BS ISO 19847:2024

BSI Standards Publication

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

Documents
Document Sharing Hub

Full document details: BS ISO 19847:2024

National foreword

This British Standard is the UK implementation of ISO 19847:2024. It supersedes BS ISO 19847:2018, which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee EPL/80, Maritime navigation and radiocommunication equipment and systems.

A list of organizations represented on this committee can be obtained on request to its committee manager.

Contractual and legal considerations

This publication has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient's own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute a contract. Users are responsible for its correct application.

© The British Standards Institution 2024
Published by BSI Standards Limited 2024

ISBN 978 0 539 15620 1

ICS 47.020.70

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 29 February 2024.

Amendments/corrigenda issued since publication

Date	Text affected

Documents
Document Sharing Hub

Full document details: BS ISO 19847:2024

International Standard

ISO 19847

Second edition
2024-02

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

Reference number
ISO 19847:2024(en)

© ISO 2024

Documents
Document Sharing Hub

Full document details: BS ISO 19847:2024

COPYRIGHT PROTECTED DOCUMENT

© ISO 2024

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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

Documents
Document Sharing Hub

Full document details: BS ISO 19847:2024

Contents

Page

Foreword ... **v**
Introduction ... **vi**
1 Scope ... **1**
2 Normative references ... **1**
3 Terms and definitions ... **1**
4 Abbreviated terms ... **6**
5 General requirements for the shipboard data server ... **7**
5.1 Function and performance of the shipboard data server ... 7
5.1.1 Processing performance ... 7
5.1.2 Storage function ... 10
5.1.3 Interface function ... 10
5.1.4 Condition monitoring function ... 11
5.1.5 Data backup and restoration functions ... 11
5.1.6 Function to protect against unauthorised access ... 11
5.1.7 Status reporting ... 11
5.2 Environmental performance of shipboard data server ... 12
5.2.1 Power-supply performance ... 12
5.2.2 Vibration-resistant feature ... 12
5.2.3 Requirement for electromagnetic immunity and emission ... 12
5.2.4 Temperature and humidity resistant requirements ... 13
5.3 Installation requirements for shipboard data server ... 13
5.3.1 Environment requirements ... 13
5.3.2 Requirements for maintenance areas ... 13
5.3.3 Requirement for networks and network security ... 13
6 Data input/output and data management on shipboard data server ... **14**
6.1 General ... 14
6.2 Data management function ... 14
6.2.1 General ... 14
6.2.2 Management of system clock ... 14
6.2.3 Management of Data Channel List ... 14
6.2.4 Management of Data Source Information ... 15
6.2.5 Management of Alias List ... 15
6.3 Data input and output functions ... 15
6.3.1 General ... 15
6.3.2 Input function ... 16
6.3.3 Output function ... 17
6.3.4 Request-response data transport service ... 17
6.3.5 Streaming data transport service ... 18
6.3.6 File transport service ... 18
6.4 Alias function ... 18
6.4.1 General ... 18
6.4.2 Alias List ... 19
6.5 Data calculation function ... 19
6.5.1 General ... 19
6.6 Log management function ... 19
7 Operation requirements ... **20**
7.1 General ... 20
7.2 Protection from logical threats ... 20
7.2.1 Access control ... 20
7.2.2 Usage control ... 21
7.2.3 Network access ... 22
7.2.4 System defence ... 22

© ISO 2024 – All rights reserved

AVA Documents
Document Sharing Hub

Full document details: BS ISO 19847:2024

7.3 Protection from physical threats 23
7.3.1 General 23
7.3.2 Installation requirements 23
7.3.3 Connection cables 23
7.3.4 Power source management 23
7.3.5 Interfaces for removable devices 24
7.3.6 Protection (others) 24
7.3.7 Equipment maintenance 24
7.4 Software maintenance 25
7.4.1 General 25
7.4.2 Maintenance mode 25
7.4.3 Setting changes 25
7.4.4 Software update 25
7.4.5 Failure recovery 26
7.4.6 Software version information 26

8 Test requirements 26
8.1 Outline 26
8.2 Test items 26
8.2.1 Test environments 26
8.2.2 Test methods 27

Annex A (informative) **Ship-to-shore communication management 43**

Annex B (informative) **Structure of Alias List 45**

Annex C (normative) **Request-response protocol 49**

Annex D (normative) **Streaming protocol 60**

Annex E (normative) **File input and output protocol by the HTTP(S) 62**

Annex F (informative) **Data source information 64**

Annex G (informative) **User management of the shipboard data server 74**

Annex H (informative) **Internal calculation function 77**

Bibliography 86

© ISO 2024 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 19847:2024

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.

