INTERNATIONAL STANDARD

ISO 19847

First edition
2018-10

Ships and marine technology — Shipboard data servers to share field data at sea

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

Reference number
ISO 19847:2018(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
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 documents 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).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

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*.

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 for operating ships safely and efficiently are becoming more and more popular.

These applications need to access data provided by shipboard machinery and equipment.

Navigational instruments may 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 standardised.

For the purpose of sharing field data at sea, including non-standardised machinery data, ISO 19847 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 governed by ISO 16425. The requirements to cyber security of shipboard data server refer to ISO 16425.

Ships and marine technology — Shipboard data servers to share field data at sea

1 Scope

This document specifies requirements for the shipboard data server that is 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.

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, *Data elements and interchange formats — Information interchange — Representation of dates and times*

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

ISO 19848, *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 61162-1, *Maritime navigation and radiocommunication equipment and systems — Digital interfaces — Part 1: Single talker and multiple listeners*

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

3 Terms and definitions

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

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

— IEC Electropedia: available at https://www.electropedia.org/

— ISO Online browsing platform: available at https://www.iso.org/obp

3.1
actual recorded data
actual (sensor) data acquired from *data providers* (3.10) and recorded to the *shipboard data server* (3.32)

3.2
Alias ID
symbol to refer to one or more *Local IDs* (3.20) with different names

3.3
Alias List
defined list

3.4
Comma-Separated Value
CSV
method of storing tabular data in plain text in a file where each row of the file forms a data record and where fields within one data record are separated by a comma character

3.5
Data Channel
virtual channel for data transmission from shipboard machinery and equipment to the *shipboard data server* (3.32), defining static properties of data

[SOURCE: ISO 19848:2018, 3.5]

3.6
Data Channel ID
identifier for *Data Channel* (3.5) that identifies Data Channel universally and on-board a ship

Note 1 to entry: There are three types of Data Channel ID: Universal ID, *Local ID* (3.20) and Short ID.

[SOURCE: ISO 19848:2018, 3.6]

3.7
Data Channel List
list of definitions for *Data Channel* (3.5) that define *Data Channel ID* (3.6) and *Data Channel Property* (3.8), and is shared through the *shipboard data server* (3.32)

[SOURCE: ISO 19848:2018, 3.7]

3.8
Data Channel Property
attributes of *Data Channel* (3.5), such as units, ranges and others

[SOURCE: ISO 19848:2018, 3.8]

3.9
Data Channel Type
identification of the types of *Data Channels* (3.5), such as row numeric value, average value, alarms and status

Note 1 to entry: See ISO 19848:2018, 5.3 a).

3.10
data provider
equipment that provides (sends) data to the *shipboard data server* (3.32) and has interfaces for providing data

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

3.12
data sample
one measurement datum that has one timestamp

3.13
Extensible Markup Language
XML
text-based data description language used for exchanging data on the Internet

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 *FTP* (3.14) with Secure Sockets Layer (SSL) or Transport Layer Security (TLS)

3.16
Hypertext Transfer Protocol
HTTP
communication protocol used to exchange HTML(Hyper Text Markup Language) or other contents on the Internet

Note 1 to entry: See RFC 2616 “Hypertext Transfer Protocol”.

3.17
Hypertext Transfer Protocol over SSL/TLS
HTTPS
protocol in which Web servers and clients encrypt data transmissions

3.18
Java Script Objection 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 *XML* (3.13).

3.19
Local Data Name
identifier for *Data Channels* (3.5) that is named in accordance with a *Naming Rule* (3.23)

Note 1 to entry: The syntax of the identification string shall be disclosed and precisely defined using ABNF.

Note 2 to entry: See ISO 19848:2018, 5.2.2 b).

3.20
Local ID
identification of an on-board *Data Channels* (3.5) locally, consists of a *Naming Rule* (3.23) and a *Local Data Name* (3.19)

Note 1 to entry: See ISO 19848:2018, 5.2.2.

3.21
management data
catalogues that allow access to and interpretation of recorded data

EXAMPLE Timestamped *Data Source Information* (3.11), *Data Channel List* (3.7) and *Alias List* (3.3).

3.22
MQTT Protocol
machine-to-machine (M2M)/"Internet of Things" connectivity protocol designed as an extremely lightweight publish/subscribe messaging transport

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

3.23
Naming Rule
sets 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 19848:2018, 5.2.2 a).

3.24
Network File System
NFS
distributed file system and a protocol for distributed file systems defined by RFC 1094, RFC 1813, RFC 3530 and other protocol specifications

3.25
owner
restrict editors and users by a specifying owner

3.26
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]

3.27
REST API
program invocation convention for using Web systems from outside, developed in accordance with the architectural style called REST

Note 1 to entry: Resource operations are designated by *HTTP* (3.16) sources. Results are sent back in *XML* (3.13), *JSON* (3.18) and other formats.

3.28
Secure File Transfer Protocol
SFTP
protocol that uses the *SSH* (3.29) protocol to securely transfer files between computers

3.29
Secure Shell
SSH
cryptographic protocol that allows secure communications over an unsecured network

3.30
session
stateful or stateless dialogue established to exchange data between a *shipboard data server* (3.32) and shipboard equipment or systems

3.31
Server Message Block
SMB
protocol for sharing files and printers among several Windows computers in networks

3.32
shipboard data server
ship's "information hub" that stores data from shipboard machinery and equipment, shares data at sea including machine data, and sends stored data outboard

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 these products.

3.33
Syslog
standard for message logging

4 Abbreviated terms

AMS	Alarm Monitoring 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	Hyper Text Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol over SSL/TLS
JSON	Java Script Objection Notation
MQTT	Message Queuing Telemetry Transport
NFS	Network File System
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
TLS	Transport Layer Security
URI	Uniform Resource Identifier
UTC	Coordinated Universal Time
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

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, etc.

5.1.1.1 Input data processing performance

The shipboard data server using the request-response transport service shall have a processing performance to input data for 30 data sample sets at less than one-second from at least five simultaneous sessions (e.g. VDR, GNSS, alarm and monitoring systems, ballast systems and cargo systems). See Figure 1.

