

The shipboard data server shall satisfy the test requirements of the vibration test specified in IEC 60092-504.

Refer to No.10, Vibration, of IEC 60092-504:2016, Table 1.

5.2.3 Requirement for electromagnetic immunity and emission

The shipboard data server shall satisfy the test requirements of the electromagnetic immunity tests specified in IEC 60092-504. Refer to IEC 60092-504:2016, Table 1, Tests No. 13, 14, 15, 16 and 17.

The shipboard data server shall satisfy the test requirements of the electromagnetic emission tests specified in IEC 60092-504. Refer to IEC 60092-504:2016, Table 1, Tests No. 19 and 20.

The electromagnetic immunity and emission tests shall be conducted according to the installation location. For example, if installed on a ship bridge, the requirements of IEC 60945 shall be met. If installed in an engine control room, the requirements of IEC 60092-504 shall be met.

5.2.4 Temperature and humidity resistant requirements

The shipboard data server shall satisfy the following requirements in IEC 60092-504:2016, Table 1:

- No.6, cold with gradual change of temperature;
- No.7, dry heat with gradual change of temperature; and
- No.8, damp heat cyclic.

Where electrical equipment is installed within environmentally controlled spaces, the ambient temperature for which the equipment is suitable may be reduced from 45 °C and maintained at a value not less than 35 °C.

Also, according to the temperature conditions, the location of installation shall be drawn in the installation manual.

For setting up the environmentally controlled space, refer to the following:

- the equipment shall not be used for emergency services;
- temperature control is achieved using at least two cooling units arranged so that if one of the cooling units fails, the remaining unit(s) is capable of satisfactorily maintaining the design temperature;
- the equipment can be initially set to work safely within an ambient temperature of 45 °C until such a time that the lesser ambient temperature may be achieved; the cooling equipment shall be rated for an ambient temperature of 45 °C; and
- audible and visual alerts are provided, at a continually manned control station, to indicate any malfunction of the cooling units.

5.3 Installation requirements for shipboard data server

5.3.1 Environment requirements

The manufacturer shall define the surrounding environment requirements for installing the shipboard data server in installation manuals.

5.3.2 Requirements for maintenance areas

The manufacturer shall define the work areas that are needed for maintenance and provide details in installation manuals.

5.3.3 Requirement for networks and network security

The shipboard data server shall be installed within networks that comply with network security related requirements given in ISO 16425.

NOTE ISO 16425 sets network security related requirements on:

- network system design,
- network interface for shipboard equipment and systems,
- protection from malware, and
- protection from illicit access and equipment protection.

6 Data input/output and data management on shipboard data server

6.1 General

The shipboard data server shall have the following functions for data input/output and data management:

a) data management function;

b) data input and output functions;

c) alias function;

d) data calculation function;

e) log management function.

6.2 Data management function

6.2.1 General

The data management function comprises time stamping of the Data Channel List, the Data Source Information, and the Alias List based on the system clock and administration of management data.

The shipboard data server shall accept change requests in management data only when the requests are received from authorized sources. See 6.3.

6.2.2 Management of system clock

The system clock of the shipboard data server shall be managed as specified below to add a precise timestamp to the data.

a) The system clock of the shipboard data server shall be synchronised with UTC.

b) Drift in the system clock of the shipboard data server shall be no more than one second per hour.

c) To ensure that relative timings are determined within a resolution of one second, all data items shall be recorded with a time index derived from the shipboard data server system clocks with a resolution of 0,5 s or less.

d) The shipboard data server shall indicate state of loss of UTC synchronization (see 5.1.4).

NOTE Network time protocol can be used for UTC synchronization of the shipboard data server.

6.2.3 Management of Data Channel List

The shipboard data server shall have a management function of the Data Channel List that meets the following requirements.

a) The Data Channel List shall be able to be registered, revised, deleted and referred by data input and output functions.

b) When the Data Channel List is added, updated or deleted, the shipboard data server shall record the changed information with date and time.

c) The shipboard data server shall be able to clearly indicate the Data Channel List which is currently used for recording and output of recorded data. This may be done by offering a function for showing the current Data Channel List to the user or by describing the information in the user or installation manual.

d) The shipboard data server shall require proper authentication before allowing management or alteration of the Data Channel List.

6.2.4 Management of Data Source Information

The shipboard data server shall have a management function of the Data Source Information that meets the following requirements and guidance.

a) The Data Source Information shall be able to be added on, updated and deleted by direct editing or data input functions.

b) When the Data Source Information is added on, updated or deleted, the shipboard data server shall record the changed information with date and time.

c) The shipboard data server may be able to indicate what data sources are currently configured for the recording of data. This may be done by offering a function for showing the current data source configuration list to the user or by describing the information in the user or installation manual.

Refer to Annex F for the Data Source Information.

6.2.5 Management of Alias List

The shipboard data server shall have a management function for the Alias List that meets the following requirements.

a) An Alias List shall be able to be registered, revised, deleted and referred by direct editing or data input and output functions.

b) When an Alias List is added, updated or deleted, the shipboard data server shall record the changed information with date and time.

c) The shipboard data server shall be able to clearly indicate the Alias List which is currently used for recording and output of recorded data. This may be done by offering a function for showing the current Alias List to the user or by describing the information in the user or installation manual.

d) The shipboard data server shall require proper authentication before allowing management or alteration of the Alias List.

Refer to 6.4 for alias function and to Annex B for Alias List.

6.3 Data input and output functions

6.3.1 General

The shipboard data server shall have interface functions that meet the requirements in a) to d) below. For data input and output function concepts, refer to Figure 4.

The shipboard data server shall provide an access control method to prevent unauthorised access to actual recorded data and management data. Annex G provides examples of access control methods.

a) The shipboard data server shall use the ethernet interface when inputting and outputting data.

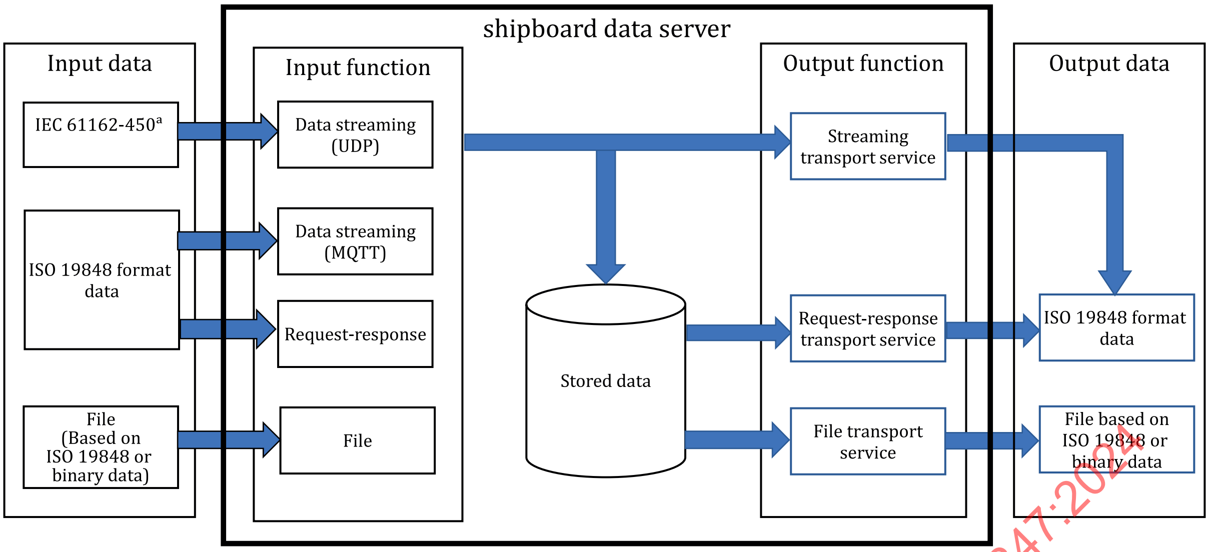
b) The shipboard data server shall offer the following data transport services having data input and output functions:

   - request-response data transport services;
   - streaming data transport services.

c) The shipboard data server shall be provided with file transport services having data input and output functions.

d) The data interface functions of the shipboard data server shall be defined in the Data Source Information.

   Examples of the Data Source Information for data interfaces are shown in Annex F.



Key

[a] IEC 61162-450 handles only "IEC 61162-1 formatted sentences", not binary or image data.

Figure 4 — Data input and output concept model

6.3.2 Input function

The shipboard data server shall have an input function that meets the following requirements.

a) The shipboard data server shall be able to receive data that comply with the data format specified in ISO 19848, the sentence specified in IEC 61162-450:2018, 7.2 using the IEC 61162-1 formatted sentence and the file based on ISO 19848, all of which are defined in the Data Source Information of the shipboard data server.

The data transmitted as specified in IEC 61162-450 is not guaranteed to be reachable because it uses the UDP multicast protocol.

NOTE The shipboard data server is not a navigational device and does not necessarily meet the other requirements of IEC 61162-450.

The shipboard data server may accept protocols other than those described here as input functions; for example, Modbus TCP, OPC UA and MQTT. If the shipboard data server receives data from such data sources, they shall be defined in the Data Source Information.

b) When input data do not have UTC timestamps, the shipboard data server shall timestamp all recorded data based on the system clock of the shipboard data server. The shipboard data server may additionally record external timestamps and their related UTC synchronization status information, if provided by data providers.

c) The shipboard data server shall receive data that comply with the data format specified in ISO 19848 using the protocol defined in Annex C.

d) The shipboard data server shall receive data that comply with the data format specified in ISO 19848 and the sentence specified in IEC 61162-450 using the protocol defined in Annex D.

e) The shipboard data server shall receive the file based on ISO 19848 using the protocol defined in Annex E.

f) The data received with illegal integrity checking information, such as checksum/cyclic redundancy check (CRC), or from a source marked as invalid shall either be stored as received and flagged to be invalid by use of quality coding (see ISO 19848:2024, 5.2 e) or be discarded and logged by the log management function as an entry of invalid information. See 6.6.

- The shipboard data server shall discard received data having no integrity-checking information and which is logged by the log management function as an entry of no integrity-checking information.

g) The data received with quality coding from the source shall be passed on to the Data Consumer by the use of quality coding, See ISO 19848:2024, 5.2 e).

- If the shipboard data server receives data that contains quality information, it shall record that information.
- The quality information recorded in the shipboard data server shall be sent to the Data Consumer using the request-response transport service.
- The value recorded in the shipboard data server may be changed to unified quality coding managed by shipboard data server as long as the meaning of the quality information assigned by the Data Provider is maintained (change of code system).

6.3.3 Output function

The shipboard data server shall conform to the output function of XML specified in ISO 19848:2024, A.2 or JSON specified in ISO 19848:2024, A.3.

In addition, the shipboard data server may have the output function of CSV specified in ISO 19848:2024, A.4.

Also, the shipboard data server shall have an output function that meets the following requirements.

a) The shipboard data server shall be able to send data that comply with ISO 19848:2024, A.2 and the file based on ISO 19848.

b) The shipboard data server shall send data defined in 6.3.2 a) by 6.3.4 and 6.3.5.

c) The shipboard data server shall send the file defined in 6.3.2 a) by 6.3.6.

6.3.4 Request-response data transport service

The request-response data transport services offer a function of processing data which are arrayed in chronological order at a time.

The shipboard data server shall have a request-response data transport service that meets the following requirements.

a) The request-response data transport services shall receive and update one or more data at a time which are arrayed in chronological order.

b) The request-response data transport services shall send data that contain data items and periods requested from shipboard machinery and equipment with this protocol.

c) The request-response data transport services shall receive data from shipboard machinery and equipment with this protocol.

d) The request-response data transport service shall generate a normative XML file defined by ISO 19848:2024, A.2 from data records stored in the shipboard data server and shall then transport the generated file to a location as indicated in the URI-parameter given by the requesting shipboard machinery and equipment in the request.

NOTE The applicable file transport mechanisms are described in 6.3.6.

Protocols for providing request-response data transport services are described in Annex C.

6.3.5 Streaming data transport service

The streaming data transport services offer a function of sending the most recent data at that moment to one or more shipboard machinery and equipment.

The shipboard data server shall have a streaming data transport service that meets the following requirements.

a) The streaming data transport services shall offer a function of putting a timestamp to input data received from shipboard machinery and equipment, and of sending data at that moment to one or more shipboard machinery and equipment.

b) The streaming data transport services shall be able to record data that are specified in Data Source Information and received continuously from shipboard machinery and equipment.

c) The streaming data transport service shall be able to start sending required data when they receive begin commands from shipboard machinery and equipment.

Protocols for providing streaming data transport service are described in Annex D.

6.3.6 File transport service

The file transport services provide a function of data exchange of file formats.

The shipboard data server shall have file transfer function to output the normative XML file that is defined by ISO 19848:2024, A.2. Other file formats may also be supported.

For compatibility with already installed systems, file transport services may save received data files in designated storage location areas defined in the configuration of shipboard data server.

The manufacturer shall describe in the manufacturer's documentation the maximum capacity that can be input and output in a single session.

The shipboard data server shall support HTTP or FTP as file transport services. From the viewpoint of security, the shipboard data server may support HTTPS or FTPS.

When using HTTP(HTTPS), see Annex E. Similarly, when using FTP(FTPS), see RFC 959 or RFC 4217.

6.4 Alias function

6.4.1 General

The alias function provides the ability to simultaneously access one or more Local IDs or Short IDs with one simple name from the actual recorded data. See Figure 5.

The shipboard data server may be provided with an alias function. The alias function is executed by the GET method of the request-response transport service.

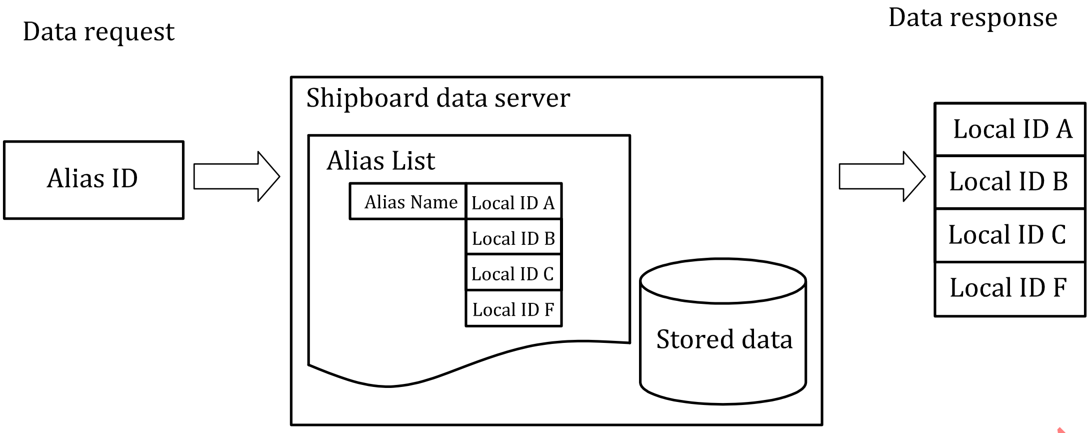


Figure 5 — Alias function

6.4.2 Alias List

The alias function is managed in an Alias List.

Virtual ID registration which is used with the shipboard data server can be done with the Alias List. The virtual ID shall be unique within the shipboard data server.

A virtual ID is called an Alias ID and can have the function of limiting what the user can use.

Deletion of the Alias ID or Alias List does not delete actual recorded data contained in the Alias ID or Alias List.

For details of the Alias List, refer to Annex B.

6.5 Data calculation function

6.5.1 General

The shipboard data server shall have a function to provide calculated data (e.g. min, max and average) in accordance with the calculation data structures specified in ISO 19848.

If an internal calculation function is implemented, its use and examples shall be given in the instruction manual so as not to interfere with user operation.

Examples of an internal calculation function are shown in Annex H.

NOTE Calculated data can be the result of the service agent calculating input data.

For the service agent, refer to Annex A.

6.6 Log management function

The shipboard data server shall record the following events in detail into the system log:

a) history of access: date and time of operational access to the shipboard data server including the result of access control check;

b) history of status change: all changes in statuses described in 5.1.4;

c) history of changes in management data: the Data Channel List, the Data Source Information and adjustment of system clock; and

d) Error information: input data are not recorded because a checksum error or CRC error occurs.

Each system log record shall include the logical name of the shipboard data server and the date and time of the event occurrence.

Log contents shall cover a complete history of all records for at least the last 30 days.