© ISO 2024 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 19847:2024

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.

© ISO 2024 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO 19847:2024

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 2024 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 19847:2024

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).

© ISO 2024 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 19847:2024

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.

© ISO 2024 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO 19847:2024

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.

© ISO 2024 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 19847:2024

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.

© ISO 2024 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 19847:2024

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

© ISO 2024 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 19847:2024

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.

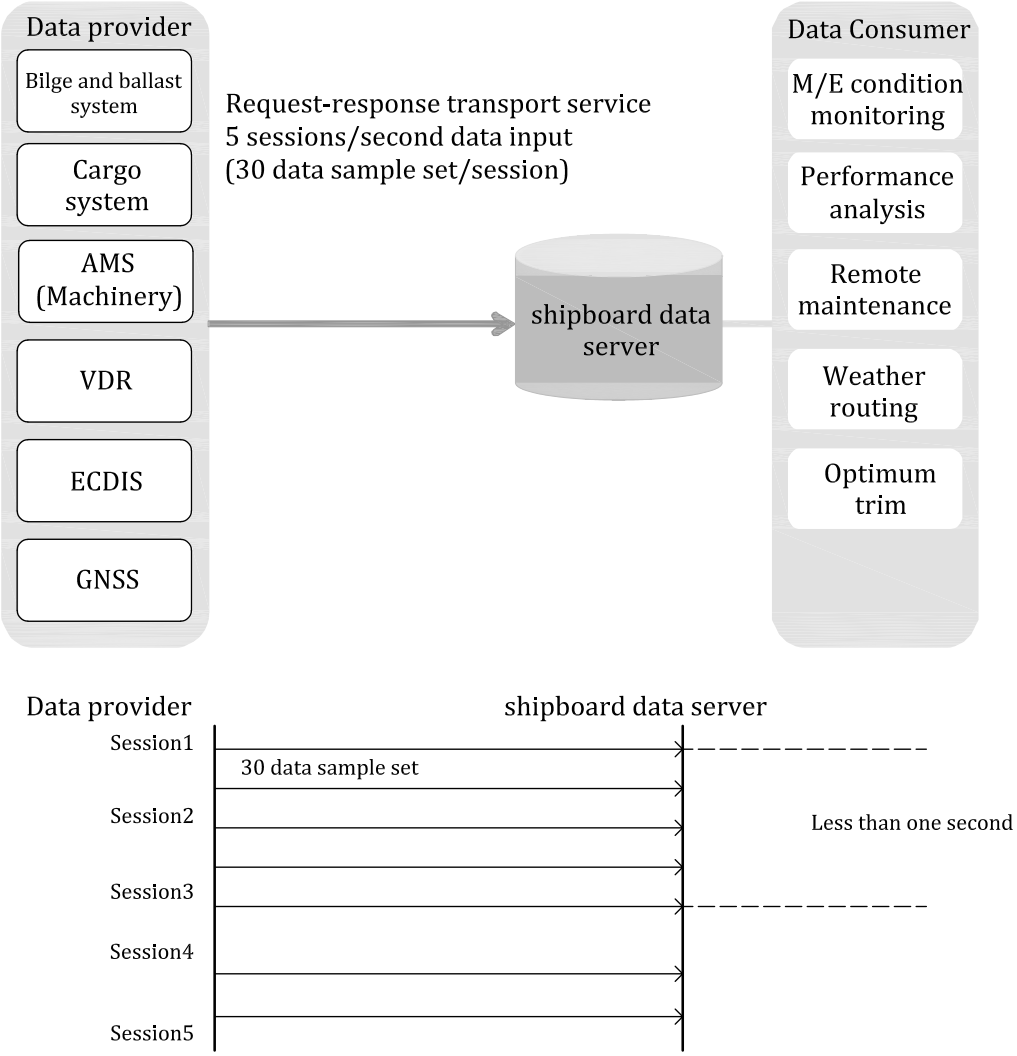


Figure 1 — Input data processing performance requirement

© ISO 2024 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 19847:2024

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.