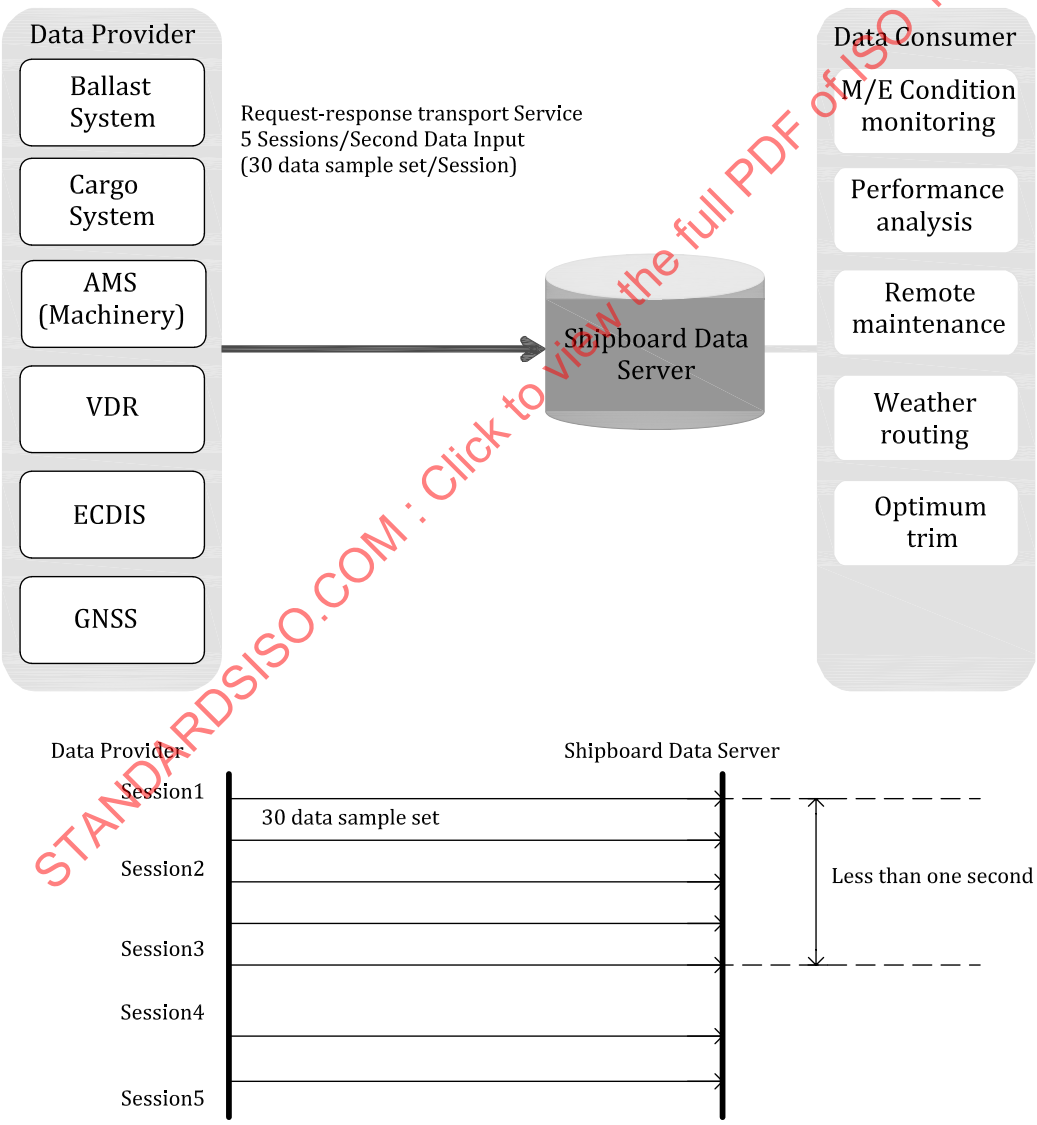

Figure 1 — Input data processing performance requirement

5.1.1.2 Output data processing performance

The shipboard data server using the request-response transport service shall have a processing performance to respond within five seconds against read requests for 30 data sample sets from a database having a maximum size as declared by the manufacturer and simultaneously from at least five sessions (for example main engine condition monitoring, weather-routing, optimum trim, remote maintenance and performance analysis). See Figure 2.

The shipboard data server using the File transport service shall have a processing performance to respond within five seconds against read requests for 30 data sample sets from database having a maximum size as declared by the manufacturer on at least one session. See Figure 2.

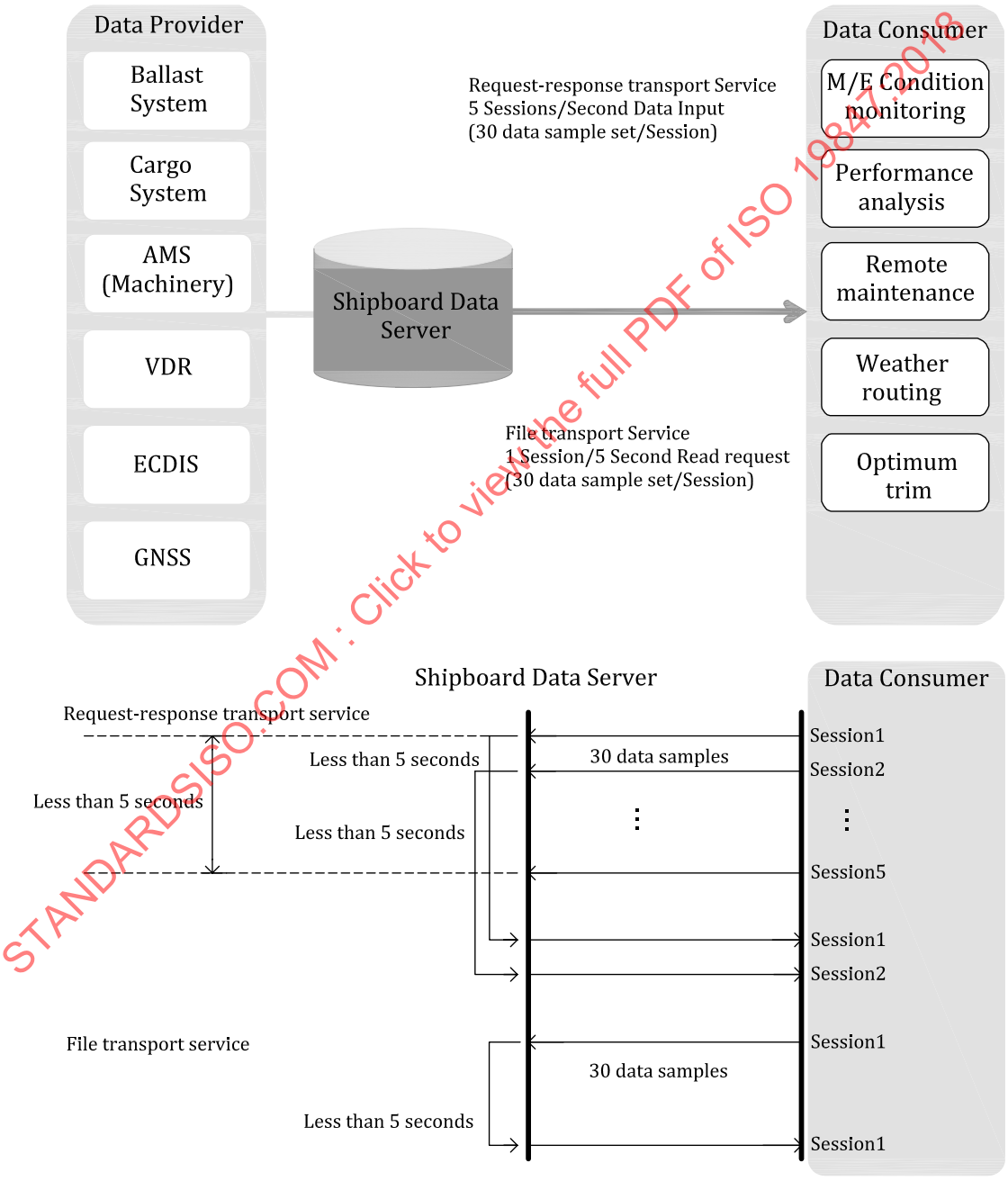

Figure 2 — Output data processing performance requirement

5.1.1.3 Streaming transport processing performance

The shipboard data server using the streaming transport service shall have a processing performance to input of 150 data sample sets at less than one-second to at least one session.

The shipboard data server using the streaming transport service shall have a processing performance to output of 150 data sample sets at less than one-second to at least two sessions by 150 input data sample sets (e.g. condition monitoring and performance analysis system). See Figure 3.