7 Operation requirements

7.1 General

The shipboard data server shall be protected from the following logical threats — those which may damage software systems, data and networks without damaging the hardware — through on-board and off-board network systems, as well as physically connected shipboard systems.

a) Malware infection from shipboard systems.

b) Interruption and discontinuation of network services by large-volume broadcast traffic and/or internet control message protocol (ICMP) and/or internet group management protocol (IGMP) packets.

c) Deletion and falsification of internal files by remote access.

The shipboard data server shall be protected from physical threats of direct access from removable devices, interfaces and other factors with which they are equipped.

The shipboard data server should be installed in controlled areas.

7.2 Protection from logical threats

7.2.1 Access control

7.2.1.1 General

The shipboard data server shall have a system to identify and authorize users to control operations and use resources. When users are appropriately authorized, the shipboard data server shall allow only those users to conduct operations and use resources granted by their authorization.

To control operations, the shipboard data server shall have at least two types of authority: one covering general users and one covering administrators with maintenance modes. It is necessary to identify users with identification, called accounts. To authenticate user accounts, it is necessary to introduce authentication with passwords and/or physical keys, or to adopt multifactor authentication. In case of the latter, it is necessary to combine passwords and keys. As an authentication procedure, users' physical locations may be used. When they are used, however, the procedure shall be applied to both local and remote access. In many cases, access is controlled at a system level, where all users are identified and authenticated. In addition, identification and authentication mechanisms are also adopted at an application level. When users function as groups, user identification and authentication may be carried out on roles and/or groups in some cases.

7.2.1.2 Account management

The shipboard data server shall provide functions of support so that authorized users can manage all accounts, such as those for adding, activating, changing, deactivating and deleting accounts. Account management tasks include organizing account groups, setting conditions for group memberships and allotting relevant approvals. Application service accounts used for communication between software processes shall have security policies and procedures that are different from those of user accounts. When enhancing security, unified policies for account management shall be followed and developed in the shipboard data server's local components. Default system accounts shall be deactivated or deleted after they have been used for system installation.

7.2.1.3 Identifier management

The shipboard data server shall provide a function to support identification management by users, groups, roles and/or shipboard data server interfaces.

7.2.1.4 User authentication

Mechanisms for user identification and authentication are applied to both general operation and administrator authority modes. User authentication is carried out with one or more of the options described in a) to d) below. When user authentication fails repeatedly, ways to limit the number of attempts shall be provided. To control the number of attempts made over the designated number, for example, a function shall be provided to reject access either for a certain period, or until locks are released by administrators. The shipboard data server shall be able to record the 10 latest approvals either internally or in external syslogs.

a) Passwords

The equipment has alphanumeric keyboards and/or other data entry devices so that complicated passwords can be entered while normal operations are being made. It is necessary to allow user authentication with login information, such as passwords used with users' names and in key cards.

When password-based user authentication is allowed, the following requirements shall be met.

1) passwords shall be case sensitive.

2) passwords for administrator authorities shall be made up of 10 or more letters that include three of the following: arabic numerals, the uppercase and lowercase letters of the alphabet and special characters.

3) passwords for general users shall be made up of eight or more letters that include two of the following: arabic numerals, the uppercase and lowercase letters of the alphabet and special characters.

4) words contained in dictionaries and proper nouns shall not be used; passwords shall be random and meaningless.

5) passwords shall be strictly controlled and not shared with other individuals.

b) Secret keys and other symmetric cryptosystems

When remote-access functions are provided, the requirements set forth in 7.2.3.3 shall be met.

c) Smartcards and other asymmetric cryptosystems

When asymmetric cryptosystems with smartcards and other means are used, cryptographic security levels shall be equal to those for the 2048-bit RSA key or higher.

7.2.1.5 Authenticator feedback

The shipboard data server shall provide a function to obscure authentication information feedback during the authentication process.

7.2.2 Usage control

7.2.2.1 General

The shipboard data server shall be able to control access to operations and resources with authorization granted by authorized users. By confirming whether the necessary approvals are conferred before allowing users to execute functions, usage control prevents unauthorized functions from being executed on the shipboard data server and on the resources managed by the shipboard data server. It also prevents such resources from being accessed.

7.2.2.2 Authorization enforcement

By separating its functions or exercising minimum authorizations, the shipboard data server shall provide a function to exercise authorizations granted to use in all of its interfaces.

7.2.3 Network access

7.2.3.1 Network access

To keep itself from threats from unmanaged networks, the shipboard data server shall be installed in demilitarised zones (DMZs) with 16425-gateway or 460-gateway compliant gateways. The shipboard data server shall halt communication services, except for those specified in 6.3.2 to 6.3.6. The shipboard data server shall also limit usage so that the communication ports of networks that are not used in services cannot be accessed from the outside. The manufacturer shall clarify available port numbers in instruction manuals.

The shipboard data server shall not accept any commands other than those used by the services set forth in 6.3.2 to 6.3.6. The shipboard data server shall provide a function to control the use of mobile codes that it downloads to itself and executes. See ISO 16425 for requirements for protection from threats from unmanaged networks.

7.2.3.2 Remote access

For remote access to the shipboard data server, the shipboard data server shall be installed on the vessel in accordance with the requirements for Category I of IACS Rec.166:2020, 7.6.

7.2.3.3 Use of cryptography

When encryption is implemented, secret keys or other symmetric cryptosystems shall be used. When secret keys are used, they shall essentially be random.

7.2.4 System defence

7.2.4.1 General

System defences are made up of malware infection prevention, firewalls, intrusion prevention and user alerts in preparation for malware and other software infections being detected. They can be provided in accordance with the devices and/or the environments in which the devices are installed. For example, they can be provided by devices which are compliant with IEC 61162-460, which are installed on networks which are compliant with IEC 61162-460 and/or those installed on networks compliant with ISO 16425.

NOTE The ship owner is responsible for disasters and restoration plans, which are included in the ship's integrated safety management plans (ISMPs).

7.2.4.2 Malware protection

Protection from malware is provided with one or more of the following options.

a) Devices compliant with IEC 61162-460.

b) Devices that have removed accessible interfaces that can be penetrated inside by malware.

   Examples are built-in systems that do not have operating systems and those that have physical interfaces that do not allow malware from invading. Examples are IEC 61162-1 serial interfaces or wireless device (frequency) interfaces and specific functions of marine radiocommunication or navigation systems from the International Maritime Organization (IMO) (i.e. interfaces of radio frequency where files cannot be forwarded).

   NOTE "Accessible interfaces" refer to interfaces that can be accessed without tools or keys. Examples include USB ports that are used to load files, serial interfaces or debug ports and network ports.

c) Devices that have accessible interfaces that can be penetrated inside by malware.

When deciding on protection to apply, the manufacturer shall consider risks related to device functions and environments in which devices are designed to be operated. The manufacturer shall provide detailed information on ways to reduce device-related cybersecurity risks. It is necessary to allow access only to the device functions that are required to execute normal operations. For example, reading, writing and executing files are appropriately configured in accordance with functions intended to be used in normal operations. Devices shall provide enhanced functions when they are attacked and/or damaged. All unused interfaces, network ports, services and applications that are not required in normal operations shall be inactivated.

To reduce risks on devices, the following measures are required.

1) Devices shall include software for protection from malware and a function to update protection from malware.

Devices equipped with software for protection from malware shall meet the performance requirements prescribed in 5.1.1, even when they are in normal operation. Where blocklisted anti-malware is used, the manufacturer shall describe in installation and operation manuals how to evaluate the impact on devices of the updating of files for defining anti-malware measures and software, and the conditions for updates to be made. When a certain amount of time has passed since malware protection software was last updated, notices shall be submitted to inform users that the software is outdated. When malware protection software is updated, it shall not be inferior to the performance requirements set forth in 5.1.1. If allow-list anti-malware software is used, the manufacturer's manuals shall be checked for the impact of any changes to the system on the anti-malware software and update the allow list appropriately if necessary.

2) It is necessary to install devices in DMZ with a firewall to protect from malware. For example, firewalls that meet the 460-Gateway requirements and consist of L3 Switch, UTM or 16425-Gateway.

7.3 Protection from physical threats

7.3.1 General

The shipboard data server shall be protected from physical damage, such as theft, natural breakage and intentional destruction. The shipboard data server should be installed in the restricted areas designated in the ISPS Code, Part B, 9.18 and 9.21.[13] When the shipboard data servers cannot be installed in the abovementioned designated restricted areas, protection shall be provided from physical threats, as instructed in this clause. The manufacturer shall include requirements regarding this clause in the installation manual for the shipboard data server.

7.3.2 Installation requirements

As for places to install the shipboard data server, the ship owner shall create policies and develop procedures to control access in accordance with risk assessments. To prevent unauthorised access, the shipboard data server shall be installed in locked rooms, on locked racks, in locked cabinets or in locked consoles. Keys shall be appropriately managed so that only the ship manager has access.

7.3.3 Connection cables

Communication cables intended to be connected to the shipboard data server shall not be casually laid on the floor to keep away from damage and disconnection.

7.3.4 Power source management

Electric-power supply cables intended to be connected to the shipboard data server shall be protected from damage and disconnection.

7.3.5 Interfaces for removable devices

7.3.5.1 General

The number of points with which removable devices are connected shall be the bare minimum for operations and maintenance.

7.3.5.2 Unused connection points

Unused connection points shall be protected from easy access with one or more of the following options:

a) blocks by tools or keys;

b) logical invalidation (which cannot be validated);

c) invalidation with settings requiring authentication.

7.3.5.3 Operation protection

Connection points used for access to data storage shall be configured to permit connection only to data sources identified as USB device class 08h (USB mass storage).

Other connection points (other USB device classes and non-USB devices) shall be blocked from easy access to avoid connection and use of a different device than the one intended, e.g. by means of a tool or a key or by password-protection (disable/enable) in the device set-up.

The manufacturer shall provide information about the technology used and how the connection point fulfils the requirement to limit connection to its intended operation.

7.3.5.4 Executable program file verification

The shipboard data server shall have prohibited all automatic execution from REDS, including auto-run from USB and CD/DVD. Manual execution of any type of file from REDS shall only be possible after passing authentication for accessing the executable content of the REDS. Manual execution shall be possible only for the files which are verified before execution, using digital signature or special keys.

NOTE 1 A digital signature method is based on a private/public key pair. Typically, a hash-function is used, for example the SHA-2 family (use of MD5 and SHA-1 are now discouraged, see ISO/IEC 10118-3.)

NOTE 2 Special keys can be values calculated from the delivered data using a specified function and compared against a known and expected value, both the function and the value being specified by the trusted source or sender.

7.3.5.5 Non-executable data verification

All accessible data in REDS shall be verified using a digital signature or a special key before being used on the equipment.

7.3.6 Protection (others)

The shipboard data server shall protect interfaces that are not used for operations.

7.3.7 Equipment maintenance

To ensure the continuous availability of the shipboard data server, the manufacturer shall write down appropriate maintenance methods in maintenance manuals.

7.4 Software maintenance

7.4.1 General

The shipboard data server shall support a maintenance mode to enable software maintenance.

The maintenance mode is intended to be accessible only by users authorized by the manufacturer or the manufacturer's authorized representatives.

NOTE Authorized users are typically those working for a company that performs installation or after-installation maintenance. They are not necessarily employees of the manufacturer.

7.4.2 Maintenance mode

Restrictions shall be imposed so that the maintenance mode cannot be entered with just single operations, but also:

— with operations with managed keys;

— with administrative authorities approved by users, roles and/or groups;

— and/or on special conditions.

Operations made in the maintenance mode shall be recorded either internally or in external syslogs. Records shall include the following: authentication information with time stamps used when the maintenance mode is entered, as well as operation details and results. There shall be a system to inform users in the maintenance mode of operation results. Also, there shall be a system to end the maintenance mode, when processing is not performed and operations are not made for certain periods during the maintenance mode.

7.4.3 Setting changes

The shipboard data server shall allow users to change its settings, but only in maintenance mode. There shall be a system to import and export Data Source Information and Data Channel List settings.

NOTE In the maintenance mode, Data Source Information and Data Channel List can be added, updated and deleted. The account management function (see 7.2.1.2) and the identification management function (see 7.2.1.3) can also be provided.

7.4.4 Software update

As a measure against vulnerability, the shipboard data server shall have a function to update its software (including the OS, database system, etc.). However, this function may only be performed in the maintenance mode. When the software contains version information; the software versions shall be managed so that traceability is ensured. The software should constantly be kept up to date. When vulnerabilities are found in the software, they shall be restored either online or offline.

The operator's manual shall provide instructions for software maintenance.

The files associated with the maintenance shall be authenticated as applicable.

The execution of a software update shall begin only after successful user authentication. The user identity shall differ from that of users permitted to access maintenance mode.

The equipment shall ask users to confirm the start of the software update. This means that two steps are required before execution of an update: user authentication and obtaining express permission to begin installing the update. Both steps may be performed at the same time.

The user shall be notified if, once initiated, the software update fails to successfully occur.

7.4.5 Failure recovery

The shipboard data server shall have a function to cancel updates and make rollbacks during software maintenance.

7.4.6 Software version information

The shipboard data server shall show at least its software version on a screen, or on a hardware where the software is installed, if no screen is available by label, etc.

NOTE The shipboard data server can manage its software version in a way which is consistent with ISO 24060.

8 Test requirements

8.1 Outline

The manufacturer of the shipboard data server shall carry out tests on general requirements, on data input/output and management and on operation requirements. The tests are conducted in accordance with the methods listed in Tables 2, 3 and 4, and the results are judged by the evaluation standards. The methods and results shall be documented in a test report.

Test plans shall be formulated before conducting the tests to clarify test environments, test subjects and judgment criteria.

Test reports shall be compiled after conducting the tests to report the test results.

Test methods, judgment criteria and test results shall be reported in detail.

When the shipboard data server is intended to be certified by a third-party organization, the manufacturer shall contact the organization and agree to the documentation(s) and testing(s) necessary to demonstrate compliance with the relevant requirements.

8.2 Test items

8.2.1 Test environments

The shipboard data server shall be tested according to the following definitions.

The functional tests shall be performed as outlined in IEC 60092-504. Confirm that the output of one data sample set can be performed using request-response transport service from five sessions with input and output of 30 data samples, using a streaming transport service from two sessions. Also confirm that the output of one data sample set can be performed using file transport service from one session with output of 30 data samples the file defined by ISO 19848 at the same time. The test structure is shown in Figure 6.

The functional check shall be performed as outlined in IEC 60092-504. Confirm that condition monitoring of 5.1.4 functions normally.