© ISO 2024 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 19847:2024

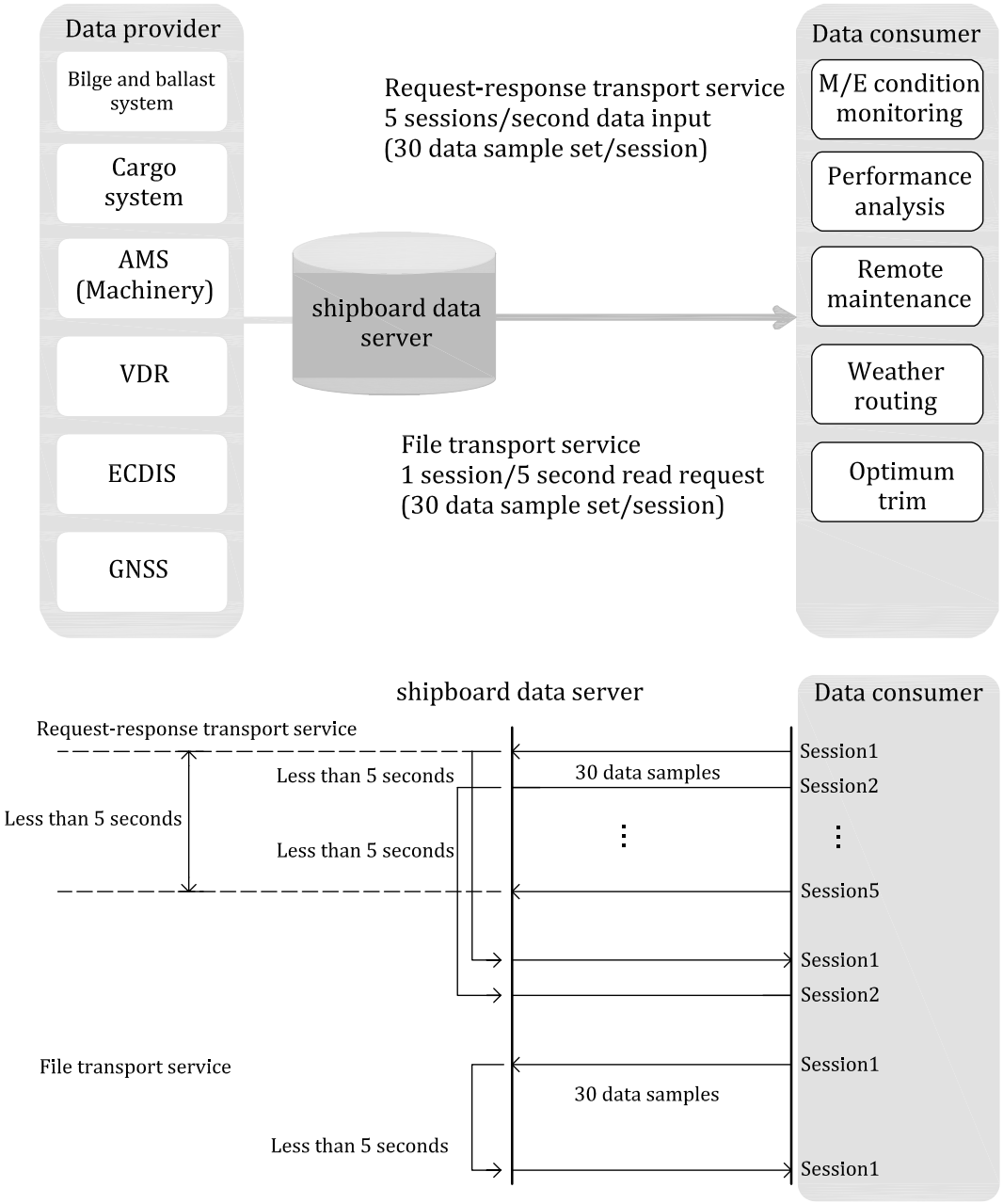


Figure 2 — Output data processing performance requirement

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.