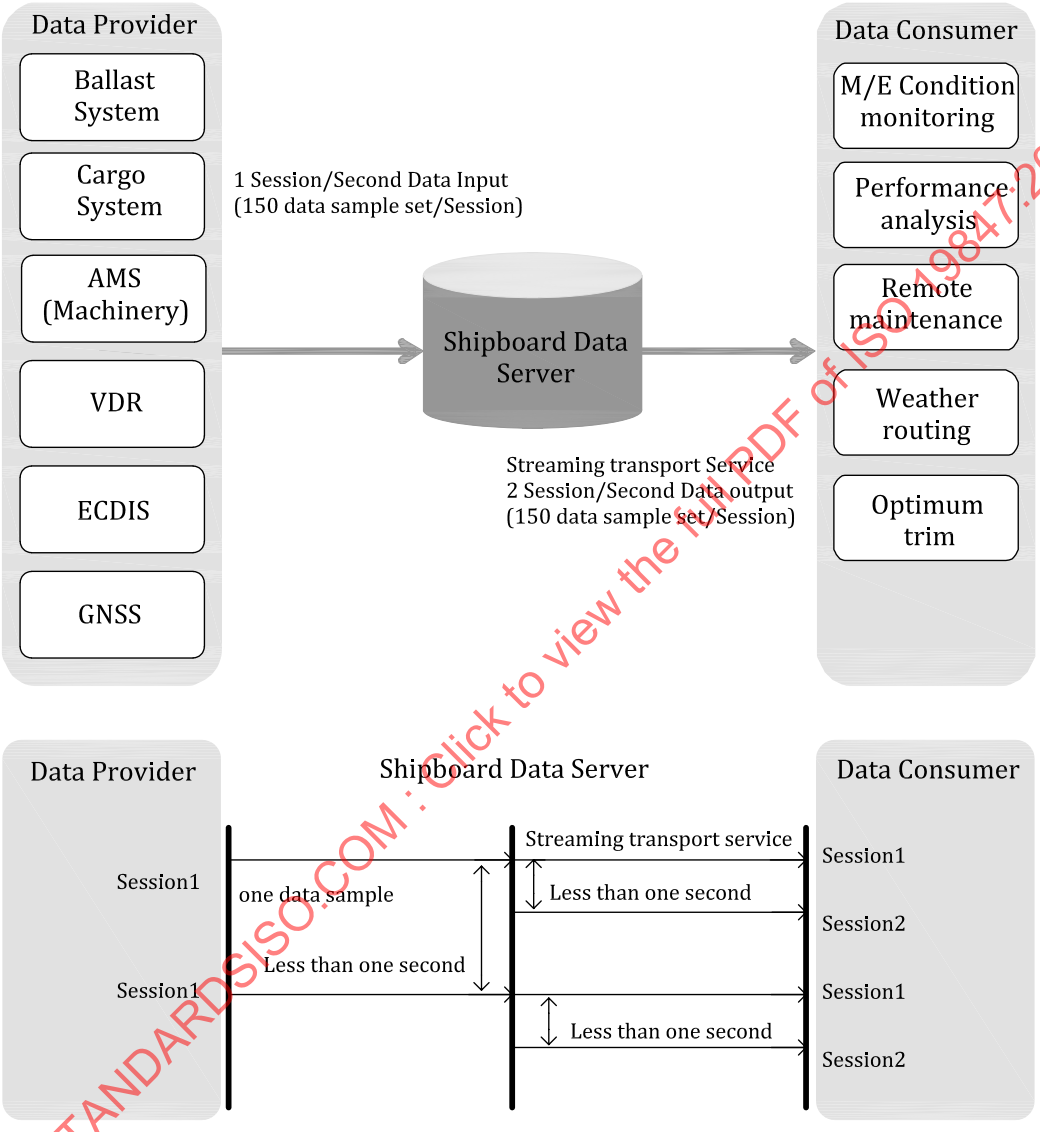

Figure 3 — Streaming transport processing performance requirement

5.1.2 Storage function

The shipboard data server shall be able to store input data, which are defined in 6.3.1, for at least 30 days.

The manufacturer shall give guidance in a user or installation manual on how much storage space is required per one record. Information about total storage capacity within the ship data sever shall also be provided.

The shipboard data server shall provide means to assist the user in estimating if the total storage capacity of the shipboard data server is sufficient for the required time period.

NOTE The shipboard data server can have a redundant function to protect management data and actual recorded data (e.g., 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 Mbps or greater.

NOTE The shipboard data server can also have other interfaces capable of serial communications or other means for input of 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;

e) storage device full or having insufficient capacity for storing configured records up to 30 days.

The shipboard data server shall be able to report the above statuses to other systems on-board (see 5.1.8) and may provide local indication for the above 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.

5.1.7 VDR security

5.1.7.1 Physical protection

Unused connection points such as USB ports shall be physically blocked from easy access by a user without a tool or key.

5.1.7.2 Operational protection

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

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).

For other operations with other USB device classes and non-USB REDS, the manufacturer shall provide information about the technology used and how the connection point fulfils the requirement to limit connection to only data [storage devices] [sources].

5.1.7.3 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 files 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.

5.1.7.4 Non-executable data verification

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

5.1.8 Status reporting

The shipboard data server shall be provided with a status reporting interface. The interface shall as a minimum consist of one relay contact output capable of signalling normal/abnormal status of the shipboard data server. The relay contact output may be replaced by other means, as specified by the manufacturer, which allow ship's personnel to identify a related failure of the shipboard data server.

NOTE An alternate method to the relay contact output can be based for example on provision of specific status display at ship data server or on generating priority caution alerts in the shipboard data sever and reporting the alerts to other systems on-board by employing IEC 61162-1 sentences ACN, ALF, ALC, ARC and HBT.

5.2 Environmental performance of shipboard data server

5.2.1 Power-supply performance

The shipboard data server shall have satisfied the test requirements of the power supply performance of IEC 60092-504.

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

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 have satisfied the test requirements of the vibration test of IEC 60092-504.

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

5.2.3 Requirement for electromagnetic immunity and emission

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

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

5.2.4 Temperature and humidity resistant requirements

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

— No.6, Cold with graduate change of temperature;

— No.7, Dry Heat with graduate change of temperature;

— No.8, Damp Heat cyclic.

Where electrical equipment is installed within environmentally controlled spaces, the ambient temperature for which the equipment is to be suitable may be reduced from 0 °C to 45 °C.

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

For the definition of the control space, refer to the following:

— the equipment is not for use for emergency services;

— temperature control is achieved by at least two cooling units arranged, so that in the event of loss of one cooling unit, for any reason, the remaining unit(s) is capable of satisfactorily maintaining the design temperature;

— the equipment is able to be initially set to work safely within a 45 °C ambient temperature until such a time that the lesser ambient temperature may be achieved; the cooling equipment is to be rated for a 45 °C ambient temperature;

— 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

Data management function comprises time stamping of Data Channel List, Data Source Information, and Alias List based on 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 authorised sources. See 6.3.

6.2.1 Management of system clock

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

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

b) Drift in 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 1 s, 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.

6.2.2 Management of Data Channel List

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

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

b) When 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.

6.2.3 Management of Data Source Information

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

Refer to Annex F for Data Source Information.

a) Data Source Information shall be able to be added, updated and deleted by data input functions.

b) When Data Source Information is added, 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.

6.2.4 Management of Alias List

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

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

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

b) When 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.

6.3 Data input and output functions

The shipboard data server shall have interface functions that meet the following requirements. 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 Data Source Information.

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

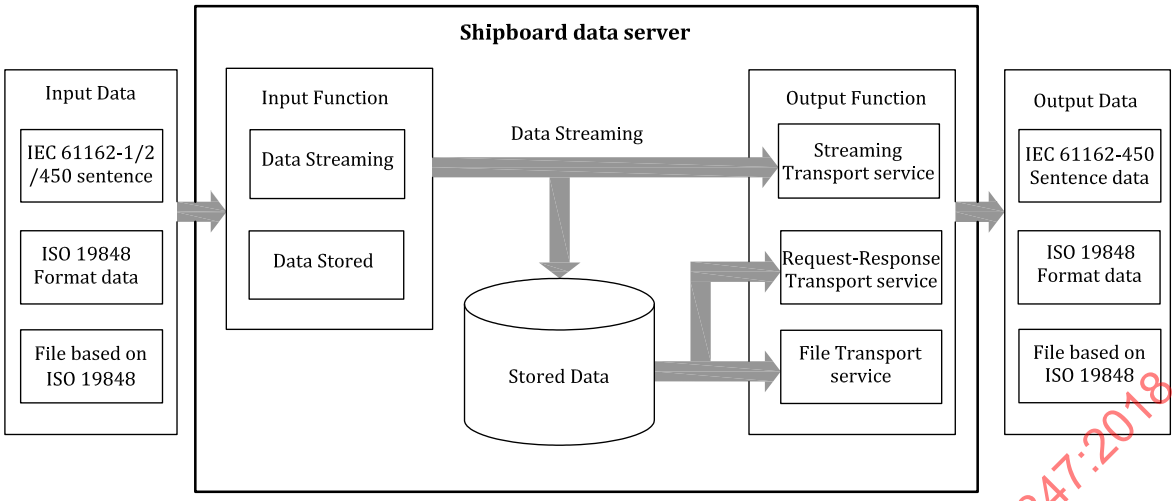

Figure 4 — Data input and output concept model

6.3.1 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 ISO 19848 data format and the sentence specified in general IEC 61162-1 sentence transmission of IEC 61162-450 and the file defined by ISO 19848, all of which are defined in the data source information of the shipboard data server.

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 defined in 6.3.1 a) by the protocol defined in Annex C and Annex D.

d) The shipboard data server may receive the file defined in 6.3.1 a) by 6.3.5.

6.3.2 Output function

The shipboard data server shall conform to the output function of XML specified in A.2 of ISO 19848:2018.

In addition, the shipboard data server may have the output function of JSON and CSV specified in A.3 and A.4 of ISO 19848:2018.

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 A.2 of ISO 19848:2018 and the IEC 61162-1 sentence data format and the file defined by ISO 19848.

b) The shipboard data server shall send data defined in 6.3.1 a) by 6.3.3 and 6.3.4.

c) The shipboard data server shall send the file defined in 6.3.1 a) by 6.3.5.

6.3.3 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 A.2 of ISO 19848:2018 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 6.3.5.

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

6.3.4 Streaming data transport service

The streaming data transport services offer a function of sending the latest 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.

6.3.5 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 A.2 of ISO 19848:2018. 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 FTP and HTTP file transport protocols as described in Annex E. Other protocols such as FTPS, SFTP, HTTPS for transport and SMB or NFS for file sharing may also be supported.

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 shall be provided with an Alias Function. The alias function is executed by the GET method of request-response transport service.