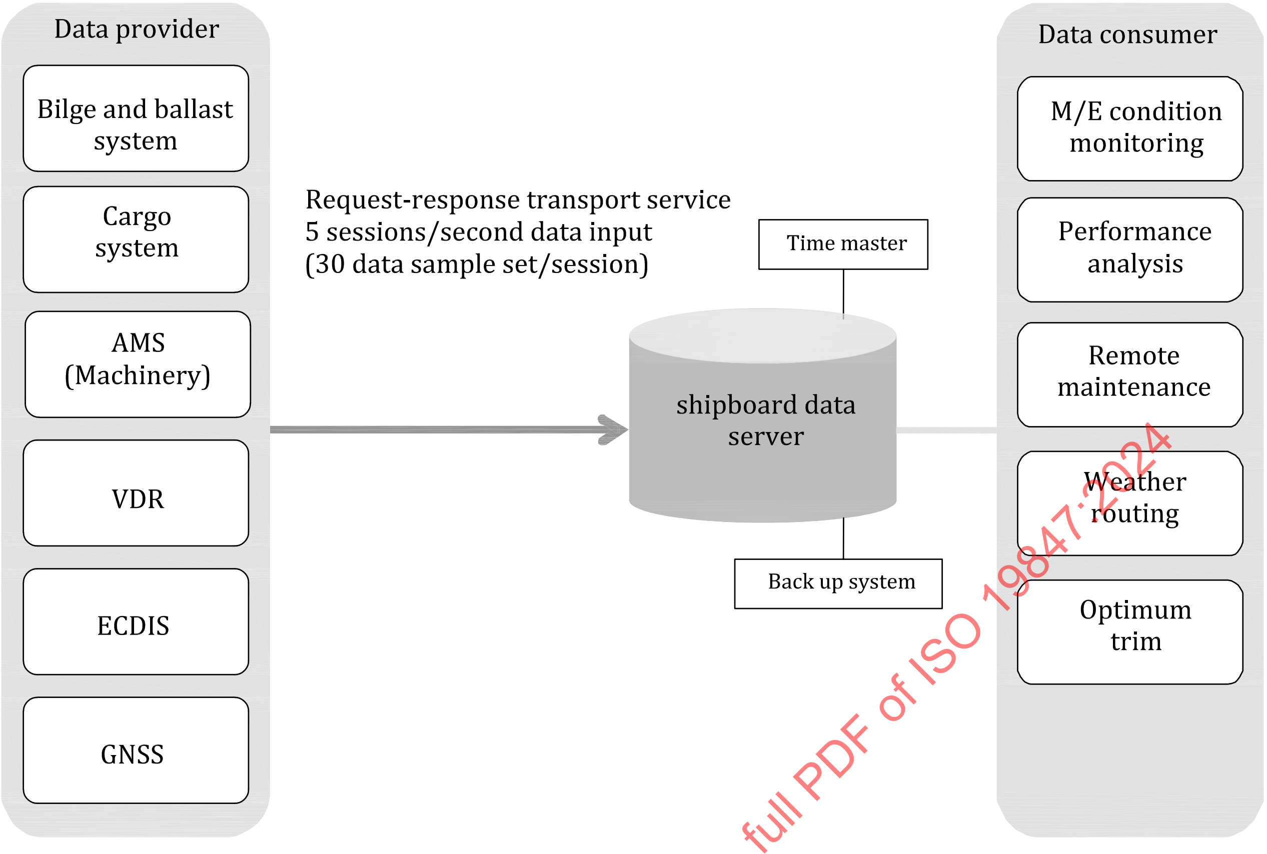


Figure 6 — Test structure

Conditions for peripheral test devices are as follows.

a) Data providers that can make more than one data input request as shown in Chapter 5 are connected to the equipment under test (EUT).

b) Data consumers that can make more than one data output request as shown in Chapter 5 are connected to the EUT.

c) Data receivers that can receive files in EUT's file transport service are connected to the EUT.

d) When the EUT does not have an administrative user interface, management devices that do have administrative user interfaces are connected to the EUT.

e) Time masters that can perform time synchronisation are connected to the EUT.

f) Backup systems that can receive backup data from the EUT and store them are connected to the EUT.

g) The above-mentioned functions may be consolidated in one or more devices.

8.2.2 Test methods

The test items in Table 2 correspond to subclauses of Clause 5. The test conditions and methods listed in the test methods column in Table 2 consists of three parts. The top part describes the test outline. The middle part describes the test conditions and lists pairs of condition items and contents. The bottom part describes the test procedures. The tests are conducted in accordance with the test procedures under the test conditions and confirm that the evaluation standards are satisfied.

Table 2 — Test items, test methods and evaluation standards for general requirements

Test items	Test methods		Evaluation standards
5.1.1.2 Input data processing performance	Confirm that the input data processing performance in 5.1.1.2 is satisfied.		Confirm that there is no time stamp omission in data retrieved in shipboard data servers, and that the data completely agree with request data.
	Data volume	60 min × 60 s × 150 data sets	
	Data input frequency (1)	5 sessions/s (30 data sample sets/session)	
	Data input frequency (2)	1 sessions/0,2 second (30 data sample sets/session)	
	Issue data input requests consecutively from data providers to shipboard data servers in accordance with the conditions listed above in this table, and write data on shipboard data servers periodically.		
5.1.1.3 Output data processing performance	Confirm that the output data processing performance in 5.1.1.3 is satisfied.		Confirm that there is no time stamp omission in data retrieved in data consumers, and that the data completely agree with request data.
	Data volume	60 min × 60 s × 50 data sets	
	Data request frequency	1 sessions/second (30 data sample sets/session)	
	Issue data output requests from data consumers to shipboard data servers for each of the following two protocols, in accordance with the conditions listed above in this test item, and retrieve the data written in shipboard data servers in data consumers. a) Request-response transport b) File transport		
5.1.1.4 Streaming transport processing performance	Confirm that the streaming transport processing performance in 5.1.1.4 is satisfied.		a) Incoming: Confirm that there is no time stamp omission in data retrieved in shipboard data servers, and that the data completely agree with request data. b) Outgoing: Confirm that there is no time stamp omission in data retrieved in data consumers, and that the data completely agree with request data.
	Incoming data volume	60 min × 60 s × 150 data sets	
	Outgoing data volume	60 min × 60 s × 150 data sets × 2 streams	
	a) Send streaming data from data providers to shipboard data servers in accordance with the conditions listed above in this test item. b) Send streaming data from shipboard data servers to data providers in accordance with the conditions listed above in this test item.		
5.1.2 Storage function	Confirm that the storage function in 5.1.2 is satisfied.		Convert data volume recorded in shipboard data servers and logs at the time of processing into one-month volumes, and confirm that the volumes are smaller than available storages prescribed in specification documents.
	Data volume	60 min × 60 second × 150 data sets	
	Confirm the above-mentioned with the Input data processing performance in 5.1.1.2, using data written in shipboard data servers.		

Table 2 *(continued)*

Test items	Test methods		Evaluation standards
5.1.4 Condition monitoring function	Confirm that with the condition monitoring function in 5.1.4, shipboard data server statuses are monitored, and the statuses are reported to other shipboard systems.		Confirm the following: a) Abnormalities generated on shipboard data servers shall be reported to other shipboard systems. b) (In case local displays are available): Abnormalities generated on shipboard data servers shall be displayed locally.
	Subject to monitor	One or all the following: a) system abnormalities in shipboard data server processors (CPUs), b) access failures in storage devices, c) failures in recording interfaces (LANs), d) troubles in UTC time synchronisation and e) insufficient vacant space in storage devices.	
	Standard for judging insufficient vacant space in storage devices	Vacant space accounts for zero percent or data volumes for 30 days or less.	
	Volume of data to be saved in shipboard data servers (for 30 days)	30 d × 24 h × 60 min × 60 s × 150 data sets (or designated by makers)	
	Status reporting interface	The interface for reporting shipboard data server statuses prescribed in 5.1.7	
	a) Generate abnormalities (artificially) at each subject and monitor shipboard data server statuses to be reported from the status reporting interface to other shipboard systems (also see 5.1.7). b) (In case local displays are available): Generate abnormalities (artificially) at each subject and monitor shipboard data server statuses which shall be displayed locally.		
5.1.5 Data backup and restoration functions	Confirm the data backup and restoration function.		Confirm that management data and actual recorded data saved in backup systems are restored in the EUT.
	Volume of data to be saved in the EUT	30 d × 24 h × 60 min × 60 s × 150 data sets	
	Save in the backup systems management data and actual recorded data in the EUT. Restore in the EUT management data and actual recorded data saved in backup systems.		
5.1.6 Function to protect against unauthorised access	NOTE Cybersecurity-related tests are described in Table 4.		
5.1.7 Status reporting	Confirm that shipboard data server statuses can be recognized on board ship with the status reporting interface described in 5.1.7.		In status reporting interfaces, confirm that shipboard data server statuses (normal/abnormal) shall be output.
	Status to report	Shipboard data server statuses (normal/abnormal) monitored in 5.1.4.	
	Status reporting interface	Single outputs at relay contacts or methods designated by makers (crewmembers shall recognize abnormalities on shipboard data servers).	
	Generate shipboard data server abnormality (artificially) and confirm interfaces for reporting shipboard data server statuses (normal/abnormal).		

The test items in Table 3 correspond to subclauses of Clause 6. The test methods column in Table 3 consists of three parts. The top part describes the test outline. The middle part describes the test conditions and lists pairs of condition items and contents. The bottom part describes the test procedures. The tests are conducted in accordance with the test procedures under the test conditions and confirm that the evaluation standards are satisfied

Table 3 — Test items, test methods and evaluation standards for date input/output and data management

Test items	Test methods		Evaluation standards
6.2.2 Management of system clock	Confirm that the management of the system shown in 6.2.2 is carried out.		Confirm the following: a) EUT time is synchronized with time masters at predefined intervals. b) When time synchronization cannot be made, the EUT issues a “loss of UTC synchronization” warning. c) EUT real-time clock (RTC) shall not be inaccurate for more than one second per hour.
	Time	Approximately 2 h	
	Synchronization frequency with time masters	1 h/session	
	a) Set the UTC in the EUT one day or more in advance of test days, and confirm the UTC in the EUT is synchronized with the UTC in the time masters within an hour. b) After synchronization with the time masters as described in a), dissolve connections between the EUT and time masters, and confirm that the EUT issues a “loss of UTC synchronisation” warning (see 5.1.7 for methods). c) An hour after synchronization with the time masters as illustrated in a), when connections between the EUT and the time masters are dissolved as shown in b), confirm that the time lag between the EUT’s UTC and the time masters’ UTC is no more than one second.		
6.2.3 Management of Data Channel List 6.3.2 Input function 6.3.3 Output function 6.3.4 Request-response data transport service	Confirm the data input/output functions in 6.2.3, 6.3.2, 6.3.3 and 6.3.4.		Confirm that there is no time stamp omission in the data retrieved in the data consumers.
	Volume of data to be saved in the EUT	30 d × 24 h × 60 min × 60 s × 150data sets	
	Frequency of data inputs	5 sessions/s (30 data sample sets/session)	
	Frequency of data outputs	5 sessions/5 s	
	Number of data inputting devices	At least one device	
	Number of data outputting devices	At least one device	
	a) Issue data input requests shown in 6.3.2 and 6.3.4 consecutively from data providers to the EUT in accordance with the conditions listed above in this test item, and write data in the EUT periodically. b) At the same time as the abovementioned requests, issue data output requests shown in 6.3.3 and 6.3.4 from data consumers to the EUT in accordance with the conditions listed above in this test item, and retrieve in data consumers the abovementioned data written in the EUT.		

Table 3 *(continued)*

Test items	Test methods		Evaluation standards
6.2.3, 6.2.4 and 6.2.5 Management of management data	Confirm whether three files managed by the EUT (Data Channel List, Data Source Information and Alias List) can be created, updated and deleted from management devices, and whether access is controlled from management devices to the files.		a) In case the EUT itself is also a management device, confirm that: 1) with incorrect authentication information, it is not possible to perform creating, updating and deleting operations. 2) with correct authentication information, it is possible to perform creating, updating and deleting operations. When such operations are made, confirm that Data Channel List, Data Source Information and Alias List are updated. b) In case the EUT is not a management device, confirm that: 1) updating and deleting operations can be made successfully when management devices have been authorized by the EUT. Data Channel List, Data Source Information and Alias List are updated as intended by the operations made. 2) when management devices are not authorized by the EUT, updating and deleting operations are unsuccessful, and Data Channel List, Data Source Information and Alias List are not updated.
	Frequency of data inputs	30 d × 24 h × 60 min × 60 s × 150 data sets	
	Frequency of data inputs	5 sessions/s (30 data sample sets/session)	
	Number of data inputting devices	5 sessions/5 s	
	Number of data inputting devices	At least one device	
	Number of data outputting devices	At least one device One management device	
	a) In case the EUT itself is also a management device: 1) Input incorrect information in the EUT, and apply creating, updating and deleting operations to three files: Data Channel List, Data Source Information and Alias List. 2) Input correct information in the EUT, and apply creating, updating and deleting operations to three files: Data Channel List, Data Source Information and Alias List. b) In case the EUT is not a management device: 1) While management devices have been authorized by the EUT, apply creating, updating and deleting operations to three files: Data Channel List, Data Source Information and Alias List. 2) While management devices are not authorized by the EUT, apply creating, updating and deleting operations to three files: Data Channel List, Data Source Information and Alias List.		

Table 3 *(continued)*

Test items	Test methods		Evaluation standards
6.2.3 Management of Data Channel List 6.3.2 Input function 6.3.3 Output function 6.3.4 Request-response data transport service	Confirm the data input/output functions in 6.2.3, 6.3.2, 6.3.3 and 6.3.4.		Confirm that there is no time stamp omission in data that data consumers retrieve from the EUT.
	Volume of data to be saved in the EUT	30 d × 24 h × 60 min × 60 s × 150 data sets	
	Frequency of data inputs	5 sessions/s (30 data sample sets/session)	
	Frequency of data inputs	5 sessions/5 s	
	Number of data inputting devices	At least one device	
	Number of data outputting devices	At least one device	
	a) Issue data input requests shown in 6.3.2 and 6.3.4 consecutively from data providers to the EUT in accordance with the conditions listed above in this test item, and write data in the EUT periodically. b) At the same time as the abovementioned requests, issue data output requests shown in 6.3.3 and 6.3.4 from data consumers to the EUT in accordance with the conditions listed above in this test item, and retrieve in data consumers the abovementioned data written in the EUT.		
6.3.5 Streaming data transport service	Request to subscribe/unsubscribe streaming data from data outputting devices to the EUT and confirm whether the request is accepted and whether access is controlled by the appropriate authentication.		Confirm the following. a) When subscriptions are made from data outputting devices to the EUT, data on this topic are sent to data outputting devices. b) When the topic is unsubscribed, data outputting devices no longer receive data from the EUT.
	Volume of data to be saved in the EUT	30 d × 24 h × 60 min × 60 s × 150 data sets	
	Frequency of data inputs	5 sessions/s (30 data sample sets/session)	
	Frequency of data inputs	5 sessions/5 s	
	Number of data inputting devices	At least one device	
	Number of data outputting devices	At least one device	
	a) Subscription requests are made to MQTT topics by data outputting devices. b) Requests are made to unsubscribe to topics subscribed in a) by data outputting devices.		

Table 3 *(continued)*

Test items	Test methods		Evaluation standards
6.3.6 File transport service	Confirm that the file transport service shown in 6.3.6 is performed.		Confirm the following. a) Protocol functions prescribed in maker specifications work appropriately. b) All sample files sent from data providers have been saved in the EUT. c) All sample files sent from the EUT have all been saved in data receivers. d) Sample files saved in the EUT can be deleted.
	Protocol	All compatible protocols	
	Sample file data format	XML files complying with ISO 19848	
	File size	Maximum volumes in maker specifications	
	a) Confirm that protocol functions (authentication, exclusive control, command, etc.) prescribed in maker specifications work appropriately. b) Send sample files from data providers to the EUT and confirm that they are saved at arbitrary locations in the EUT. c) Send sample files from the EUT to data receivers, and confirm that they are saved at arbitrary locations in data servers. d) Connect the EUT with data receivers, and confirm that sample files saved in the EUT can be deleted with protocols with which the EUT complies.		
6.4 Alias function	Confirm the Alias function shown in 6.4, if the shipboard data server has this function.		Confirm that the data: - have been retrieved by data consumers from the EUT; - have been obtained in agreement with registered Alias IDs; - have no time stamp omissions.
	Volume of data to be saved in the EUT	30 d × 24 h × 60 min × 60 s × 150 data sets	
	Frequency of data inputs	5 sessions/5 s (30 data sample sets/session)	
	Number of alias lists registered	One or more	
	Make data output requests from data consumers with Alias IDs registered with the EUT in accordance with the conditions listed above in this test item. Retrieve the requested data from the EUT to data consumers.		

Table 3 *(continued)*

Test items	Test methods		Evaluation standards
6.6 Log management function	Confirm that the sufficient number of logs required for the EUT have been recorded.		Confirm that the following details are recorded in EUT logs. a) HTTP status codes done by data consumers: requests that reply “200” and “403” as well as their details (time stamps, URLs, HTTP status codes and IPs of request sources) b) 1) Records of changes in Data Channel List, Data Source Information and Alias List (time stamps and revised file names) 2) Changes in time (time before and after changes) c) Details of generated self-diagnostic abnormalities (time stamps and abnormality details)
	Volume of data to be saved in the EUT	30 d × 24 h × 60 min × 60 s × 150 data sets	
	Frequency of data inputs	5 sessions/s (30 data sample sets/session)	
	Frequency of data inputs	5 sessions/5 s	
	Number of data inputting devices	At least one device	
	Number of data outputting devices	At least one device	
	a) Make the following requests from data consumers to the EUT. 1) Request GET so that request results are 200. (Request-response protocols are used.) 2) Request GET so that request results are 403. (Request-response protocols are used.) b) Make the following changes from management devices or the EUT. 1) Changes in Data Channel List, Data Source Information and Alias List. 2) Changes in time. c) Generate self-diagnostic abnormalities 1) Generate the self-diagnostics abnormalities required in this document, one by one.		

