INTERNATIONAL STANDARD

ISO 23807

First edition
2023-03

Ships and marine technology — General requirements for the asynchronous time-insensitive ship-shore data transmission

Reference number
ISO 23807:2023(E)

COPYRIGHT PROTECTED DOCUMENT

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

Published in Switzerland

Contents

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*.

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

Sharing data between ships and the shore to ensure the safe and efficient operation of ships is becoming increasingly common.

Progress has been made in establishing data sharing between ships and the shore, related to ports, cargo and shipping routes. This includes the development of and discussions around standards related to Maritime Single Window and e-Navigation, which help to share some stylized data safely and in a timely manner between ships and shore.

On the other hand, the ship-shore communication environment is still narrower than those on land, and its connection is unstable. Therefore, a method for stably and efficiently sharing files of any format with a relatively large file size, such as various data and image files used in ship operation business applications, between ships and shore has not yet been standardized.

For example, in ship operations, onboard and on-shore application users determine the timing of data transmission and reception in relation to the connection status and communication quality of ship-shore communication each time, and perform data retransmission processing independently for each application.

In order to further promote the safe and efficient operation of ships, it is increasingly important to be able to send and receive files between ships and shore in a stable and efficient manner asynchronously without being affected by the ship-shore communication status.

In this document, asynchronous communication means the communication and/or application processing perspective, such as time-insensitive data transmission for non-real-time applications where the timing of the data generating and consuming can be different.

Although ISO 19847 and ISO 19848 provide standardized processes for efficient collection and storage of data for ship equipment systems, the method of asynchronously transmitting and receiving a large amount of ship equipment data accumulated on board between ships and shore has not been standardized yet. In order to promote shore support for ship operation and maintenance of onboard equipment systems, there is a need for a stable and efficient method for transmitting and receiving such onboard field data asynchronously between ships and shore.

This document specifies the functional requirements but does not intend to specify technical protocols.

See Annex A for more information on the correlation between the different relevant standards.

Ships and marine technology — General requirements for the asynchronous time-insensitive ship-shore data transmission

1 Scope

This document describes the requirements involved in ship to shore data communication between the shipboard data servers and the on-shore data servers. It provides information on:

- asynchronous communication;
- a method to measure end-to-end communication quality;
- transport integrity;
- transport security (e.g. encryption, authentication and authorization);
- management of data transmission (e.g. prioritization, logging, carrier awareness/management);
- communication optimization (e.g. deduplication, compression, resume, multiplexing);
- compliance with the data communication protocols, including but not limited to ISO 19847.

This document does not cover:

- the security of the data producer/consumer (e.g. identity management);
- communication equipment requirements;
- carrier performance requirements (e.g. bandwidth and latency).

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/IEC 20922, *Information technology — Message Queuing Telemetry Transport (MQTT) v3.1.1*

3 Terms and definitions

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

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

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

3.1
asynchronous communication
time-insensitive data transmission for onboard applications that transmit ship data and/or non-real-time applications where the timing of the data generating and consuming can be different

Note 1 to entry: This definition is not from the data protocol perspective.

Note 2 to entry: ISO 19847 is an example of an onboard application.

Note 3 to entry: The scope of the definition of asynchronous communication in this document covers messaging services such as message queueing telemetry transport and similar protocols but not streaming using datagram protocol.

Note 4 to entry: Table 1 compares the definition of synchronous and asynchronous communication.

Table 1 — Intentions regarding synchronous/asynchronous in this document

	Communication/application perspective
Synchronous	The receiver sends a response, and the sender waits for the response before sending the next data.
Asynchronous	The receiver sends a response, and the sender sends the next data without waiting for the response.

3.2
data transport agent
software installed on a ship or shore that interfaces with peripheral devices and systems

Note 1 to entry: The data transport agent collects and sends data to the *asynchronous data management agent* (3.3), or receives data from the asynchronous data management.

3.3
asynchronous data management agent
software used for the control and transport of data between ship and shore *data transport agent* (3.2)

4 Abbreviated terms

AES	advanced encryption standard
AES-CCM	AES-counter with cipher block chaining-message authentication code
AES-GCM	AES-galois/counter mode
API	application programming interface
BIZ-LAN	business local area network
ChaCha20	a stream cipher specified in RFC 8439
ChaCha20-Poly1305	a cryptographic algorithm that combines ChaCha20 and Poly1305
DH	Diffie-Hellman key exchange algorithm
DHE	Diffie-Hellman Ephemeral key exchange algorithm
DMZ	DeMilitarized Zone
ECDH	elliptic curve Diffie–Hellman key exchange algorithm
ECDHE	elliptic curve Diffie–Hellman ephemeral key exchange algorithm
ECDSA	elliptic curve digital signature algorithm
F/W	firewall
GraphQL	query language and runtime designed for APIs
HTTP	hypertext transfer protocol