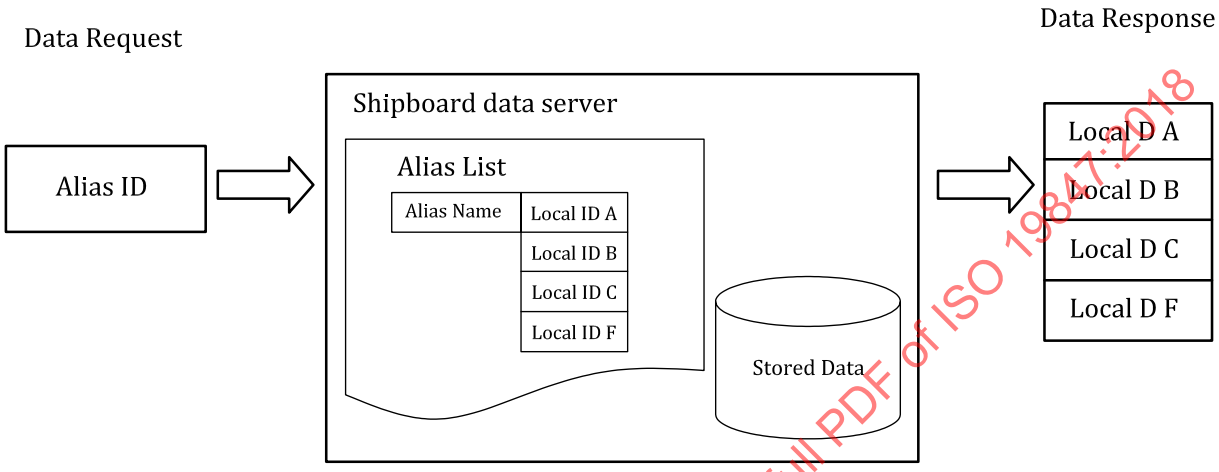

Figure 5 — Alias function

6.4.2 Alias List

The alias function is managed in Alias List.

With Alias List, virtual ID registration to be used with the shipboard data server can be done, the virtual ID shall be unique within the shipboard data server.

A virtual ID is called an Alias ID and may have a function of limiting use by the user.

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

For details of Alias List refer to Annex B.

6.5 Data calculation function

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

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

For 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: Data Channel List, Data source information and adjustment of system clock.

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 at least for the last 30 days.

7 Test requirements

7.1 Outline

The manufacturer of the shipboard data server shall carry out tests on general requirements and on data input/output and management, and document the methods and results in a test report.

Inspectors shall check the test reports to confirm that the shipboard data server complies with ISO 19847.

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.

7.2 Tests on general requirements

7.2.1 Test environments

The shipboard data server shall be tested against the general requirements specified in IEC 60092-504. For the purposes of IEC 60092-504, the following definitions apply.

Performance test: Confirm that using request-response transport service from five sessions with input and output of 30 data sample, and using streaming transport service from two sessions, can perform the output of one data sample set, and using file transport service from one session with output of 30 data sample the file defined by ISO 19848 at the same time.

Performance check: Confirm that condition monitoring of 5.1.4 functions normally.

7.2.2 Test items

a) Processing performance

(See 5.1.1.1)

Confirm by inspection of the manufacturer's documentation that the shipboard data server has processing performance to input data for 30 data sample at one-second from at least five simultaneous sessions by using the request-response transport service.

(See 5.1.1.2)

Confirm by inspection of the manufacturer's documentation that the shipboard data server has processing performance to read requests for 30 data sample at five seconds intervals on at least five simultaneous sessions by using the request-response transport service.

Confirm by inspection of the manufacturer's documentation that the shipboard data server has processing performance to read requests for 30 data sample at five seconds intervals on one session by using the File transport service.

(See 5.1.1.3)

Confirm by inspection of the manufacturer's documentation that the shipboard data server can process input of one data sample set at one-second intervals to at least one session by using the streaming transport service.

Confirm by inspection of the manufacturer's documentation that the shipboard data server can handle two requests made at the same time within one second by using the streaming transport service.

b) Storage function

(See 5.1.2)

Confirm by inspection of the manufacturer's documentation that the total storage capacity and storage capacity required to store one record is described in the instruction manual. Confirm by observation that the shipboard data server has a function to calculate the storage capacity needed to store all the data that is configured to be recorded, for a period of 30 days, and inform the user about the result of the calculation.

c) Interface function

(See 5.1.3)

Confirm by inspection of the manufacturer's documentation that the shipboard data server has interfaces where data are sent and received at a speed of 100 Mbps or faster.

d) Data backup and restoration functions

(See 5.1.4)

Confirm by inspection of the manufacturer's documentation that the shipboard data server has a function to monitor statuses.

e) Function to have connections with external storage devices

(See 5.1.5)

Confirm by inspection of the manufacturer's documentation that the shipboard data server has a function to export actual recorded data to external storage devices.

f) Function to be protected from unauthorised access

(See 5.1.6)

Confirm by inspection of the manufacturer's documentation that the shipboard data server is protected from unauthorised access.

g) Function to be protected from REDS

(See 5.1.7)

Confirm by analytical evaluation that the shipboard data server provides adequate means for physical and operational protection against REDS related security threats and provides means to protect the shipboard data server against executable files and non-executable data that originate from REDS.

h) Status reporting

(See 5.1.8)

Confirm by inspection of the manufacturer's documentation that the shipboard data server has a status reporting interface.

i) Power-supplying function

(See 5.2.1)

Confirm by inspection of the manufacturer's documentation.

j) Vibration-resistant feature

(See 5.2.2)

Confirm by inspection of the manufacturer's documentation.

k) Requirement for Electromagnetic immunity and Emission

(See 5.2.3)

Confirm by inspection of the manufacturer's documentation.

l) Temperature and humidity resistant requirements

(See 5.2.4)

Confirm by inspection of the manufacturer's documentation.

If the operating temperature of the shipboard data server is declared to be between 0 and 45° C, it shall be confirmed that information is provided indicating that the only allowable installation place is a climate controlled space.

m) Installation manual

(See 5.3.1 to 5.3.3)

Confirm by inspection of the manufacturer's documentation that the installation manuals describe maintenance procedures for the shipboard data server.

7.3 Tests on input/output and management functions

7.3.1 Test environments

The shipboard data server shall be tested against the general requirements contained in IEC 60092-504.

The shipboard data server shall be tested in advance and certified with documents and other evidence.

7.3.2 Test items

a) Management of the system clock

(See 6.2.1)

Confirm by inspection of the manufacturer's documentation that the shipboard data server has a function to synchronise the internal system clock with UTC.

It is necessary to confirm that the shipboard data server's system clock has a precision of one second or less per hour, regardless of whether the shipboard data server is synchronised to UTC or not.

Confirm that the shipboard data server has a function to release an alert when it is no longer synchronised with UTC.

b) Management of data to be processed

(See 6.2.2, 6.3.1 and 6.3.2)

Confirm by inspection of the manufacturer's documentation that the shipboard data server is able to actual recorded data regardless of the validity or existence of the associated UTC time stamp derived from the data source.

Confirm by inspection of the manufacturer's documentation that the shipboard data server has a function to process data formats that are defined in ISO 19848.

Confirm by inspection of the manufacturer's documentation that the shipboard data server has a function to process data formats that are defined in general IEC 61162-1 sentence transmission of IEC 61162-450.

c) Management of Management data

(See 6.2.2, 6.2.3 and 6.2.4)

Confirm by inspection of the manufacturer's documentation that the shipboard data server has a function to record management data.

Confirm by inspection of the manufacturer's documentation that the shipboard data server has a function to record configuration information data as well as dates, times and details of revisions when management data are revised.

Confirm by inspection of the manufacturer's documentation that the shipboard data server has a function to provide recorded management data when requests are made to do so.

Confirm by inspection of manufacturer's documentation and observation that the shipboard data server has an access control method and that it is used to control the access to actual recorded data and the changes in management data;

Confirm by observation that the shipboard data server is capable of using the ethernet interface for the recording of data and for responding to requests from other equipment or systems.

d) Request-response data transport service

(See 6.3.3)

Confirm by observation that the shipboard data server sends data meeting conditions requested in request-response data transport services.

Confirm by observation that the shipboard data server receives data sent in request-response data transport services and processes them in accordance with methods.

Tests shall be conducted on all methods that the request-response data transport services may service.

e) Streaming data transport service

(See 6.3.4)

Confirm by observation that the shipboard data server sends data that meet the conditions requested in streaming data transport services.

Confirm by observation that the shipboard data server begins and ends data transmissions when valid external requests are received.