The test items in Table 4 correspond to Clause 7. The test methods column in Table 4 consists of two parts. The upper part describes the test outline. The lower part describes the test procedures. The tests are conducted in accordance with the test procedures and confirm that the evaluation standards are satisfied.

Table 4 — Test items, test methods and evaluation standards for operation requirements

Test items	Test methods	Evaluation standards
7.2.1.2. Account management	Confirm support functions so that authorized users can manage all accounts.	Confirm the following. a) Only authorized users shall be permitted to add, activate, change, deactivate and delete accounts. b) Only authorized users shall be permitted to organize account groups and set group membership conditions. c) Read/write access to authorized files is possible. Read-only access should be readable and not writable, and read/write access to unauthorised files should be disabled. d) The application shall be able to read/write the necessary files, etc. e) The default system account shall be deactivated or deleted after installation.
	a) Confirm that an authorized user can add, activate, change and deactivate accounts. Confirm that general users cannot perform these operations. b) Confirm that an authorized user managing accounts can organize account groups and set conditions for group membership. Confirm that general users cannot perform these operations. c) Confirm whether read/write access to files, etc. is allowed or denied for each account group. d) Execute the application and confirm whether the necessary files can be read/written. e) Confirm that the default account used during installation cannot be used.	
7.2.1.3. Identifier management	Confirm the effectiveness of functions that support the management of users, groups, roles and/or identification through the shipboard data server interface.	Confirm the following.
	Confirm that there are functions to support identifier management. a) Confirm that a management policy for identifiers has been set. b) Confirm that the distributed identifiers are unique and defined in accordance with the management policy.	There shall be functions to support the identifier management by users, groups, roles and/or shipboard data server interfaces. a) The method of identifier management shall be rule-based. b) The distributed identifiers shall be unique and defined in accordance with the management policy.

Table 4 *(continued)*

Test items	Test methods	Evaluation standards
7.2.1.4. User authentication	Confirm the effectiveness of the functions used to identify users to the server, control access to specific information, and provide protection of information.	a) Confirm that a user identification and user authentication mechanism for at least two types of user privileges, general operation mode and administrator authority mode, shall be provided.
	a) Confirm that the shipboard data server has at least two types of user privileges. b) Confirm that if user authentication fails, there is a limit to the number of attempts allowed. c) Confirm that the most recent authentication information is recorded.	
	d) Confirm that the account employs password, physical key authentication or multi-factor authentication methods. e) 1) When authenticating users with passwords — Confirm that passwords are case-sensitive.	b) Confirm that there shall be a method to limit the number of attempts when user authentication fails repeatedly.
	— Confirm that administrator passwords are at least 10 characters including arabic numerals, upper and lower case letters of the alphabet and three special characters.	c) Confirm that the last 10 occurrences of authentication information shall be recorded in an internal or external syslog.
	— Confirm that general user passwords consist of at least eight characters including arabic numerals, upper and lower case letters of the alphabet and two special characters.	d) Confirm that the account shall use authentication methods such as passwords.
	— Confirm that the password is a random row of meaningless characters and that it is strictly controlled to prevent others from knowing it. 2) When remote access functions are provided, confirm that security measures are sufficiently secured.	e) 1) Confirm that in the case of user authentication by password, the password setting shall be more strict for administrators than for general users, and shall be properly managed.
	3) If an asymmetric encryption method using a smart card, etc. is used, confirm the encryption security level.	2) Confirm that if the system is provided with a remote access function, a private key or other symmetric cryptosystem shall be used. 3) Confirm that if an asymmetric cryptosystem such as a smart card is used, the cryptographic security level shall be 2048-bit RSA key or higher.
7.2.1.5. Authenticator feedback	Confirm the function of masking the authentication information feedback during the authentication process.	Confirm that the entered password shall be obscured and not displayed.
	Confirm that feedback on authentication information is hidden by displaying asterisks or other random characters when the password is entered.	

Table 4 *(continued)*

Test items	Test methods	Evaluation standards
7.2.2. Usage control	Confirm that the usage control in 7.2.2 is satisfied.	Confirm the following. The shipboard data server shall have functions that control operations and access to resources with user authorization. a) Unauthorised users shall be restricted from executing functions and accessing resources. b) Authorized users shall be permitted to execute functions and access resources normally.
	Confirm if there are any restrictions on user privileges when operating the shipboard data server or accessing resources. a) Check that it is not possible to execute the functions of the shipboard data server without authorization. b) Check to see if the user can execute authorized functions of the shipboard data server while in an authorized state.	
7.2.3.1. Network access	Confirm that the network access in 7.2.3.1 is satisfied.	Confirm the following. a) The shipboard data server shall be installed in DMZs isolated from the outer and inner networks by a firewall or similar device that complies with the 16425-gateway or 460-gateway. b) The available communication ports are described in the manual, and only those ports shall be able to communicate with each other. c) The function shall be disabled for communication with communication services which are not specified. d) There shall be no commands other than those used in the services specified. e) Only authorized mobile codes shall be executable.
	a) Confirm the configuration diagram of the network in which the shipboard data server will be installed. b) Confirm the available communication ports in the instruction manual. 1) Confirm that the available communication ports can be accessed. 2) Confirm that the unused communication ports cannot be accessed. c) Confirm the communication status by communicating with communication services other than the ones specified in 6.3.2 to 6.3.6. d) Confirm the commands available on the shipboard data server. Confirm that there are no commands other than the services specified in 6.3.2 to 6.3.6. e) Verify that the manufacturer's documentation stipulates that the shipboard server has the function to control the use of mobile code execution.	
7.2.3.2. Remote access	Confirm that the remote access in 7.2.3.2 is satisfied.	For remote access to the shipboard data server, confirm that the server shall be installed on the vessel in accordance with the requirements for Category I specified in IACS Rec.166:2020, 7.6.
	When using remote access to the shipboard data server, confirm the installation environment of the shipboard data server.	
7.2.3.3. Use of cryptography	Confirm that the use of cryptography in 7.2.3.3 is satisfied.	When encryption is implemented, confirm that a private key or other symmetric encryption systems shall be used.
	When encryption is implemented, confirm the encryption system being used.	

Table 4 *(continued)*

Test items	Test methods	Evaluation standards
7.2.4.2. Malware protection	Confirm that the malware protection in 7.2.4.2 is satisfied.	Confirm the following. a) For devices that have anti-malware software, 1) The anti-malware software shall be working. 2) Automatic updates shall be enabled. — Updates shall be executable. — Notify users of the expiration date if no updates are made for a certain period of time. 3) After the update, the performance requirements specified in 5.1.1 shall be met. b) For devices that do not have anti-malware software, 1) The shipboard data server shall be installed in a DMZ with a firewall that complies with the 460-Gateway consisting of an L3 switch, UTM, and 16425-Gateway.
	a) For devices that have anti-malware software or the ability to update it, follow the manufacturer's instruction manual. 1) Confirm that the anti-malware software installed on the device is working properly. 2) Confirm that the anti-malware update is functioning effectively. 3) Confirm that performance is not impacted by the software update by following the procedure shown in 5.1.1. b) For devices that do not have anti-malware software, 1) Confirm the installation requirements for the shipboard data server.	
7.3.2. Installation requirements	Confirm that the installation requirements in 7.3.2 are satisfied.	Confirm and record that the shipboard data server is installed in a room or panel that can be physically or electronically locked. Confirm and record the existence of a document that specifies the method of managing authentication devices such as keys and passwords.
	Confirm that the installation requirements are described in the installation manual.	
7.3.3. Connection cables	Confirm that the operational requirements in 7.3.3 are satisfied.	Confirm and record that communication cables are protected from being stepped on (e.g. laid on the roof or protected by cable ducts).
	Confirm that the installation requirements satisfied are described in the installation manual.	
7.3.4. Power source management	Confirm that the operational requirements in 7.3.4 are satisfied.	Confirm and record that the power connector of the shipboard data server is equipped with an anti-disconnection mechanism (screw fixation, hook, etc.).
	Confirm that the installation requirements satisfied are described in the installation manual.	

Table 4 *(continued)*

Test items	Test methods	Evaluation standards
7.3.5.2. Unused connection points	Confirm that unused connection points are protected.	Confirm the following. a) The connection point protected by method a) in 7.3.5.2 shall not be accessible without tools or keys. b) The connection points protected by methods b) or c) in 7.3.5.2 shall not be accessible by removable devices. c) The connection point protected by method b) in 7.3.5.2 shall be disabled. d) For connection points protected by method c) in 7.3.5.2, the activation procedure shall require authentication.
	Confirm whether the unused connection points are protected by any of the methods a) through c) in 7.3.5.2 using the manufacturer's documentation. a) Confirm the access procedure for connection points protected by the method a) in 7.3.5.2. b) Connect a removable device to a connection point protected by methods b) or c) in 7.3.5.2. c) Confirm with the manufacturer's evidence documentation that the connection point is protected by method b) in 7.3.5.2. d) Confirm the activation procedure for the connection point protected by method c) in 7.3.5.2.	
7.3.5.3. Operation protection	Confirm that the usage of the connection point is limited.	Confirm the following. a) The technology limiting the intended use shall be described in the manufacturer's evidence documentation. b) Devices other than USB device class 08h shall not be used in connection points specified for USB data storage devices.
	Confirm the following for connection points with limited usage. a) Refer to the manufacturer's evidence documents for the usage limits. b) Connect devices other than USB device class 08h to the connection points specified for USB data storage devices.	
7.3.5.4. Executable program file verification	Confirm that only REDS data that passes verification can be executed.	Confirm the following. a) Automatic execution of executable REDS shall be prohibited. b) Manual execution of executable REDS shall only be allowed for REDS that have passed authentication and verification (either by digital signature or special key). c) Manual execution of executable REDS that do not pass verification shall not be executed.
	Confirm the following for points where REDS can be connected. a) Refer to the manufacturer's evidence documentation for the automatic execution of REDS. b) Refer to the manufacturer's evidence documentation for the manual execution of REDS. c) Implement a manual execution procedure for test REDS that do not pass verification.	

Table 4 *(continued)*

Test items	Test methods	Evaluation standards
7.3.5.5. Non-executable data verification	Confirm that only REDS that pass validation can be used for non-running data in REDS.	Confirm the following. a) Only non-executable data in REDS that pass verification (either by digital signature or special key) shall be used. b) Any non-executable data in REDS not passing verification shall not be used.
	Confirm the following for points where REDS can be connected. a) Refer to the manufacturer's evidence documentation for the use of non-executable data in REDS. b) Implement usage procedures for non-executable data in REDS for testing that do not pass verification.	
7.3.6. Protection (others) (1)	Confirm that the operational requirements in 7.3.6 are satisfied.	Confirm and record that all unused Ethernet ports and USB ports are blocked so that no cables can be connected.
	Confirm that the installation requirements satisfied are described in the installation manual.	
7.3.6. Protection (others) (2)	Confirm that the operational requirements in 7.3.6 are satisfied.	If the Ethernet Port and USB Port blocks described in the previous item can be unblocked using a tool, confirm and record the existence of a document describing the management method of the tool.
	Confirm that the installation requirements satisfied are described in the installation manual.	
7.3.7. Equipment maintenance	Confirm that the operational requirements in 7.3.7 are satisfied.	Confirm and record that the following items are described in the user's manual of the shipboard data server. — Inspection items — Troubleshooting — Consumables list and recommended replacement time
	Document review	

Table 4 *(continued)*

Test items	Test methods	Evaluation standards
7.4.2. Maintenance mode	Confirm that the maintenance mode in 7.4.2 is satisfied. a) Confirm the procedure for entering maintenance mode. b) After completing the maintenance work: 1) Confirm the syslog when exiting maintenance mode. Also confirm the system showing the operation result. 2) Confirm the situation by staying in maintenance mode for a certain period without executing any operation.	a) When entering maintenance mode, confirm that a multi-step procedure shall be necessary. It shall require a managed key, administrative privileges granted by the user, role, or group, and/or special conditions. b) In maintenance mode, after maintenance is completed, confirm that: 1) i) Authentication information with time stamps used when the maintenance mode is entered and that the operation contents and results shall be recorded in the internal or external syslog. ii) There shall be a system to inform users of the operation results. 2) The maintenance mode shall be terminated if there is no operation for a certain period.
7.4.3. Setting changes	Confirm that the requirements in 7.4.3 are satisfied. a) Confirm the procedure for a user to change the settings of the shipboard data server, but not in any other mode. b) Confirm the procedure to import and export Data Source Information and Data Channel List settings.	Confirm the following. a) Users shall be able to change the settings only in maintenance mode. b) Data Source Information and Data Channel List settings shall be importable and exportable in maintenance mode.

Table 4 *(continued)*

Test items	Test methods	Evaluation standards
7.4.4. Software update	Confirm that the requirements in 7.4.4 are satisfied.	Confirm the following. a) The function to update the OS, middleware, and software shall operate only in maintenance mode. b) If the OS, middleware, or software has version information, the version shall be managed to guarantee traceability. c) The OS, middleware, and software shall be able to be immediately restored to the state before the update, either online or offline.
	a) Confirm that OS, middleware, and software updates can operate in maintenance mode, and that update functions cannot be executed outside of maintenance mode. b) Confirm the version information of the OS, middleware, and software, and the method of managing it. c) Confirm the procedure for restoring the original state online or offline after updating.	
7.4.5 Failure recovery	Confirm that the requirement in 7.4.5 is satisfied.	Confirm that the function to cancel or roll back updates during software maintenance shall be available.
	Confirm that when an update is cancelled or rolled back during software maintenance, the shipboard data server will return to the previous state.	
7.4.6. Software version information	Confirm that the requirements in 7.4.6 are satisfied.	Confirm that software version information shall be able to be displayed or output.
	Confirm that the software version information is displayed on the display unit or output to an external device.	

Annex A
(informative)

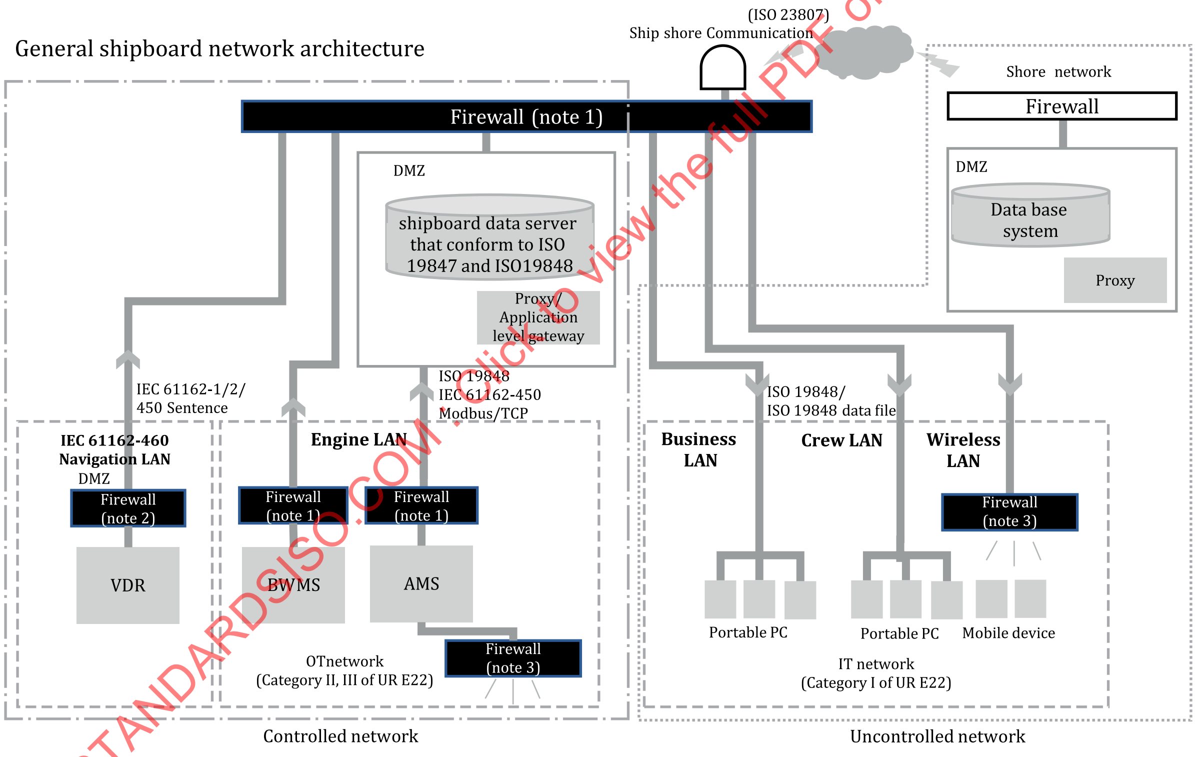
Ship-to-shore communication management

A.1 General

Storing data on the shipboard data server and the on-shore data server has the advantage of providing access to long-term data collection from several vessels for periods that exceed the shipboard data servers' recording periods.