© ISO 2024 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 19847:2024

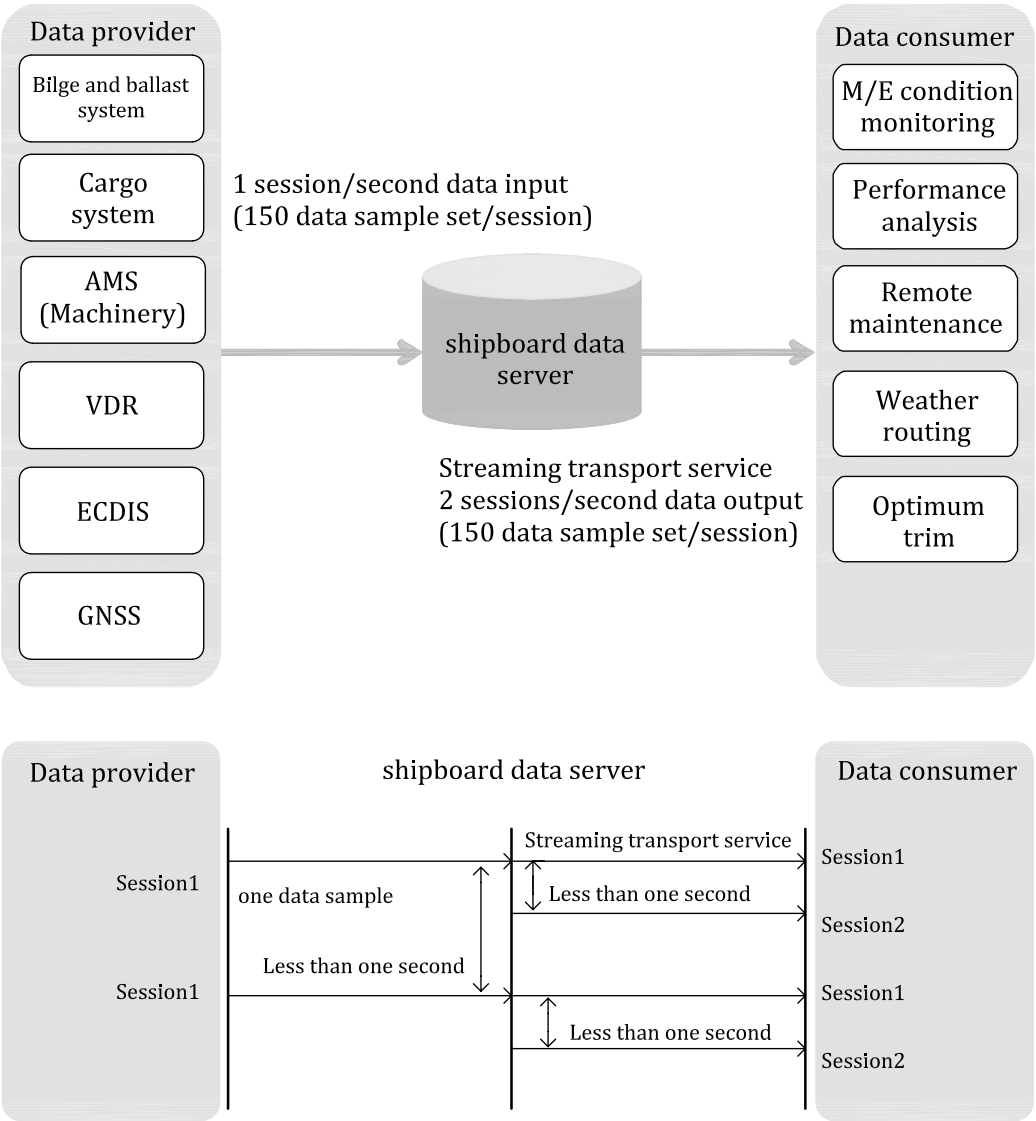


Figure 3 — Streaming transport processing performance requirements

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).

© ISO 2024 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 19847:2024

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>

© ISO 2024 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 19847:2024

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.

© ISO 2024 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 19847:2024

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.

© ISO 2024 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 19847:2024

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.

© ISO 2024 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 19847:2024

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.