Tests shall be conducted on all requests that the streaming data transport services may process (except for query conditions).

f) File transport service

(See 6.3.5)

Confirm by observation that the shipboard data server has file transport service to output the normative XML file defined in A.2 of ISO 19848:2018.

Confirm by observation that the maximum capacity of the file is inputted and outputted as described in the manufacture's document.

Confirm by observation that the shipboard data server receives commands and/or methods and data that are sent in FTP, STFP, FTPS, HTTP and/or HTTPS protocols and processes them in accordance with commands and/or methods.

Tests shall be conducted on all requests that the FTP, STFP, FTPS, HTTP and/or HTTPS protocols may process.

g) Alias function

(See 6.4)

Confirm by observation that the shipboard data server has an alias function.

Register Alias ID and confirm by observation that actual recorded data are obtained according to registered Alias ID using the request-response protocol.

Alias function shall be confirmed by observation that it is only possible to obtain actual recorded data that cannot be updated and deleted.

When a user different from the registered user uses Alias Name, confirm by observation that actual recorded data cannot be obtained.

h) Data calculation function

(See 6.5)

Confirm by observation that all of the data calculation functions provided by the shipboard data server operate as documented by the manufacturer.

i) Log management function

(See 6.6, 6.2.2 and 6.2.3)

Confirm by observation that the shipboard data server has a system log function and is capable of recording the following items into the system log:

1) information of all data requests and reported data including:

   i) identification of requested and reported data records;

   ii) requested and reported time period;

   iii) source where the request was received from and report delivered to;

   iv) result of access control check for the source of request;

2) all indications that were released by condition monitoring function;

3) all changes of management data in detail, such as Data Channel List, Data Source Information and Alias List, and applied adjustment of the system clock. Confirm by observation that all events recorded to the system log are labelled with associated logical name or the shipboard data server and date and time of event occurrence. Confirm by analytical evaluation that

all system log records remain stored and available for viewing at least 30 days after their occurrence.

Annex A
(informative)

Ship-to-shore communication management

A.1 General

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

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

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

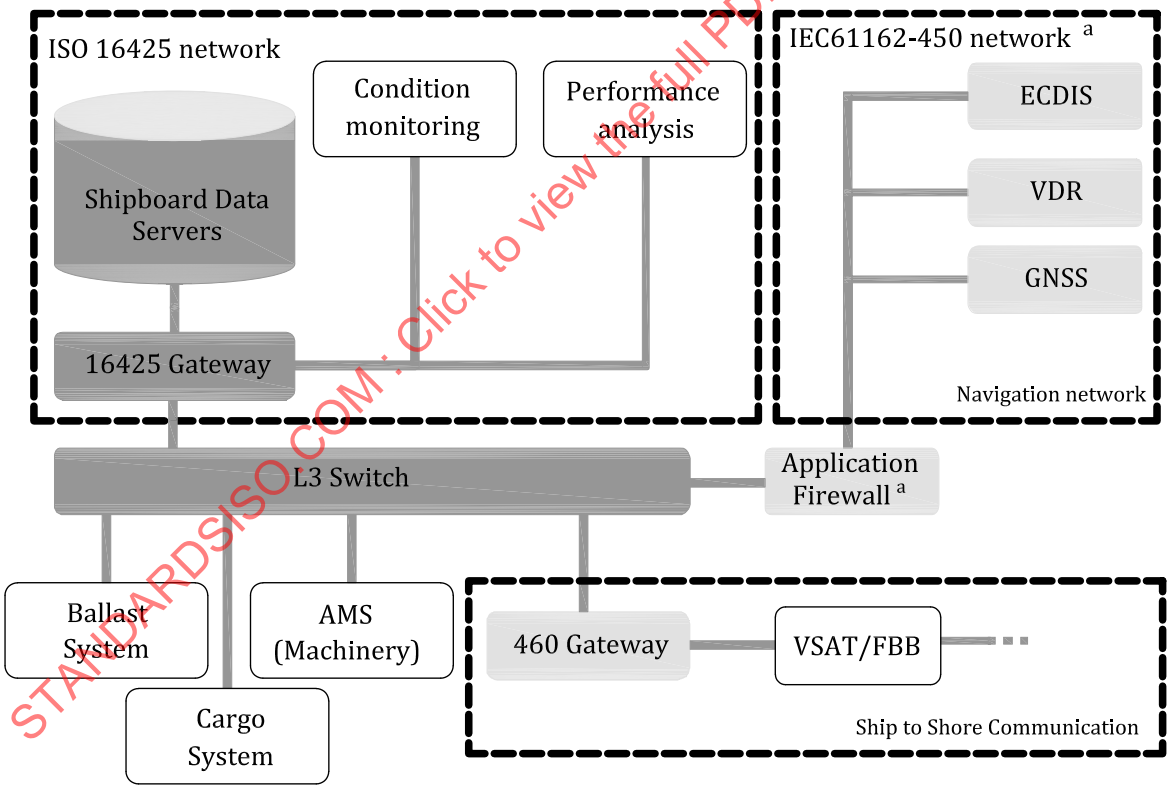

Figure A.1 — Concept model of ship-to-shore communication

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

The agent functions may perform specific tasks such as facilitate ship-to-shore communication or refine the data recorded by the ship data server by performing additional data analysis.

The agent functions may or may not reside within the shipboard data server equipment.

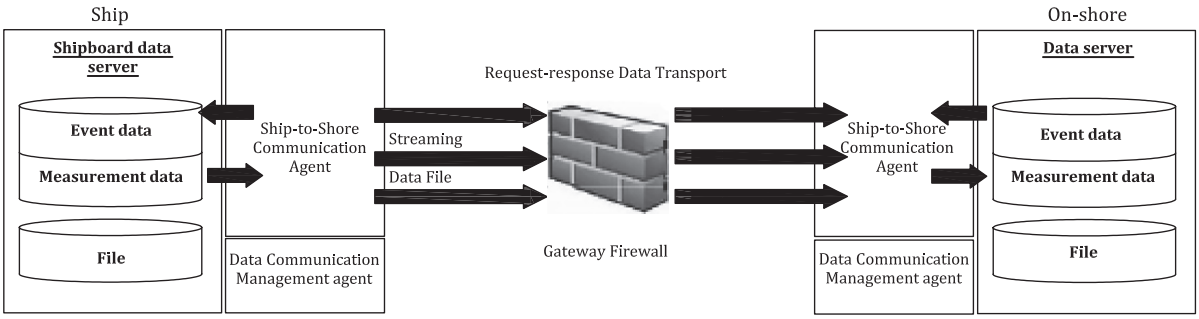

Figure A.2 — Concept model of ship-to-shore communication agent

A.2 Ship-to-shore communication agents

To realise data linkages between the unstable shipboard data server and the on-shore data server, ship-to-shore communication agents that have the following basic functions may be employed.

Transmitting data regularly from shipboard to on-shore data servers:

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

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

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, data communication management agents that have the following functions may be employed.

Data compression/decompression: compressing data to transmit and decompress data received:

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

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

c) 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
(normative)

Alias List

B.1 Structure of Alias List

B.1.1 Data model of Alias List

Alias List shall consist of the following elements.

a) Package

The package element is metadata made up of a Header, which is a metadata, 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, the author of Alias List.

c) Alias

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

Alias can be restricted by using public element and owner element.

d) DataChannel

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

Labels can be added to Local ID and Short ID. The label shall be unique in the Alias ID. However, this label is an output label of 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.