To realize such a system, this document establishes the requirements for the function which sends data stored by the shipboard data server to the on-shore data servers.

Figure A.1 describes the concept model of the ship-to-shore communication using the networks specified in ISO 16425 and IEC 61162-450 on-board. Details for mitigating the cyber safety related risks associated with ship-to-shore communication are introduced in IEC 61162-460.



NOTE 1 The firewall is part of the 460-Gateway or 16425-Gateway. The 16425-Gateway can consist of layer 3 switch, UTM etc.

NOTE 2 The firewall complies with the requirements of the 460-Gateway. The 460-Gateway can consist of layer 3 switch, UTM etc.

NOTE 3 The firewall complies with the 460-Wireless gateway or 16425-Wireless gateway.

Figure A.1 — Concept model of ship-to-shore communication

Figure A.2 describes the concept model of a ship-to-shore communication agent.

Practical implementation of the shipboard data server can require employing additional functions called agents.

Agent functions can perform specific tasks such as to facilitate ship-to-shore communication or refine the data recorded by the shipboard data server by performing additional data analysis.

It is possible that agent functions reside within the shipboard data server equipment.

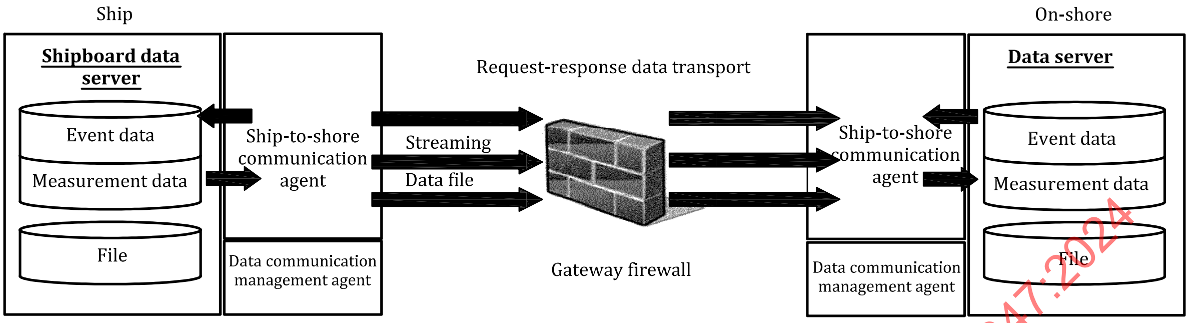

Ship
On-shore
Shipboard data server
Event data
Measurement data
File
Ship-to-shore communication agent
Data communication management agent
Request-response data transport
Streaming
Data file
Gateway firewall
Ship-to-shore communication agent
Data communication management agent
Data server
Event data
Measurement data
File

Figure A.2 — Concept model of ship-to-shore communication agent

A.2 Ship-to-shore communication agents

To realize data linkages between the unstable shipboard data server and the on-shore data server, it is possible to employ ship-to-shore communication agents that have the following basic functions:

a) transmitting data from the shipboard data server when required by on-shore data servers to send requested data gathered for requested periods of time;

b) transmitting files stored on the shipboard data server to on-shore data servers;

c) transmitting streaming data from the shipboard data server when required by on-shore data servers to send data. SFTP, HTTPS and other protocols may be used to encrypt data transmissions.

A.3 Data communication management agents

To achieve efficient ship-to-shore communication, it is possible to use data communication management agents with the following functions:

a) data compression/decompression;

b) band/capacity management: limiting the volume of data that the shipboard data server can send at one time to prevent the server from sending large data that exceed limits;

c) account management: responding solely to approved accounts and requests from senders; and

d) priority management: managing priority for each account and each task.

A.4 Service agents

Agents that have functions other than those of ship-to-shore communication agents and data communication management agents are called service agents. Service agents may be employed for statistical calculation and other tasks.

Annex B
(informative)

Structure of Alias List

B.1 Data model of Alias List

An Alias List shall consist of the following elements.

a) Package

The package element is metadata made up of a Header included in the Alias List, which is a main data body.

b) Header

The header element is metadata that includes the creation date and time, and the author of the Alias List.

c) Alias

The Alias consists of an Alias ID and multiple DataChannel including Local ID and Short ID.

The Alias can be restricted by using a public element and an owner element.

d) DataChannel

The DataChannel is defined by the Local ID or Short ID and assigned to the Alias ID.

Labels can be added to the Local ID and Short ID. The label shall be unique in the Alias ID. However, this label is an output label of the Time Series Data and cannot be used to execute a method.

One Alias ID cannot contain the same Local ID and Alias ID.

The structure model of the Alias List is shown in Figure B.1 using UML. For more information on UML notation, see ISO/IEC 19505-1 and ISO/IEC 19505-2.

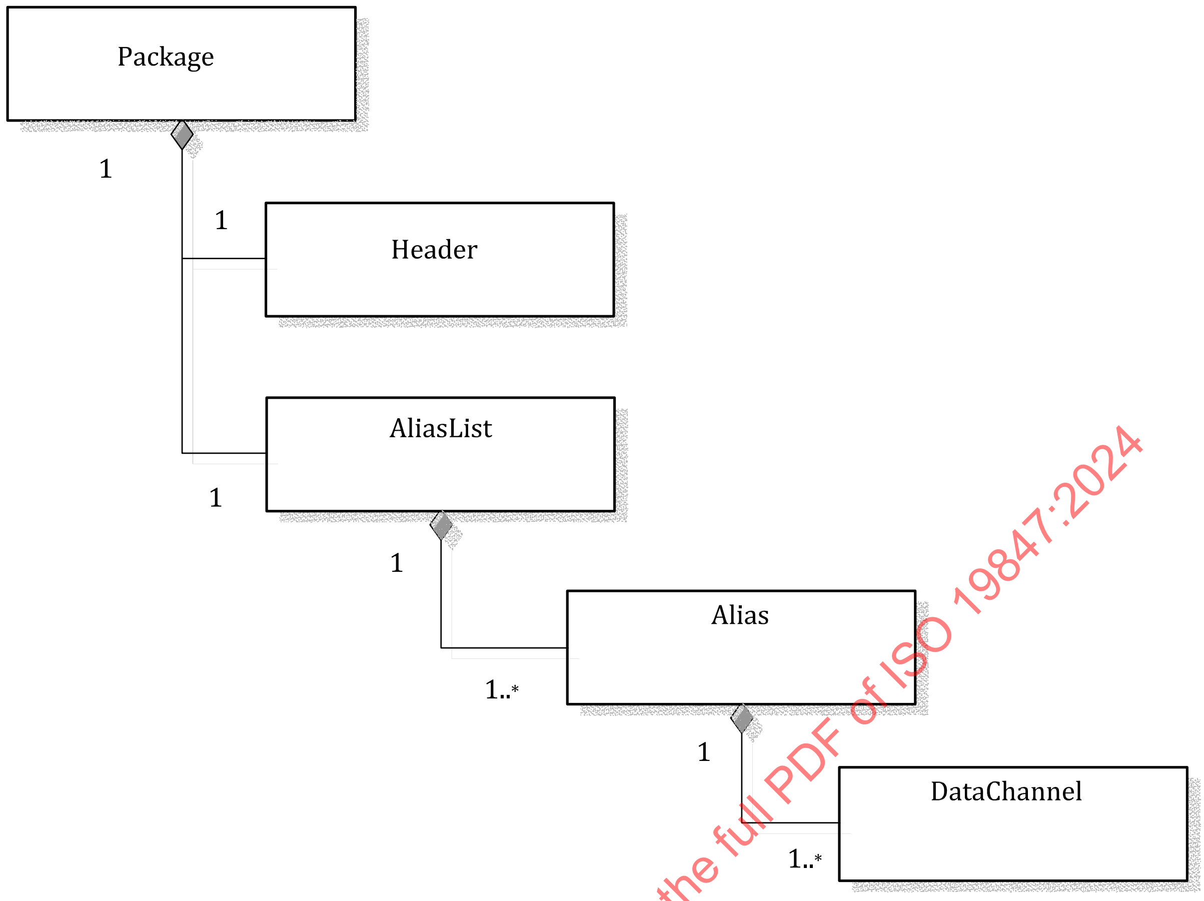


Figure B.1 — Structure model of the Alias List

B.2 Logical structure of the Alias List

The Alias List shall have the logical structure shown in Figure B.2 using UML. For more information on UML notation, see ISO/IEC 19505-1 and ISO/IEC 19505-2.

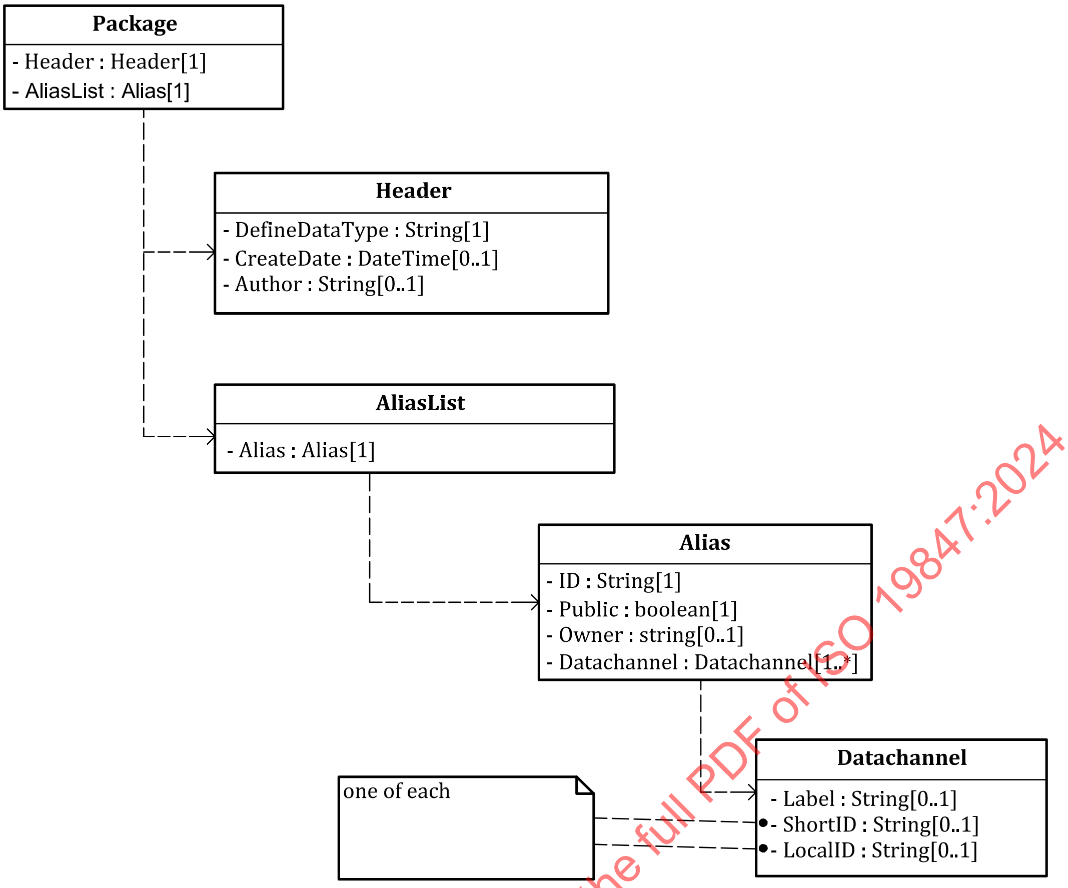


Figure B.2 — Logical structure of an Alias List model

The details of each element are shown in Tables B.1 to B.5.

Table B.1 — Package structure

Name	Data type	Note	Usage	Max count
Header	Header	See Table B.2	Mandatory	1
AliasList	Alias List	See Table B.3	Mandatory	1

Table B.2 — Header structure

Name	Data type	Note	Usage	Max count
DefineDataType	String	Alias	Mandatory	1
CreateDate	DateTime	Date when data are created	Optional	1
Author	String	Author of data	Optional	1

Table B.3 — AliasList structure

Name	Data type	Note	Usage	Max count
Alias	Alias	See Table B.4	Mandatory	1

Table B.4 — Alias structure

Name	Data type	Note	Usage	Max count
ID	String	Identifier identifying Alias. The ID is unique within the shipboard data server.	Mandatory	1
Public	Boolean	Specify the accessibility of this Alias. When the Public element is set to false, disclosure of Alias ID is restricted. In that case, designation of the Owner element is necessary.	Mandatory	1
Owner	String	Specify the owner of this Alias. When owner element is described, it is restricted to the owner where editing is described.	Optional	1
DataChannel	DataChannel	See Table B.5	Mandatory	[a]

[a] Any number greater than or equal to 1.

Table B.5 — DataChannel structure

Name	Data type	Note	Usage	Max count
Label	String	Specify the Label element when adding another label to ShortID or LocalID.	Optional	1
ShortID	String	See ISO 19848:2024, 5.1.4.	Optional	1
LocalID	String	See ISO 19848:2024, 5.1.3.	Optional	1

Annex C
(normative)

Request-response protocol

C.1 General

The request-response protocol consists of:

- requesting data processing from the shipboard machinery and equipment to the shipboard data server, and
- the shipboard data server delivering results in response to the request.

The protocol supports the delivery of data arranged in chronological order and allows the delivery of records originating from multiple data providers in the same report.

C.2 defines access control requirements while C.3 defines the specification of the protocol that shall be implemented in the shipboard data server and also contains some examples.

C.2 Access control

Access to the shipboard data server with request-response protocols shall involve the appropriate authentication method (e.g. login ID and password).

Annex G shows an example of limiting access to the shipboard data server by requiring users to log in and enter a password.

C.3 Protocol specification

The shipboard data server provides request-response protocols in REST API. See Figure C.1.

REST API handles the following information: Time Series Data, Data Channel List and Alias List.

The information is obtained, added and updated in the following method of HTTP/HTTPS: GET, POST, PUT and TRACE. The manufacturer shall include the method, its function and parameter in the manufacturer's manual.

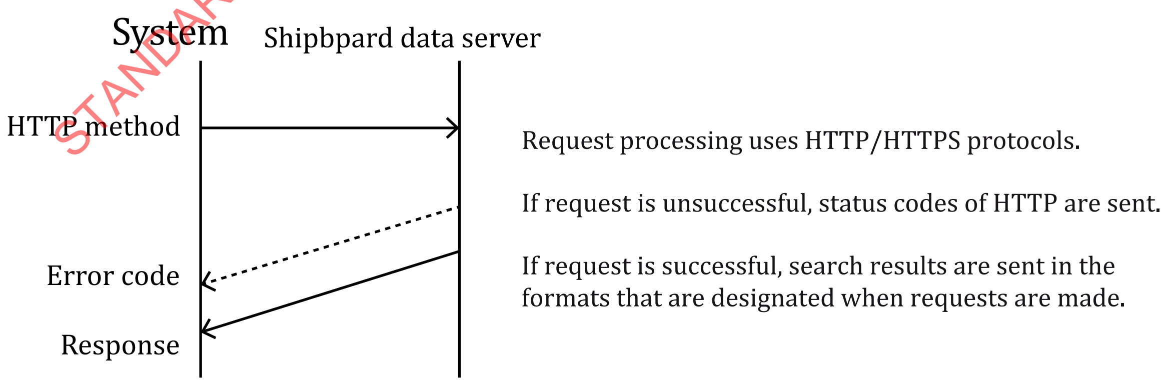

System
Shipbpard data server
HTTP method
Error code
Response
Request processing uses HTTP/HTTPS protocols.
If request is unsuccessful, status codes of HTTP are sent.
If request is successful, search results are sent in the formats that are designated when requests are made.

Figure C.1 — Structure of request-response protocols

The details of the request-response protocols are as follows.

a) Formats of requests made in request-response protocols

The structure of request-response protocols is shown in Table C.1.

When using the DataChannelType parameter, Make parameter, Query parameter, and Label parameter, the protocol shall conform to RFC 3986.

It is not necessary for the alphabet character in arguments and parameters to be case-sensitive.