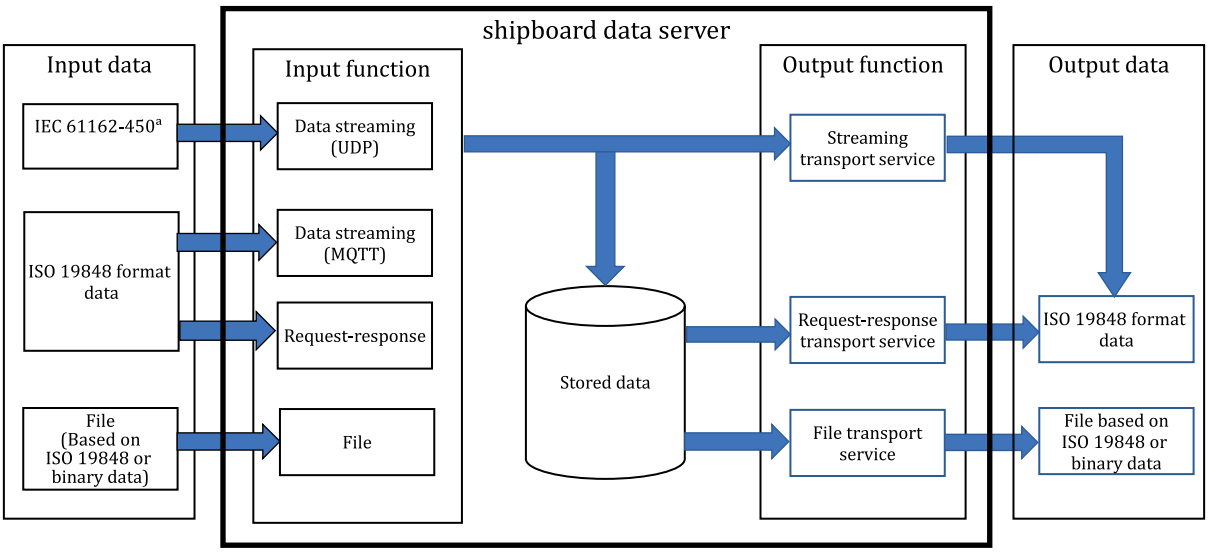
c) The shipboard data server shall be provided with file transport services having data input and output functions.

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.

© ISO 2024 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 19847:2024



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

© ISO 2024 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 19847:2024

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.

© ISO 2024 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 19847:2024

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.

© ISO 2024 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 19847:2024

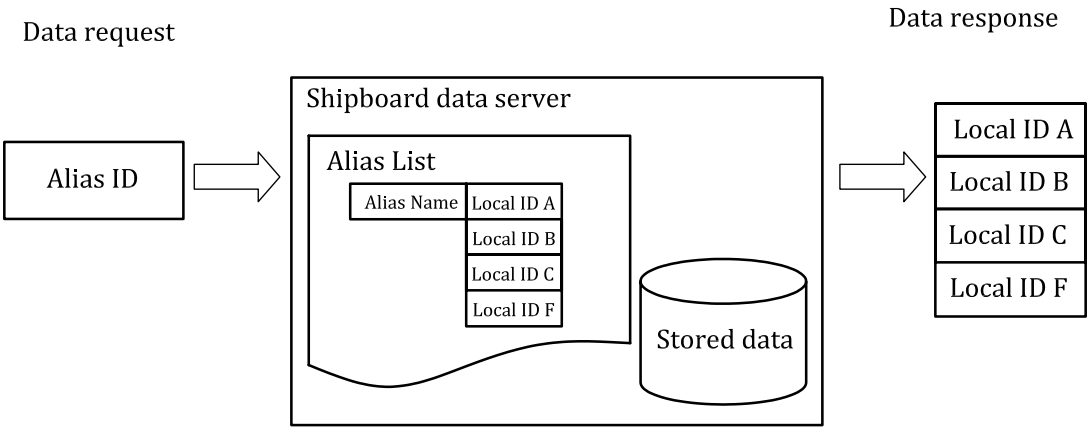


Figure 5 — Alias function

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.

© ISO 2024 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 19847:2024

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.

© ISO 2024 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 19847:2024

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.

© ISO 2024 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 19847:2024