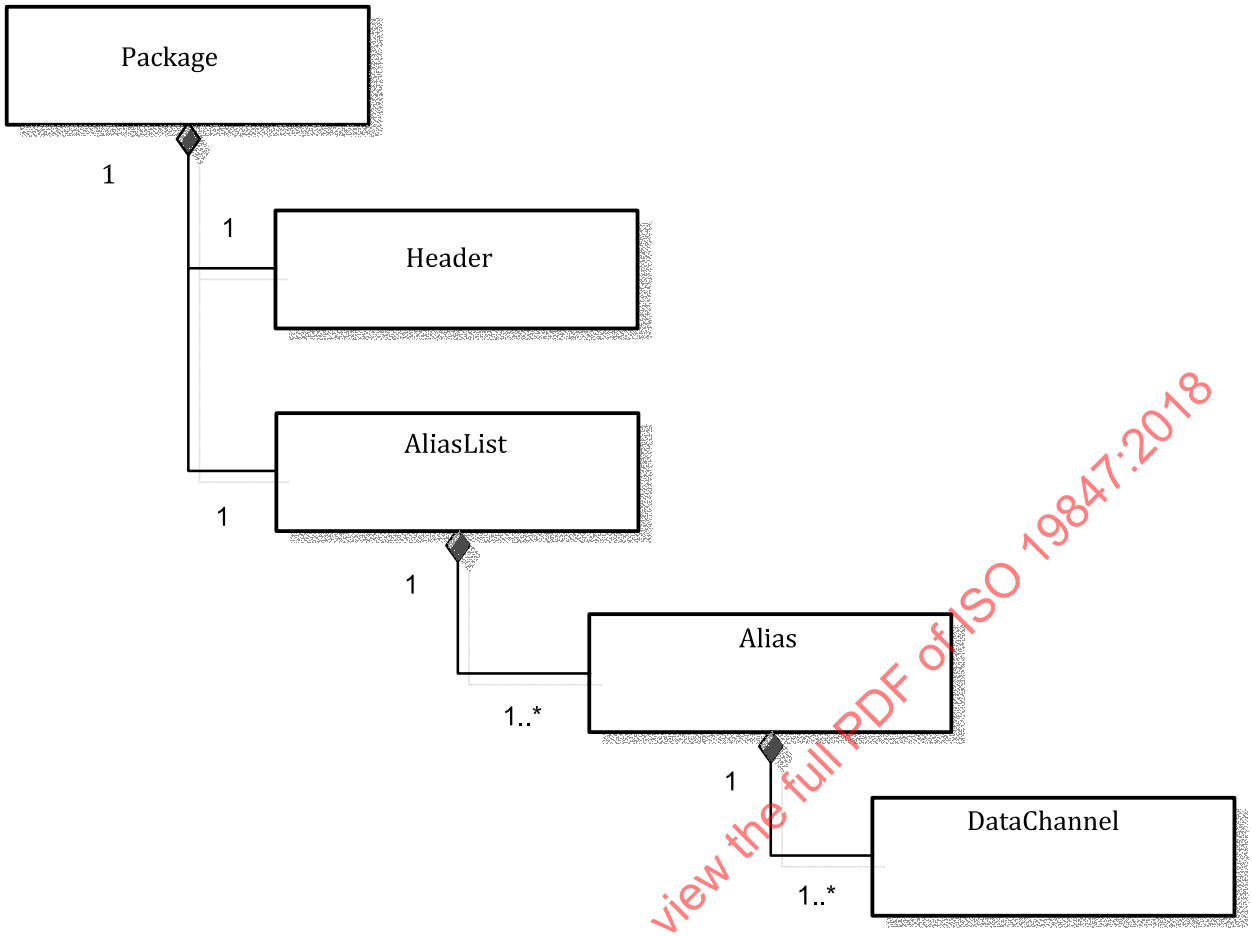

Figure B.1 — Structure model of the Alias List

B.1.2 Logical structure of Alias List

Alias List shall have the logical structure shown in Figure B.2.

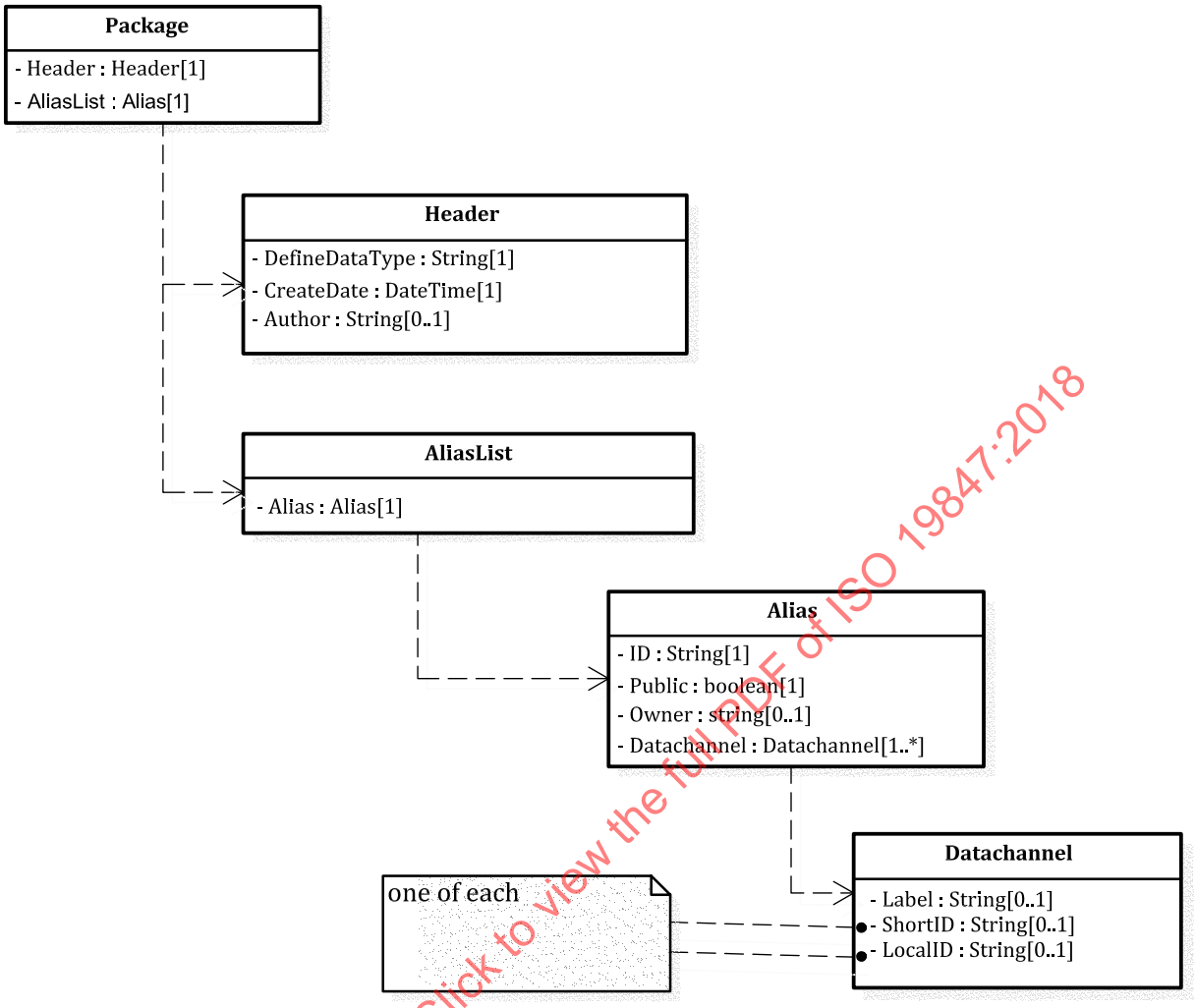

Figure B.2 — Logical structure of Alias List model

Details of each element are as follows.

1) Package structure

Name	Data type	Note	Mandatory/Option	Max count
Header	2) Header	See 2)	Mandatory	1
AliasList	3) Alias List	See 3)	Mandatory	1

2) Header structure

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

3) AliasList structure

Name	Data type	Note	Mandatory/Option	Max count
Alias	Alias	See 4)	Mandatory	1

4) Alias structure

Name	Data type	Note	Mandatory/Option	Max count
ID	String	Identifier identifying Alias. Be unique ID within the shipboard data server.	Mandatory	1
Public	Boolean	When it wants to restrict disclosure of Alias ID, sets Public element to false. In that case, designation of Owner element is necessary.	Mandatory	1
Owner	String	When owner element is described, it is restricted to owner where editing is described.	Optional	1
DataChannel	5) DataChannel	See 5)	Mandatory	*

5) DataChannel structure

Name	Data type	Note	Mandatory/Option	Max count
Label	String	Specify this when adding another label to ShortID or LocalID.	Optional	1
ShortID	String	See 5.2.3 of ISO 19848:2018	Optional	1
LocalID	String	See 5.2.2 of ISO 19848:2018	Optional	1

Annex C
(normative)

Request-response protocol

C.1 General

The request-response protocol is the protocol for the shipboard machinery and equipment to request the shipboard server to process data, and for the shipboard data server to deliver results to meet such requests. The protocols support delivery of data arranged in chronological order and allow delivery of records originating from multiple data providers in a same report.

Examples of request-response protocols that the shipboard data server provide are given in C.3.

C.2 Access control

Access to the shipboard data server with request-response protocols shall be using the appropriate authentication method (for example, Login ID and password).

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

C.3 Protocol specification

The shipboard data server provides request-response protocols in REST API.

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. When adding a method, the manufacturer shall include the method and its function in the manufacturer's manual.