Table C.1 — Structure of request-response protocols

Method	Service root	Resource path	Type parameter	Data Channel Type parameter	Make parameter	Query parameter	Label parameter
See C.3 b)	See C.3 c)	See C.3 d)	See C.3 e)	See C.3 f)	See C.3 g)	See C.3 h)	See C.3 i)

b) Functions and executions of request-response protocol methods

Methods that can be used in request-response protocols are shown in Table C.2.

When the shipboard data server receives a request from shipboard machinery and equipment, the shipboard data server shall record logs with an HTTP status code, the kind of HTTP method used, the times and dates, and the results.

It is desirable that logs be recorded in the syslog.

Table C.2 — Request-response protocol method

Method	Description	Implementation
GET	GET method retrieves the resources of the specified URI from the shipboard data server.	Mandatory
POST	POST method adds data of the message body to the shipboard data server. Resource path cannot be specified. It adds the latest data and sets values in a time series.	Mandatory
PUT	PUT method updates data of the message body to the shipboard data server. The resource path cannot be specified. It updates configuration values.	Optional

TRACE	TRACE method obtains the counting of resources of the specified URI from the shipboard data server.
	Units for counting information are as follows:
	type = data:[Time Series].[Local ID]
	type = sdd: [Local ID].[Data Channel Type].[History]
	type = alias: [Alias List].[History]
		Optional

c) Service root

Service root format and details are shown in Table C.3

Table C.3 — Details of service roots

Service root	Description	Usage	Example
<host>	Host name or IP address of the shipboard data server	Mandatory	192.168.1.253
<port>	HTTP port number	Optional	8080

d) Resource path

The resource path depends on the type parameter and method. It cannot be specified when executing POST and PUT methods.

Refer to e) for the details of the type parameter.

When the Data Channel Type is “LocalID”, Resource path format and details are shown in Table C.4.

When the Data Channel Type is “ShortID”, specify one Short ID defined in the Data Channel List. It is not possible to specify multiple Short IDs by separating Short ID with “/” or “,”.

When the Data Channel Type is “Alias”, specify one Alias ID defined in the Alias List. It is not possible to specify multiple Alias IDs by separating the Alias ID with “/” or “,”.

When the Data Channel Type is “Local ID”, in the case of the GET method, a wildcard is used in resource paths. See j) for more about wildcards.

Table C.4 — Details of resource paths

Resource path	Description	Usage	Example
< Naming Rule >	See ISO 19848:2024, 5.1.3	Mandatory	/jsmea_mac
< Local Data Name >	Can be used only when the Type parameter is either “data” or “sdd”.	Mandatory	/MainEngine//AirCooler/CoolingFreshWater/Inlet/Temp
Both resource path parameters in Table C.4 apply only when executing the GET method.			

e) Type parameter

Specify the data type to access resources in the shipboard data server.

Data type refers to Time Series Data, Data Channel List and Alias List.

Types of data that may be handled and ways to designate them are shown in Table C.5.

The type parameter is also used for methods other than the GET method.

The type parameter default is “data”.

The type parameter is specified in the message body.

Table C.5 — Details of type parameter

Types of data	Description	Number of appearances	Example
data	Handles Times Series Data	1	?type = data
sdd	Handles Data Channel List	1	?type = sdd
alias	Handles Alias List	1	?type = alias

f) Data Channel Type parameter

Specify the type of ID to access resources in the shipboard data server.

Types of Data Channel Type that may be handled and ways to designate them are shown in Table C.6.

Data Channel Type parameter default is “Local ID”.

Data Channel Type parameter is specified in the message body.

Table C.6 — Details of Data Channel Type parameter

Data Channel Type	Description	Number of appearances	Example
Local ID	Local ID is used to access resources on the shipboard data server.	1	?idtype = LocalID
Short ID	Short ID is used to access resources on the shipboard data server.	1	?idtype = ShortID
Alias ID	Alias ID is used to access resources on the shipboard data server. When type parameter is not Alias, only the GET method can be used.	1	?idtype = Alias

g) Make parameter

The make parameter specifies the destination of search results. Only the GET method can be used.

The destination shall be specified by full path.

The make parameter is specified in the message body.

The file created by the make parameter is acquired using the file input and output protocols (see Annex E).

EXAMPLE 1 ?make = /user/local/sds/IMO12345/ME_Data.xml

h) Query parameter

The query parameter is used to specify data format, change sort order, use filter, etc.

The request-response protocol shall be capable of handling the query parameter and the corresponding arguments in Table C.7.

The query parameter that may be used and its designation are shown in Table C.7.

More than one query parameter may be designated at a time.

When date and time are used for argument of parameter, they are designated in the format described as follows.

1) Absolute date and time:

The absolute date and time shall be designated in the format specified in ISO 8601-1.

2) Relative date and time:

The relative date and time are used to designate a date and time in the past based on the current time, not in the future.

The relative date and time are designated in the form of the Now (parameter).

The parameter sets the date and time backward from the current time of the shipboard data server. The parameter can be designated in the following duration format specified in ISO 8601-1.

P[n]Y[n]M[n]DT[n]H[n]M[n]S

P[n]W

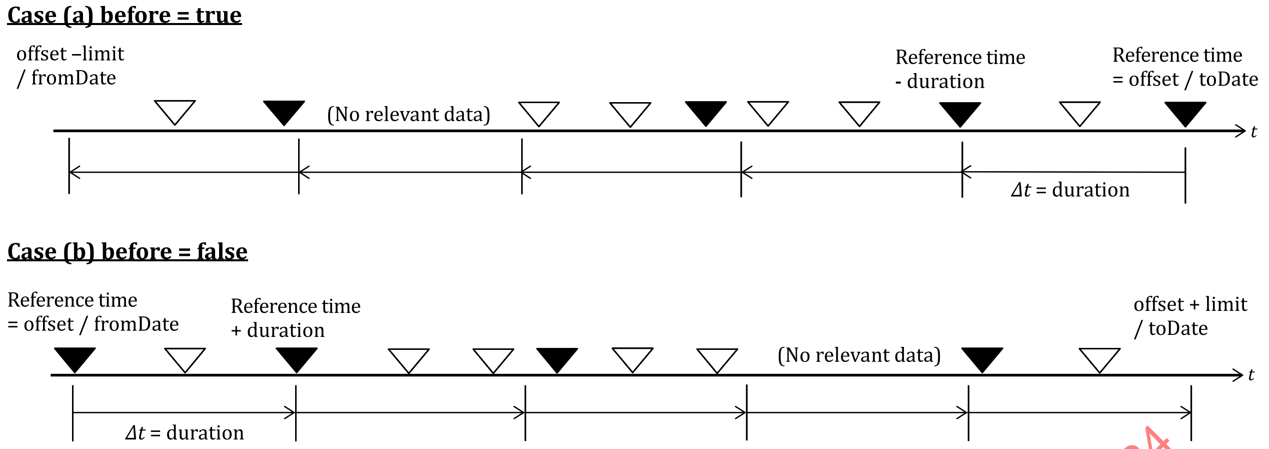
The query parameter is specified in the message body.

Table C.7 — Details of query parameters

Parameter name	Description	Default argument	Implementation	Example
?offset	Designate in UTC times and dates for obtaining data.	UTC at a time when server receives Method	Mandatory	?offset = 2016–03–31T00:00:00Z
?before	Designate whether the search is made before or after base times and dates (before: true, after: false). Can be used only when type parameters are "data".	true	Mandatory	?before = false
?header	Designate whether Time Series Data are output with or without Headers.	false	Mandatory	?header = true
?limit	Designate time frames to obtain on the second time scale, when types are "data". Designate the number of items to obtain in histories to obtain, when types are not "data". Return the latest information, when 1 is designated. Return the latest Data Channel List, when types are "sdd". Return the latest Data Source Information, when types are "siod". Return the latest Alias List, when types are "alias". The limit parameter cannot be used if the method is delete and the type parameter is not "data".	1	Mandatory	?limit = 5
?revisionfrom	When it is necessary to obtain the revision history of the Data Channel List and the Alias List, the date and time should be specified. This parameter searches the list whose time stamp of the Alias List or the Data Channel List is newer than the date and time specified. The revisionfrom parameter can be used if the type parameter is "sdd" or "alias".		Optional	?revisionfrom = 2016–03–31T00:00:00Z
?revisionto	When obtaining revision history of the Data Channel List and the Alias List, specify the date and time. This parameter searches the list whose time stamp of the Alias List or the Data Channel List is older than the date and time specified. It can be used simultaneously with revisionfrom. The revisionto parameter can be used if the type parameter is "sdd" or "alias".		Optional	?revisionto = 2015–04–01T23:59:59Z
?orderby	Designate either ascending or descending chronological orders for data obtained. (asc: ascending; desc: descending)	asc	Mandatory	?orderby = asc
?fromDate	Designate start date and time for obtaining data in UTC times and dates. This parameter can be used if the type parameter is "data". Use in conjunction with the toDate parameter. Designate a date and time earlier than the toDate parameter. This parameter cannot be used with the offset, limit, and before parameters If the above conditions are not met, a bad request (HTTP status code "400") is returned.		Mandatory	?fromDate = 2021–09–01T12:00:00Z
?toDate	Designate the end date and time for obtaining data in UTC times and dates. The toDate parameter can be used if the type parameter is "data". Use in conjunction with the fromDate parameter. Designate a date and time more recent than the fromDate parameter. This parameter cannot be used with the offset, limit, and before parameters. If the above conditions are not met, a bad request (HTTP status code "400") is returned.		Mandatory	?toDate = 2021–09–06T12:00:00Z

Table C.7 *(continued)*

Parameter name	Description	Default argument	Implementation	Example
?duration	Designate the data period for obtaining down sampled data. Designate in the duration format specified in ISO 8601-1. In the data down sampling method, data are obtained for each designated period based on the reference time (see Figure C.2). If the before parameter is true, search backward from the reference time to retrieve the most recent data from the next relevant time through to the next relevant time minus duration. — If the before parameter is false, search forward from the reference time to the future, and the oldest data contained in the next relevant time to the next relevant time + duration is retrieved. — When there is no corresponding data, there is no output of data corresponding to the time. — When the offset, limit, and before parameters are designated, the reference time is the time designated by the offset parameter. — When the fromDate and toDate parameters are designated, the reference time is the toDate when the before parameter is true, and the fromDate when the before parameter is false. Data are not interpolated. For example, if the stored data are in a period of one hour and the duration is one minute, data are output every hour because data interpolation is not performed. The duration parameter can be used if the Type option is "data". The limit parameter can be used with the duration parameter.		Mandatory	? duration = P4DT12H30M5S
?substr	Designate the specified substring to search partial matching of the Local ID. 1) The substring shall not be case-sensitive. 2) The substring shall not contain [\ ] [:] [*] [?] ["] [<] [>] [|] and any white space characters. 3) The length of the substring shall be less than or equal to 255 characters. It can be used in combination with the Wildcard filter shown in j), and when used together, it becomes an AND condition. When using "/", convert to the URL-encoded character "%2F".		Mandatory	?substr = "Cool"



Key

t	data time
▼	data to be retrieved
▽	data not retrieved

Figure C.2 — Down sampling method

i) Label parameter

Specify the priority of the output format of the column header when obtaining Time Series Data with the GET method.

If not specified, use Short ID and Local ID, in that order.

Table C.8 shows the label parameter that may be used and how to designate these parameters.

The label parameter is specified in the message body.

Table C.8 — Details of label parameters

Label type	Description	Number of appearances	Example
ShortID	Use ShortID with the highest priority. The Column header is used with the priority of ShortID, LocalID.	1	? label = ShortID
LocalID	Use LocalID with the highest priority.	1	? label = LocalID

j) Use of wildcard in resource paths

For the structure of resource paths, refer to the Local ID specified in ISO 19848:2024, 5.1.3.

Filters are created if wildcard in resource paths are used when obtaining Time Series Data, Data Channel List and Data Source Information saved in the shipboard data server.

Conditions for searching can be designated in the same way as MQTT protocol filters.

Wildcard strings of characters comprise the following:

— Multi-level wildcards represented by #. The multi-level wildcard is used to match any number of levels within a URI; however, it shall be the last character specified in the search string.

— Single-level wildcards represented by +. The single-level wildcard matches only one URI level.

As clients may replace “#” and “+” by their respective URL-encoded characters, the shipboard data server shall be able to handle both parameters. Therefore, the shipboard data server shall interpret the following:

— “%23” as multi-level wildcard (“#”)

— “%2B” as single level wildcard (“+”)

EXAMPLE 2 Search URI /jsmea_mac/MainEngine/AirCooler/+/Outlet/Temp.

Table C.9 shows search results with URI option using +.

Table C.9 — Search results with URI option using +

URI list	Match/Unmatch
/jsmea_mac/MainEngine/AirCooler/CoolingFreshWater/Outlet/Temp	Matched
/jsmea_mac/MainEngine/AirCooler/CoolingFreshWater/Inlet/Temp	Unmatched
/jsmea_mac/MainEngine/AirCooler/CoolingFreshWater/Outlet/Press	Unmatched
/jsmea_mac/MainEngine/AirCooler/ScavAir/Inlet/Temp	Unmatched
/jsmea_mac /MainEngine/AirCooler/ScavAir/Outlet/Temp	Matched
/jsmea_mac /MainEngine/Cylinder/ScavAir/Outlet/Temp	Unmatched

EXAMPLE 3 Search URI /jsmea_mac/MainEngine/AirCooler/CoolingFreshWater/#.

Table C.10 shows search results with URI option using #.

Table C.10 — Search results with URI option using #

URI list	Match/Unmatch
/jsmea_mac/MainEngine/AirCooler/CoolingFreshWater/Outlet/Temp	Matched
/jsmea_mac/MainEngine/AirCooler/CoolingFreshWater/Inlet/Temp	Matched
/jsmea_mac/MainEngine/AirCooler/CoolingFreshWater/Outlet/Press	Matched
/jsmea_mac/MainEngine/AirCooler/ScavAir/Inlet/Temp	Unmatched
/jsmea_mac /MainEngine/AirCooler/ScavAir/Outlet/Temp	Unmatched
/jsmea_mac /MainEngine/Cylinder/ScavAir/Outlet/Temp	Unmatched

EXAMPLE 4 Search substring “Cool”

Table C.11 shows search results with substring option.

Table C.11 — Search results with substring option

URI list	Match/Unmatch
/jsmea_mac/MainEngine/AirCooler/CoolingFreshWater/Outlet/Temp	Matched
/jsmea_mac/MainEngine/AirCooler/CoolingFreshWater/Inlet/Temp	Matched
/jsmea_mac/MainEngine/AirCooler/CoolingFreshWater/Outlet/Press	Matched
/jsmea_mac/MainEngine/AirCooler/ScavAir/Inlet/Temp	Matched
/jsmea_mac/MainEngine/AirCooler/ScavAir/Outlet/Temp	Matched
/jsmea_mac/MainEngine/Cylinder/ScavAir/Outlet/Temp	Unmatched

k) Return code of method

When the shipboard data server receives a method, it sends processing results and the HTTP status code (see Table C.12) to the sender.

Table C.12 — HTTP status code

Status code	Message	Description
200	OK	
201	Created	The URI of the resource newly created is returned.
400	Bad request	Syntax error
401	Unauthorized	User confirm error
403	Forbidden	Accessed an unauthorised directory and file
404	Not found	Data not available
405	Method not allowed (client error)	
408	Request time out	It did not result within a specific time
413	Payload too large	Accepted an unexpected request
500	Internal server error	Execute the unauthorised method
501	Not implemented	An attempt was made to execute a method or parameter that is not implemented.

C.4 Example of request-response protocol

The following a) to e) lists examples of request-response protocols.

a) Table C.13 shows an example of actual recorded data.

Table C.13 — Actual recorded data example

Time stamp	Local ID	Value
2016/11/25 06:43:00	/jsmea_mac/MainEngine/Cylinder1/ExhaustGas/Outlet/Temp	268
2016/11/25 06:43:00	/jsmea_mac/MainEngine/Cylinder2/ExhaustGas/Outlet/Temp	269
2016/11/25 06:43:00	/jsmea_macMainEngine/Cylinder3/ExhaustGas/Outlet/Temp	255
2016/11/25 06:43:00	/jsmea_macMainEngine/Cylinder4/ExhaustGas/Outlet/Temp	253
2016/11/25 06:43:00	/jsmea_macMainEngine/Cylinder5/ExhaustGas/Outlet/Temp	260
2016/11/25 06:43:00	/jsmea_macMainEngine/Cylinder6/ExhaustGas/Outlet/Temp	261
2016/11/25 06:43:00	/jsmea_mac/ MainEngine/FuelOilLine/FuelOil/Inlet/Press	0,75
2016/11/25 06:43:00	/jsmea_mac/ MainEngine/FuelOilLine/FuelOil/Inlet/Temp	131
2016/11/25 06:43:00	/jsmea_mac/ DieselGeneratorSet1/TurboCharger/ExhaustGas/Inlet/Temp	351
2016/11/25 06:43:00	/jsmea_mac/ DieselGeneratorSet2/TurboCharger/ExhaustGas/Inlet/Temp	360
2016/11/25 06:43:00	/jsmea_mac/ DieselGeneratorSet3/TurboCharger/ExhaustGas/Inlet/Temp	358
2016/11/25 06:43:01	/jsmea_mac/MainEngine/Cylinder1/ExhaustGas/Outlet/Temp	269
2016/11/25 06:43:01	/jsmea_mac/MainEngine/Cylinder2/ExhaustGas/Outlet/Temp	268
2016/11/25 06:43:01	/jsmea_mac/MainEngine/Cylinder3/ExhaustGas/Outlet/Temp	256
2016/11/25 06:43:01	/jsmea_mac/MainEngine/Cylinder4/ExhaustGas/Outlet/Temp	254
2016/11/25 06:43:01	/jsmea_mac/MainEngine/Cylinder5/ExhaustGas/Outlet/Temp	261
2016/11/25 06:43:01	/jsmea_macMainEngine/Cylinder6/ExhaustGas/Outlet/Temp	260
2016/11/25 06:43:01	/jsmea_mac MainEngine/FuelOilLine/FuelOil/Inlet/Press	0,76
2016/11/25 06:43:01	/jsmea_mac/ MainEngine/FuelOilLine/FuelOil/Inlet/Temp	131
2016/11/25 06:43:02	/jsmea_mac/MainEngine/Cylinder1/ExhaustGas/Outlet/Temp	267
2016/11/25 06:43:02	/jsmea_mac/MainEngine/Cylinder2/ExhaustGas/Outlet/Temp	270
2016/11/25 06:43:02	/jsmea_mac/MainEngine/Cylinder3/ExhaustGas/Outlet/Temp	258
2016/11/25 06:43:02	/jsmea_mac/MainEngine/Cylinder4/ExhaustGas/Outlet/Temp	256

Table C.13 *(continued)*

Time stamp	Local ID	Value
2016/11/25 06:43:02	/jsmea_mac/MainEngine/Cylinder5/ExhaustGas/Outlet/Temp	264
2016/11/25 06:43:02	/jsmea_mac/MainEngine/Cylinder6/ExhaustGas/Outlet/Temp	263
2016/11/25 06:43:02	/jsmea_mac MainEngine/FuelOilLine/FuelOil/Inlet/Press	0,77
2016/11/25 06:43:02	/jsmea_mac/ MainEngine/FuelOilLine/FuelOil/Inlet/Temp	134
2016/11/25 06:43:03	/jsmea_mac/MainEngine/Cylinder1/ExhaustGas/Outlet/Temp	268
2016/11/25 06:43:03	/jsmea_mac/MainEngine/Cylinder2/ExhaustGas/Outlet/Temp	270
2016/11/25 06:43:03	/jsmea_mac/MainEngine/Cylinder3/ExhaustGas/Outlet/Temp	258
2016/11/25 06:43:03	/jsmea_mac/MainEngine/Cylinder4/ExhaustGas/Outlet/Temp	254
2016/11/25 06:43:03	/jsmea_mac/MainEngine/Cylinder5/ExhaustGas/Outlet/Temp	261
2016/11/25 06:43:03	/jsmea_macMainEngine/Cylinder6/ExhaustGas/Outlet/Temp	261
2016/11/25 06:43:03	/jsmea_mac MainEngine/FuelOilLine/FuelOil/Inlet/Press	0,77
2016/11/25 06:43:03	/jsmea_mac/ MainEngine/FuelOilLine/FuelOil/Inlet/Temp	133
2016/11/25 06:43:04	/jsmea_mac/MainEngine/Cylinder1/ExhaustGas/Outlet/Temp	269
2016/11/25 06:43:04	/jsmea_mac/MainEngine/Cylinder2/ExhaustGas/Outlet/Temp	269
2016/11/25 06:43:04	/jsmea_mac/MainEngine/Cylinder3/ExhaustGas/Outlet/Temp	259
2016/11/25 06:43:04	/jsmea_mac/MainEngine/Cylinder4/ExhaustGas/Outlet/Temp	256
2016/11/25 06:43:04	/jsmea_mac/MainEngine/Cylinder5/ExhaustGas/Outlet/Temp	260
2016/11/25 06:43:04	/jsmea_mac/MainEngine/Cylinder6/ExhaustGas/Outlet/Temp	262
2016/11/25 06:43:04	/jsmea_mac/MainEngine/FuelOilLine/FuelOil/Inlet/Press	0,76
2016/11/25 06:43:04	/jsmea_mac/MainEngine/FuelOilLine/FuelOil/Inlet/Temp	132

b) POST method example

1) POST method

POST http://localhost/

{Transmission data in the format specified in ISO 19848 }

See ISO 19848:2024, A.2.4 c).

2) Results

The processing result is returned in the HTTP return code.

See Table C.12 HTTP status code.

c) GET method example

Execute the GET method for the actual recorded data in Table C.13.

GET http://localhost/+/+/+/ ExhaustGas /+/+

*?offset = 2016-11-25T06:43:03Z&before = true&limit = 2

Search conditions include:

a) ExhaustGas in Local ID,

b) date and time on 25 November 2016, 6:43:03 or earlier and

c) search over the last 2 seconds.

Table C.14 shows search results of an example of actual recorded data.

Table C.14 — Search results of actual recorded data example

Time stamp	Local ID	Value
2016/11/25 06:43:02	/jsmea_mac/MainEngine/Cylinder1/ExhaustGas/Outlet/Temp	267
2016/11/25 06:43:02	/jsmea_mac/MainEngine/Cylinder2/ExhaustGas/Outlet/Temp	270
2016/11/25 06:43:02	/jsmea_mac/MainEngine/Cylinder3/ExhaustGas/Outlet/Temp	258
2016/11/25 06:43:02	/jsmea_mac/MainEngine/Cylinder4/ExhaustGas/Outlet/Temp	256
2016/11/25 06:43:02	/jsmea_mac/MainEngine/Cylinder5/ExhaustGas/Outlet/Temp	264
2016/11/25 06:43:02	/jsmea_mac/MainEngine/Cylinder6/ExhaustGas/Outlet/Temp	263
2016/11/25 06:43:03	/jsmea_mac/MainEngine/Cylinder1/ExhaustGas/Outlet/Temp	268
2016/11/25 06:43:03	/jsmea_mac/MainEngine/Cylinder2/ExhaustGas/Outlet/Temp	270
2016/11/25 06:43:03	/jsmea_mac/MainEngine/Cylinder3/ExhaustGas/Outlet/Temp	258
2016/11/25 06:43:03	/jsmea_mac/MainEngine/Cylinder4/ExhaustGas/Outlet/Temp	254
2016/11/25 06:43:03	/jsmea_mac/MainEngine/Cylinder5/ExhaustGas/Outlet/Temp	261
2016/11/25 06:43:03	/jsmea_mac/MainEngine/Cylinder6/ExhaustGas/Outlet/Temp	261

For the output format, refer to ISO 19848:2024, A.2.4 c).

d) PUT method example

1) PUT method

PUT http://localhost/

{Transmission data in the format specified in ISO 19848}

See ISO 19848:2024, A.2.4 c).

Actual recorded data corresponding to TimeStamp and Local ID of DataSet Structure is updated.

2) Results

The processing result is returned in the HTTP return code.

See Table C.12 for details on the HTTP status code.

e) TRACE method example

Execute the TRACE method for the actual recorded data in Table C.13.

TRACE http://localhost/+/+/+/ ExhaustGas /#

?offset = 2016-11-25T06:43:02Z&before = true

Search conditions include:

a) ExhaustGas in Local ID, and

b) date and time on 25 November 2016, 6:43:02 or earlier.

Select in the past direction and the results are returned.

The processing results are returned in the HTTP return code and the number of records matching the search condition.

See Table C.12 for the HTTP status code.

The search results for the example in Table C.13 are returned at normal end as follows:

<Result>8</ Result >

Annex D
(normative)

Streaming protocol

D.1 General

The streaming protocol arranges data sent from the shipboard machinery and equipment to other equipment and systems in real time.

Examples of streaming protocols that the shipboard data server provide are given in D.3.

D.2 Access control

The shipboard data server with streaming protocols shall be accessed using the appropriate authentication method (e.g. login ID and password).

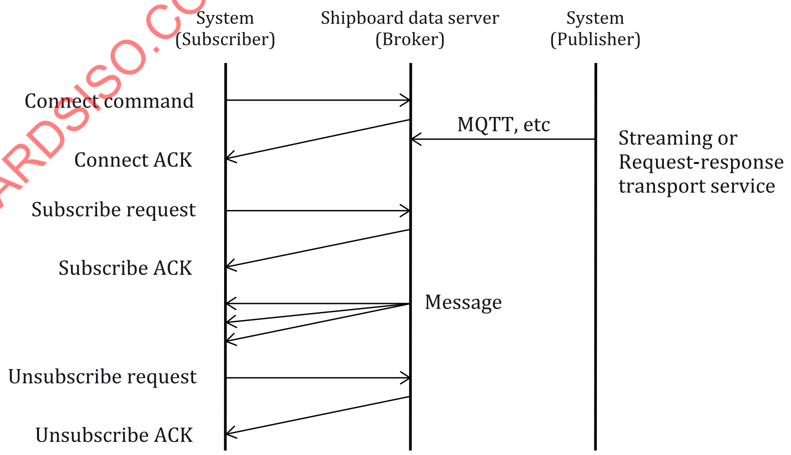
Annex G shows an example of limiting access to the shipboard data server by requiring users to log in and enter a password.

D.3 Protocol specification

The shipboard data server shall be provided with the broker and publisher functions of the MQTT protocol (see Figure D.1).

The shipboard data server can subscribe to data published by using MQTT or input by the request-response transport service in the data format specified in ISO 19848.

When the shipboard data server has a filtering function that complies with MQTT protocols, and subscriptions are requested in MQTT topics, the shipboard data server shall send data that fall under requested Local IDs as messages to subscribers in the format described in ISO 19848:2024, A.2.4 c) or A.3.4 b).



Key

ACK acknowledge

Figure D.1 — Protocol specification

The shipboard data server shall have the function of managing subscribers and managing their sessions by ID. Also, the session management function shall be provided so that the interrupted message can be transmitted.

MQTT streaming messages may adopt SSL/TLS or X.509 certificates. If encrypted data transfer is used between publisher/subscriber and broker (shipboard data server), a valid certificate is required.

Annex E
(normative)

File input and output protocol by the HTTP(S)

E.1 General

When using HTTP (HTTPS) to input files to, or output files from, the shipboard data server, the requirements described in this annex shall be met.

E.2 Structure of file input and output protocols by the HTTP(S)

Users shall access the shipboard data server using the appropriate authentication method (e.g. login ID and password).

E.3 Details of service roots by HTTP(S)

When storing a file using an http/https protocol, use the GET method.

The path that preserves a file is designated for each user.

The method of each protocol shall be able to handle multiple data with wildcards, such as those mentioned in a) to e).

a) Structure of file input and output protocols

The structure of file input and output protocols is as follows (for details refer to Table E.1):

[Method] [Service root]/[Resource path]/[File name]

Table E.1 — Structure of file input and output protocols

Method	Service root	Resource path	File name
GET	http://<host>[:port>]/	see E.3 d)	see E.3 e)
POST	http://<host>[:port>]/	see E.3 d)	see E.3 e)
PUT	http://<host>[:port>]/	see E.3 d)	see E.3 e)
DELETE	http://<host>[:port>]/	see E.3 d)	see E.3 e)

b) Function of method

Methods that may be used in file input and output protocols are shown in Table E.2.

When the method is input, logs may output on the status code for the method used, as well as request details, times and dates, and results.

It is recommended that logs are recorded in syslog.

Table E.2 — File input and output protocol method

Method	Description
GET	GET method retrieves the file of a specified URI from the shipboard data server.
POST	POST method adds the file of a specified URI to the shipboard data server
PUT	PUT method updates the file of a specified URI to the shipboard data server
DELETE	DELETE method deletes the file of a specified URI from the shipboard data server

c) Service root

The service root format and details are shown in Table E.3.

Table E.3 — Details of service roots

Service root	Description	Mandatory/optional	Example
<host>	Host name of the shipboard data server	Mandatory	192.168.1.253
<port>	HTTP port number	Optional	8080

d) Resource path

The user shall be provided a specified path allowing access.

e) File name

The file name shall meet the following requirements.

1) The file name shall not be case-sensitive.

2) The file name shall not start with "." (period).

3) The file name shall not contain [\ ] [/] [:] [*] [?] [”] [<] [>] [|] or any white space characters.

4) The length of the file name shall be less than or equal to 255 characters.

Annex F
(informative)

Data source information

F.1 General

The data source information defines the formats in which data providers supply data and identify communication protocols.

When the formats in which data providers send data do not comply with ISO 19847, users may convert the protocols by defining their relation to the data source information.

The data source information shall meet certain assumptions by defining XML schemas.

Examples of defining the data source information in W3C XML Schemas are discussed in F.5.

Examples of XML formulated in accordance with XML Schemas are shown in F.6.

F.2 Requirements for XML Schemas

XML Schemas are formulated in accordance with the requirements described in F.3 and F.4.

The minimum and maximum numbers of appearances are clearly defined.

To define data structure, the following standard data types listed in Table F.1 are used.

Table F.1 — Standard data types

Standard data type	XML Schema data type	Remarks
Integer	Integer	Integer number
Positive integer	Positive integer	Integer number that is 1 or larger
Non-negative integer	Nonnegative integer	Integer number that is 0 or larger
Real	Real	Single precision floating point number
Date Time	String	Format by ISO 8601-1. Refer to RFC 3339 for the augmented Backus-Naur form (ABNF).
String	String	Random string of characters
Boolean	Boolean	Truth value
Null		Null specifies the lack of a value (can be used for any data types)

XML Schemas are created to command XML to add Namespace to all elements and attributes.