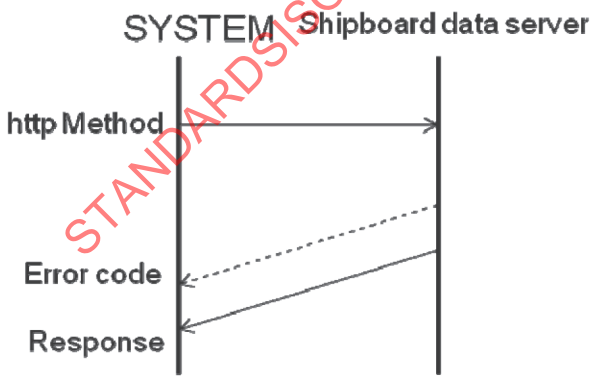

Figure C.1

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 Option, Make Option, Query Option, and Label Option options, it shall be conforming to RFC 3986.

Options and parameters do not need to distinguish between uppercase and lowercase letters.

Table C.1 — Structure of request-response protocols

Method	Service root	Resource path	Type option	DataChannelType option	Make option	Query option	Label option
See b)	See c)	See d)	See e)	See f)	See g)	See h)	See i)

b) Functions and executions of request-response protocol methods

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

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

It is desirable that logs be record in Syslog.

Table C.2 — Request-response protocol method

Method	Description
GET	GET method retrieves the resources of the specified URI from the shipboard data server.
POST	POST method adds data of message body to the shipboard data server. Resource path cannot be specified.
PUT	PUT method updates data of message body to the shipboard data server. Resource path cannot be specified.
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]

c) Service root

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

Table C.3 — Details of Service Roots

Service root	Description	Mandatory/ option	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 Data Channel Type option and method. It can't be specified when executing POST and PUT method.

Refer to e) for the details of Data Channel Type option.

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

When Data Channel Type is "ShortID", specify one Short ID defined in the Data Channel List. There cannot be specified multiple Short ID by separating Short ID with "/" or ",".

When Data Channel Type is “Alias”, specify one Alias ID defined in the Alias List. Cannot specify multiple Alias ID by separating Alias ID with “/” or “,”.

When Data Channel Type is “Local ID”, in case of GET Method, a Wildcard will be used in Resource paths. See j) for more about Wildcards.

Table C.4 — Details of resource paths

Resource path	Description	Mandatory/	Example
<Naming Rule>	See 5.2.2 of ISO 19848	Optional	/jsmea_mac
<Local Data Name>	Can be used only when Type Option is either “data”, “sdd”.	Optional	/MainEngine//AirCooler/CoolingFreshWater/Inlet/Temp

e) Type option

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

Type option is specified in the http header. Type option is also used for methods other than GET method.

Type option default is “data”.

Type option is specified in the message header.

Table C.5 — Details of Type Options

Types of data	Description	Number of appearances	Example
data	Handle Times Series Data	1	type: data
sdd	Handle Data Channel List	1	type: sdd
alias	Handle Alias List	1	type: alias

f) DataChannelType

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

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

DataChannelType option default is “Local ID”.

DataChannelType option is specified in the message body.

Table C.6 — Details of DataChannelType Options

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

g) Make option

Make option specifies the destination of search results. Only GET method can be used.

The destination shall be specified by full path.

Make option is specified in the message body.

NOTE Example of make option.

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

h) Query option

Query options are used to specify data format, change sort order, use filter, etc.

Query options that may be used and ways to designate them are shown in Table C.7.

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

When date and time are used for option parameter, add that using ISO 8601 format.

Query option is specified in the message body.

Table C.7 — Details of Query Options

Option Name	Description	Default	Example
?offset	Designate in UTC times and dates for obtaining data. In case of Delete Method, cannot be used when Type Options are not data	UTC at a time when server receives Method	?offset =2
?before	Designate whether search is made before or after base times and dates (before: true, after: false). Can be used only when type Options are “data”.	true	?before=false
?header	Designate whether Time Series Data are output with or without Headers	false	?header=true
?limit	Designate time frames to obtain on the second time scale, when types are “data”. Designate the number of items 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”. In case of Delete Method, cannot be used when Type Option is not “data”.	1	?limit=5

Table C.7 *(continued)*

Option Name	Description	Default	Example
?revisionfrom	When obtain are revision history of Data Channel List and Alias List, specify the date and time. It searches the list whose time stamp of Alias List or Data Channel List is newer than the date and time specified. The revisionfrom option can be used if the type option is "sdd" or "alias".		?revisionfrom = 2016-03-31T00:00:00Z
?revisionto	When obtain are revision history of Data Channel List and Alias List, specify the date and time. It searches the list whose time stamp of Alias List or Data Channel List is older than the date and time specified. It can be used simultaneously with revisionfrom. The revisionto option can be used if the type option is "sdd" or "alias".		?revisionto=2015-04-01T23:59:59Z
?orderby	Designate either ascending or descending chronological orders for data obtained. (asc: ascending; desc: descending)	asc	?orderby=asc

i) Label option

Specify the priority of the output format of Column header when getting time series data with GET method.

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

Label option that may be used and ways to designate them are shown in Table C.8.

Label option is specified in the message body.

Table C.8 — Details of Label options

Label type	Description	Number of appearances	Example
ShortID	Use ShortID with the highest priority. The Column header is used with the priority of ShortID, Label, 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 path, refer to the Local ID in 5.2.2 of ISO 19848:2018.

When obtaining Time Series Data, Data Channel List and Data Source Information saved in the shipboard data server, using Wildcard in Resource paths creates filters.

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

Wildcard strings of characters:

#: Multi-level wildcard. The multi-level wildcard is used to match any number of levels within a URI.

+: Single-level wildcard. The single -level wildcard matches only one URI level.

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

URI list	Match/ Unmatch	
/jsmea_mac/MainEngine/AirCooler/CoolingFresh-Water/Outlet/Temp	Matched	
/jsmea_mac/MainEngine/AirCooler/CoolingFresh-Water/Inlet/Temp	Unmatched	/jsmea_mac/MainEngine/AirCooler/Cooling-FreshWater/Inlet/Temp
/jsmea_mac/MainEngine/AirCooler/CoolingFresh-Water/Outlet/Press	Unmatched	/jsmea_mac/MainEngine/AirCooler/Cooling-FreshWater/Outlet/Press
/jsmea_mac/MainEngine/AirCooler/ScavAir/ Inlet/Temp	Unmatched	/jsmea_mac / MainEngine/AirCooler/ScavAir/ Inlet/Temp
/jsmea_mac /MainEngine/AirCooler/ScavAir/ Outlet/Temp	Matched	
/jsmea_mac /MainEngine/Cylinder/ScavAir/Out-let/Temp	Unmatched	/jsmea_mac /MainEngine/Cylinder/ScavAir/ Outlet/Temp

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

URI list	Match/ Unmatch	
/jsmea_mac/MainEngine/AirCooler/CoolingFresh-Water/Outlet/Temp	Matched	
/jsmea_mac/MainEngine/AirCooler/CoolingFresh-Water/Inlet/Temp	Matched	
/jsmea_mac/MainEngine/AirCooler/CoolingFresh-Water/Outlet/Press	Matched	
/jsmea_mac/MainEngine/AirCooler/ScavAir/ Inlet/Temp	Unmatched	/jsmea_mac/MainEngine/AirCooler/ScavAir/ Inlet/Temp
/jsmea_mac /MainEngine/AirCooler/ScavAir/ Outlet/Temp	Unmatched	/jsmea_mac/MainEngine/AirCooler/ScavAir/ Outlet/Temp
/jsmea_mac /MainEngine/Cylinder/ScavAir/Out-let/Temp	Unmatched	/jsmea_mac /MainEngine/Cylinder/ScavAir/ Outlet/Temp

k) Return code of method

When the shipboard data server receives a method, sends processing results and HTTP status code (see Table C.9) to the sender.

Table C.9 — 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	Unauthorised	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

C.4 Example for Request-response Protocol

a) Actual recorded data example

Table C.10 — 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
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/

{ISO 19848 data format}

See ISO 19848:2018, Annex A 2.4 c).

2) Results

The processing result is returned in the HTTP return code.

See Table C.9 HTTP status code.

c) GET method example

Execute GET method for the actual recorded data in Table C.10.

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

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

Search condition:

Include ExhGas in Local ID

Date and time on 25 November 2016, 6:43:03 or earlier

Search 2 in the past direction

1) Search Results of a) 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 19848:2018, Annex A 2.4 c).

d) PUT method example

1) PUT method

PUT http://localhost/

{ISO 19848 data format}

See ISO 19848:2018, Annex 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.9 HTTP status code.

e) TRACE method example

Execute TRACE method for the actual recorded data in Table C.10.