EXAMPLE < sdd:NamingRule sdd:ID = ”JSMEA_MACHINERY_STD” >

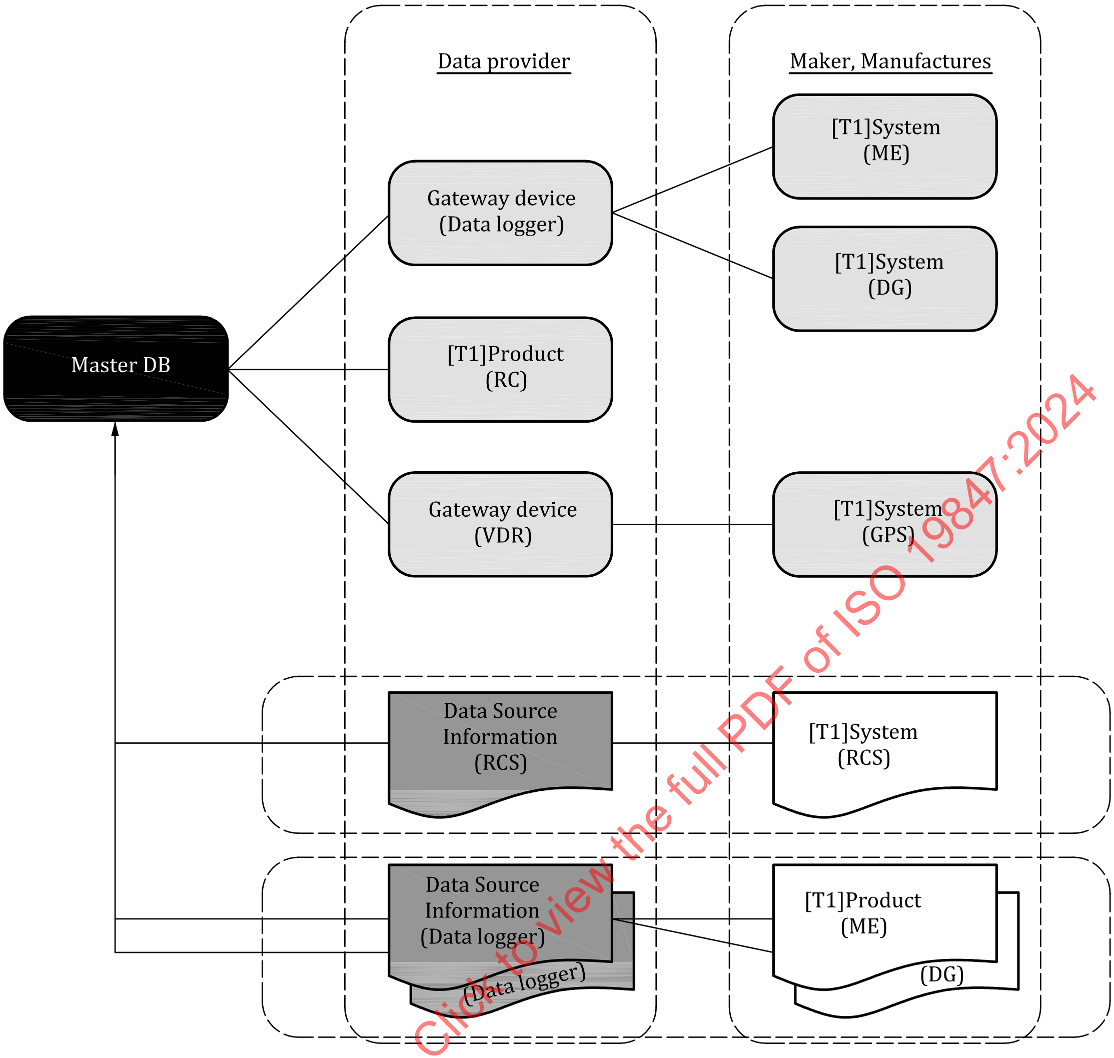
It is desirable to separate elements in Namespaces that are different in each Naming Rule from others.

F.3 Structure of Data Source Information

Each data provider may define the Data Source Information, respectively.

The Data Source Information and the Data Channel List are related to the Local ID.

Relations between the Data Source Information and the Data Channel List are shown in Figure F.1.



Key

DB	database	VDR	voyage data recorder
RC	remote control	ME	main engine
RCS	remote control system	DG	diesel generator
T1	tier 1		

Figure F.1 — Relations between Data Source Information and Data Channel List

The structure model of the Data Source Information is shown in Figure F.2 using UML. For more information on UML notation, see ISO/IEC 19505-1 and ISO/IEC 19505-2.

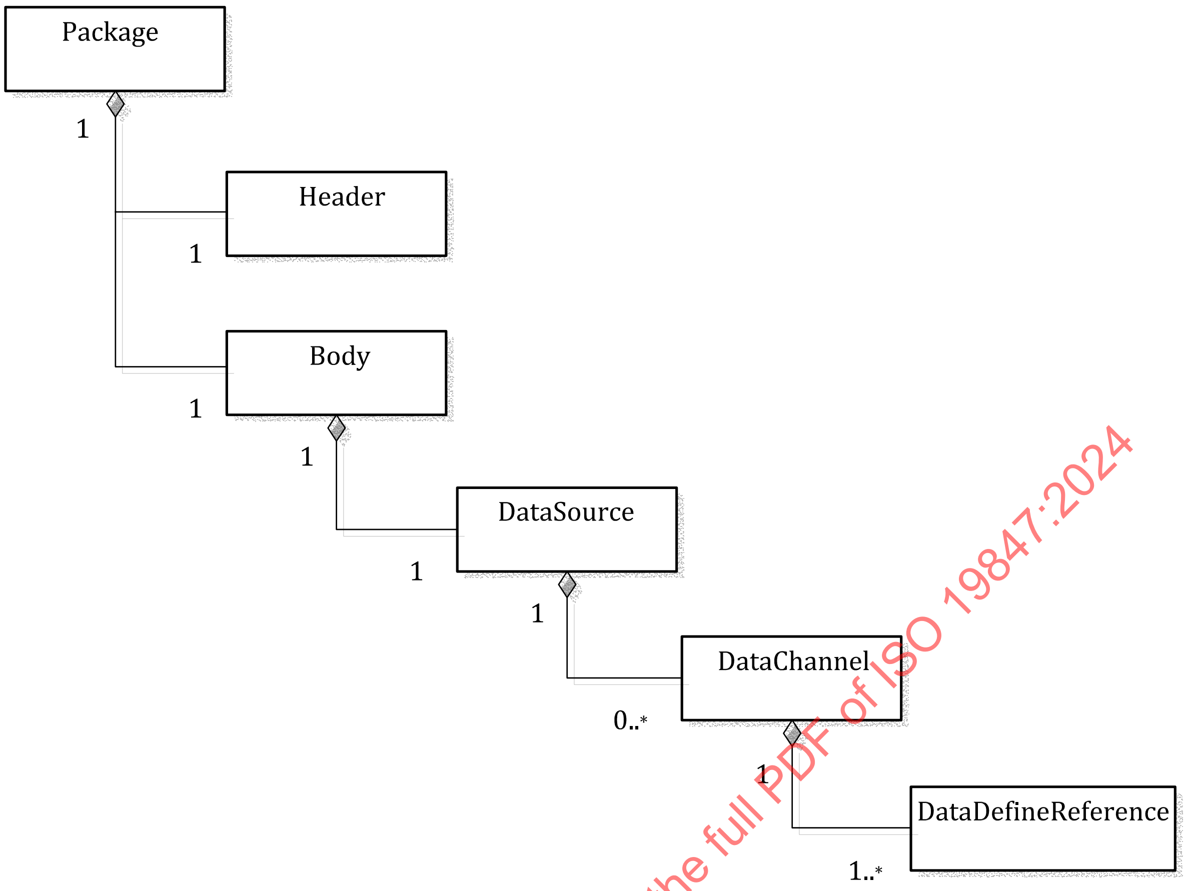


Figure F.2 — Structure model of Data Source Information

The different elements of the structure model are described in a) to f).

a) Package

The Package is data comprising Header, which is the metadata, and Body, which is the main data.

b) Header

The Header shows when the Body was created and who created it.

c) Body

The Body consists of DataSource and DataChannel, and defines Data Source and Data Channel.

d) DataSource

The DataSource elements indicate formats in which data providers supply data and information with which communication protocols are identified.

e) DataChannel

The DataChannel elements define ways to map input data elements in the Local ID, when formats other than designated in ISO 19487 are input.

f) DataDefineReference

The DataDefineReference elements indicate types of data to be handled and protocol definitions.

F.4 Logical structure of Data Source Information

The Data Source Information shall have the logical structure shown in Figure F.3 using UML. For more information on UML notation, see ISO/IEC 19505-1 and ISO/IEC 19505-2.

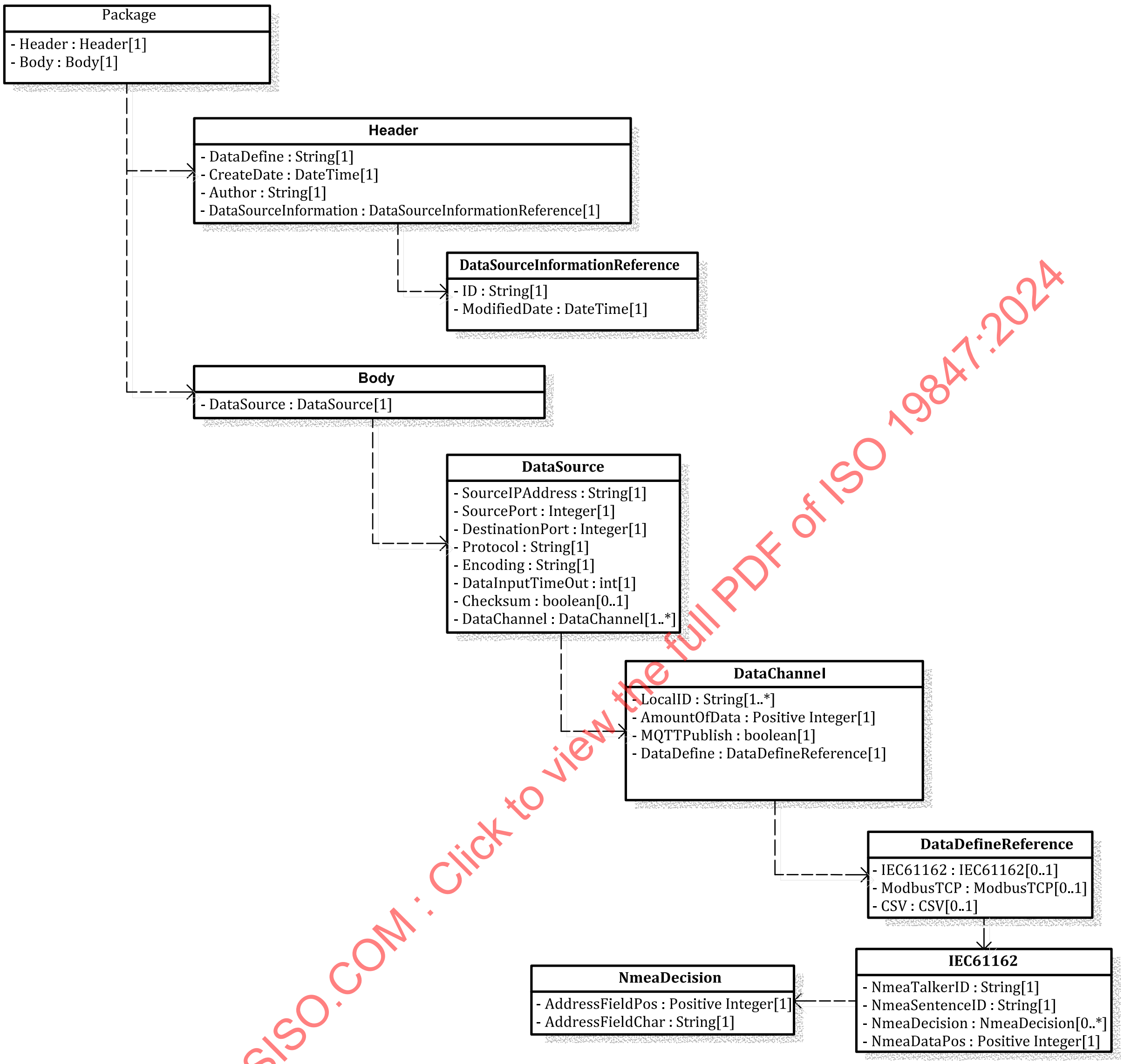

Package
- Header : Header[1]
- Body : Body[1]
Header
- DataDefine : String[1]
- CreateDate : DateTime[1]
- Author : String[1]
- DataSourceInformation : DataSourceInformationReference[1]
DataSourceInformationReference
- ID : String[1]
- ModifiedDate : DateTime[1]
Body
- DataSource : DataSource[1]
DataSource
- SourceIPAddress : String[1]
- SourcePort : Integer[1]
- DestinationPort : Integer[1]
- Protocol : String[1]
- Encoding : String[1]
- DataInputTimeOut : int[1]
- Checksum : boolean[0..1]
- DataChannel : DataChannel[1..*]
DataChannel
- LocalID : String[1..*]
- AmountOfData : Positive Integer[1]
- MQTTPublish : boolean[1]
- DataDefine : DataDefineReference[1]
DataDefineReference
- IEC61162 : IEC61162[0..1]
- ModbusTCP : ModbusTCP[0..1]
- CSV : CSV[0..1]
IEC61162
- NmeaTalkerID : String[1]
- NmeaSentenceID : String[1]
- NmeaDecision : NmeaDecision[0..*]
- NmeaDataPos : Positive Integer[1]
NmeaDecision
- AddressFieldPos : Positive Integer[1]
- AddressFieldChar : String[1]

Figure F.3 — Logical structure model of Data Source Information

The various elements of the logical structure model are described in Tables F.2 to F.9.

Table F.2 — Package structure

Name	Data type	Note	Mandatory/option	Max. count
Header	Header	See Table F.3	Mandatory	1
Body	Body	See Table F.4	Mandatory	1

Table F.3 — Header structure

Name	Data type	Note	Mandatory/option	Max. count
DataDefine	String	Description of this DataSourceInformation	Optional	1
CreatedDate	Date Time	Date when data are created	Optional	1
Author	String	Author of data	Optional	1
DataSourceInformationID	DataSource InformationReference	See Table F.5	Mandatory	1

Table F.4 — Body structure

Name	Data type	Note	Mandatory/option	Max. count
DataSource	DataSource	See Table F.6	Mandatory	1

Table F.5 — DataSourceInformationReference structure

Name	Data type	Note	Mandatory/option	Max. count
ID	String	Identifier of the Data Source Information list	Mandatory	1
ModifiedDate	Date Time	Modified Date and Time	Mandatory	1

Table F.6 — DataSource structure

Name	Data type	Description	Mandatory/option	Max. count
SourceIPAddress	String	IP address of sender	Mandatory	1
SourcePort	Integer	Port number of sender	Mandatory	1
DestinationPort	Integer	Port number of receiver	Mandatory	1
Protocol	String	ISO 19848/IEC 61162/http(https)/ftp(SFTP/FTPS)	Mandatory	1
Encoding	String	Designates types of character codes. (ASCII/JIS/Shift-JIS/EUC/UNICODE1.1/UNICODE2.0)	Mandatory	1
DataInputTimeOut	Non-Negative integer	Time-out period of data input	Mandatory	1
Checksum	Boolean	Checksum	Optional	1
DataChannel	DataChannel		Mandatory	Unlimited

Table F.7 — DataChannel structure

Element	Data type	Description	Mandatory/option	Max. count
LocalID	String	See ISO 19848:2024, 5.1.3	Mandatory	Unlimited
AmountOfData	Positive Integer	Number of data structures contained.	Optional	1
MQTTPublish	Boolean	Whether to publish in MQTT Topic or not (True/False)	Mandatory	1
DataDefine	a) DataDefineReference	See a)	Mandatory	1
Suffix	String	See ISO 19848:2024, Table B.1	Optional	1

a) DataDefineReference

Definition details vary depending on data types and protocols.

The definition of DataDefineReference depends on the protocol.

When handling general IEC 61162-1 sentence transmission protocols, see Table F.8.

Table F.8 — Examples of elements for handling general IEC 61162-1 formatted sentence transmission protocols

Element	Data type	Description	Mandatory/option	Max. count
NmeaTalkerID	String	IEC 61162-1 Talker IDs	Mandatory	1
NmeaSentenceID	String	IEC 61162-1 Sentence IDs	Mandatory	1
NmeaDecision	NmeaDecision	Condition deciding the effectiveness of the value. When all of the conditions are true the value is valid. See Table F.9	Optional	3
NmeaDataPos	Positive integer	Column index handled as a point for measuring data from IEC 61162-1	Mandatory	1

Table F.9 — Examples of elements for Nmea Decision

Element	Data type	Description	Mandatory/option	Max. count
AddressFieldPos	Positive integer	Column index handled as a point for measuring IEC 61162-1 data	Mandatory	1
AddressFieldChar	String	Column index for judging IEC 61162-1 data effectiveness	Mandatory	1

F.5 Example of XML Schema — Namespace:SIOD (Ships Server Input and Output Definition)

a) The following shows an example of general IEC 61162-1 formatted sentence transmission protocol.

```
<?xml version="1.0" encoding="utf-8"?>
<xs:schema xmlns:xs="https://www.w3.org/2001/XMLSchema"
         attributeFormDefault="unqualified"
         elementFormDefault="qualified" targetNamespace=
         "ISO19847/SHIP_SERVER_INPUT_AND_OUTPUT_DEFINITION"
         xmlns:siod="ISO 19847/SHIP_SERVER_INPUT_AND_OUTPUT
         _DEFINITION">

  <xs:element name="Package" type="siod:Package"/>

  <xs:complexType name="Package">
    <xs:sequence>
     <!--F.4 a) Header Structure-->
     <xs:element name="Header" type="siod:Header" minOccurs="0"
      maxOccurs="1"/>
     <!--F.4 b) Body Structure-->
     <xs:element name="Body" type="siod:Body" minOccurs="0"
      maxOccurs="1"/>
     </xs:sequence>
     </xs:complexType>

  <xs:complexType name="Header">
    <xs:sequence>
      <!—->
```