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

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

Search condition:

Include ExhGas in Local ID

Date and time on 25 November 2016, 6:43:02 or earlier

Select in the past direction

1) The following result is returned

2) Results

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

See Table C.9 HTTP status code.

3) Example for return message at normal end

<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

Access to the shipboard data server with streaming protocols shall be using the appropriate authentication method (for example, Login ID and password).

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

D.3 Protocol specification

The shipboard data server shall be provided with the Broker and Publisher functions of MQTT Protocol.

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 Annex A, 2.4 c) of ISO 19848:2018.

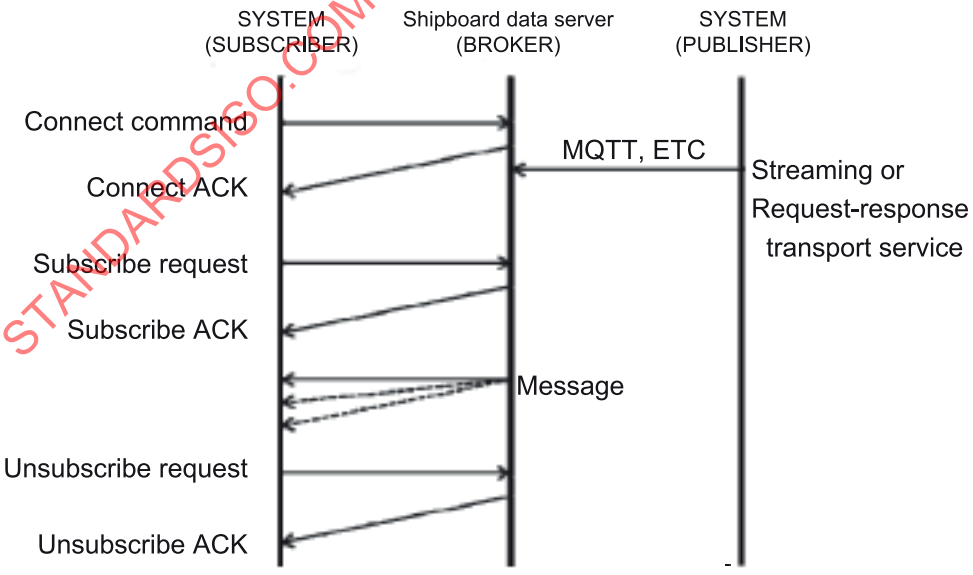

Figure D.1

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

Annex E
(normative)

File input and output protocol

E.1 General

File input and output protocol shall be used on the shipboard data server to obtain configuration information and sets of data that are unique to shipboard machinery and equipment.

E.2 Access control

Access to the shipboard data server by users shall use the appropriate authentication method (for example, Login ID and password).

E.3 Protocol specification

The shipboard data server shall use HTTP or FTP protocols. From the viewpoint of security, the shipboard data server may use SFTP/FTPS/HTTPS protocols.

When storing a file using an FTP/SFTP/FTPS protocol, use PUT command.

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

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

The method of each protocol shall be able to handle multiple data with wildcards.

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 d)	see e)
POST	http://<host>[:port>]/	see d)	see e)
PUT	http://<host>[:port>]/	see d)	see e)
DELETE	http://<host>[:port>]/	see d)	see e)

b) Function of Method

Method that may be used in File input and output protocols are shown in Table E.2.

When Method is input, logs may output on Status Code for Method used, as well as request details, times and dates, and results.

It is desirable that logs be recorded in Syslog.

Table E.2 — File input and output protocol method

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

c) Service root

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 specified a path allowing access.

e) File name

The file name shall comply to the following requirements.

1) The file name of the file shall be case-insensitive.

2) The file name of the file shall not start with “.” (period).

3) The file name of the file shall not contain [\ ] [/] [:] [*] [?] ["] [<] [>] [|] and any white space characters.

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

Annex F
(informative)

Data Source Information

F.1 General

Data Source Information defines formats in which data providers provide data and identify communication protocols.

When formats in which data providers send data do not comply with ISO 19847, users may convert protocols by defining relations to Data Source Information.

Data Source Information shall meet certain assumptions by defining XML schemas.

Examples of defining Data Source Information in W3C XML Schemas are discussed in F.5.

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

F.2 Rules for XML Schemas

XML Schemas are formulated in accordance with the rules described below.

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
Nonnegative Integer	Nonnegative Integer	Integer number that is 0 or larger
Real	Real	Single precision floating point number
Date Time	String	Format by ISO 8601 Refer to RFC 3339 for 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 Data Source Information, respectively.

Data Source Information and Data Channel List are related with Local ID.

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

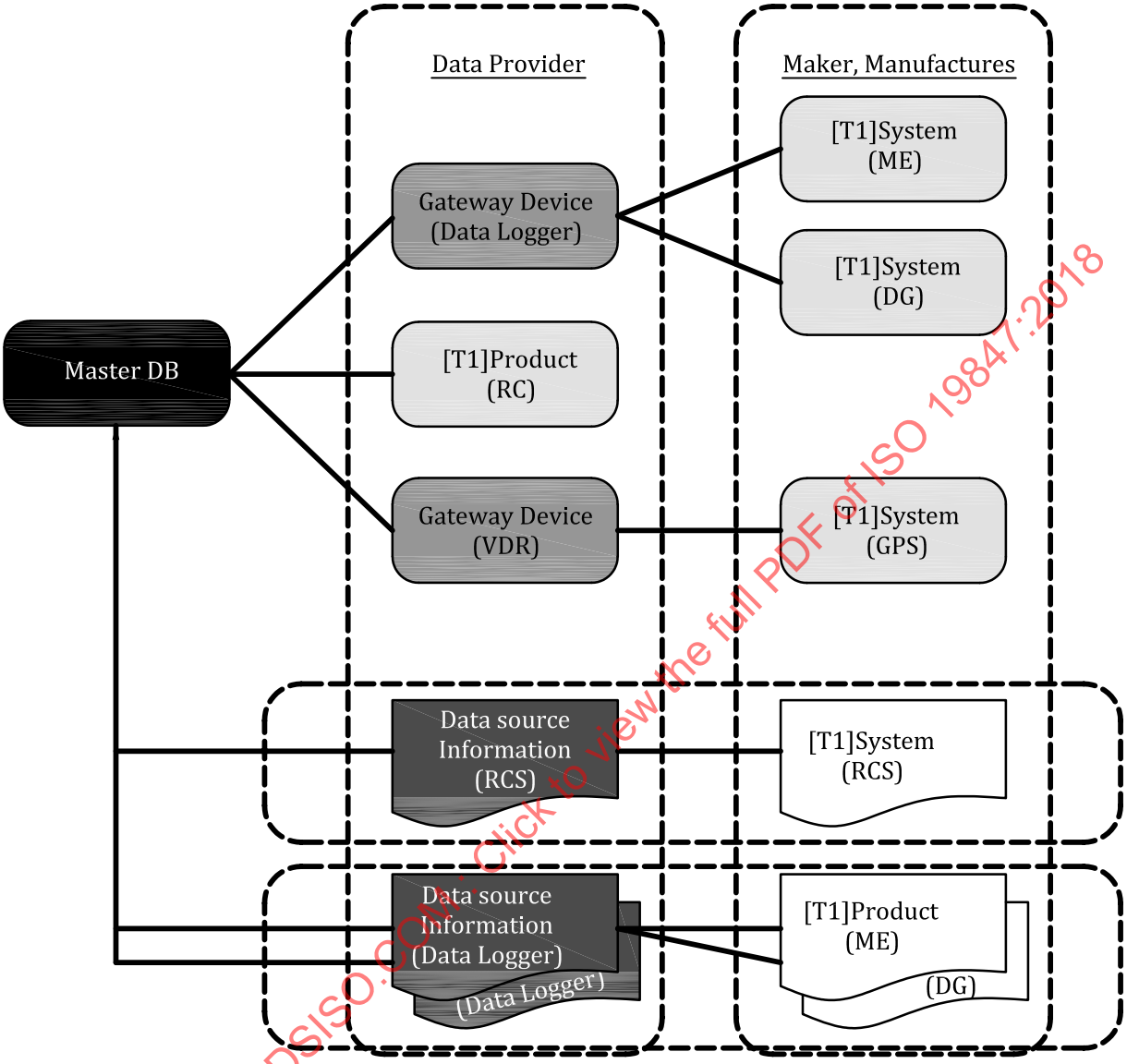

Figure F.1 — Relations between Data Source Information and Data Channel List

Structure model of the Data Source Information shown in Figure F.2