IoT	Internet of things
LAN	local area network
MQTT	message queueing telemetry transport
OT	operational technology
Poly1305	a cryptographic message authentication mode specified in RFC 8439
PSEC-KEM	provably secure elliptic curve encryption with key encapsulation mechanisms
REST	REpresentational state transfer
RSASSA-PKCS1-v1_5	a digital signature algorithm specified in RFC 8017
RSASSA-PSS	a digital signature algorithm specified in RFC 8017
SHA-256	secure hash algorithm-256
SHA-384	secure hash algorithm-384
SHA-512	secure hash algorithm-512
TCP	transmission control protocol
TLS1.3	transport layer security version 1.3
UDP	user datagram protocol
UR E22	International Association of Classification Societies (IACS) Unified Requirement Electrical and Electronic Installations 22
UTM	unified threat management
VSAT	very small aperture terminal

5 General requirements

5.1 General

Communication between shore and ship are usually initiated from the vessel side. The vessel in most cases has a random IP address and it is difficult to change the firewall rules to allow traffic from shore sites. It is both easier and safer to initiate the communication link from behind the firewall, meaning that the vessel shall initiate the contact with shore. The same is true for shore sites, such as ship managers office locations. These locations should be considered a client side location, and should be responsible for initiating the communication link to a common centre resource such as the cloud server or the on-premises.

Figure 1 shows the overall picture of this document.

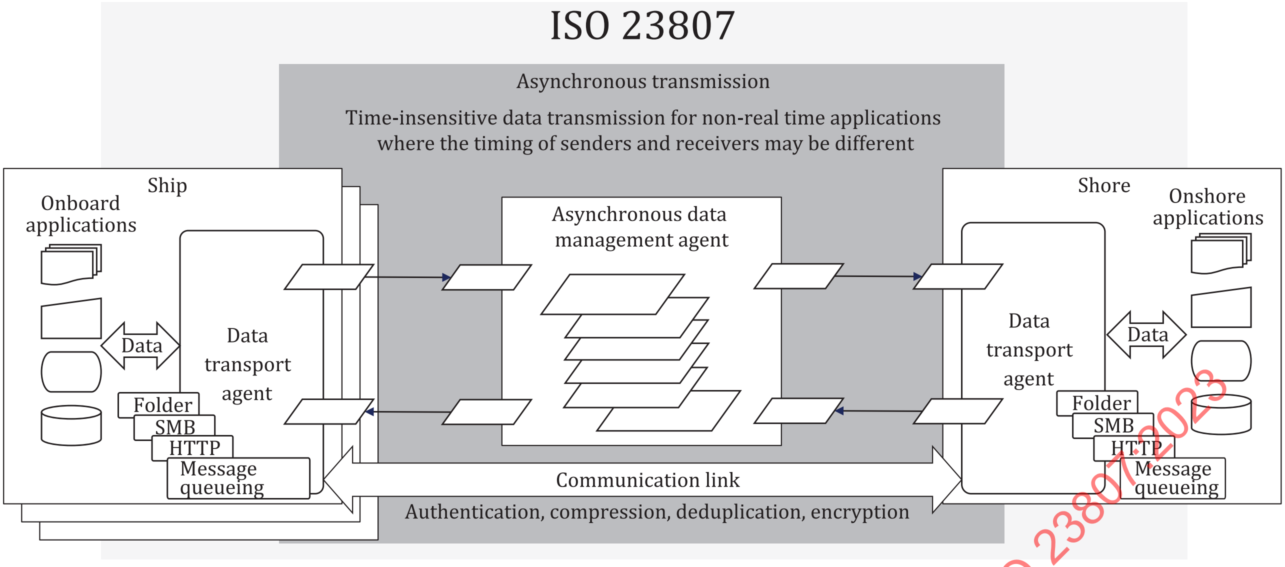

ISO 23807
Asynchronous transmission
Time-insensitive data transmission for non-real time applications where the timing of senders and receivers may be different
Ship
Onboard applications
Data
Data transport agent
Folder
SMB
HTTP
Message queueing
Asynchronous data management agent
Shore
Onshore applications
Data
Data transport agent
Folder
SMB
HTTP
Message queueing
Communication link
Authentication, compression, deduplication, encryption

Figure 1 — Image of asynchronous transmission

Asynchronous communication is used on all communication where data can be transmitted intermittently.

It shall be applied to narrow-band and unstable ship-shore communication to exchange various types of data such as documents, media files, sensor data and machine-to-machine communication, and shall be applied to transferring the onboard server data. Best effort, variable bit rate and communication at regular intervals utilize spare capacity on an available carrier. Such communication shall comply with the requirements in 5.2, 5.3, 5.4, 5.5 and 5.6.

A single agent, or multiple agents, can be used to service multiple data formats.

5.2 Encryption

All traffic shall use appropriate encryption as dictated by the sensitivity of the data.

5.3 Compression

The content shall be compressed whenever the compressed size is significantly smaller than the raw data. The compression algorithm used shall be optimal for the intended use of the data, and not necessarily what provides the highest compression.

5.4 Deduplication

Transferring a large amount of data can have significant bandwidth savings by using proper deduplication. The deduplication protocol divides sending data into chunks and tracks their progress. The chunk size used in deduplication is not a fixed size and can be from 2K to 32K in size. For small data transfers, the overhead for the control traffic for deduplication can be bigger than the data itself. In such cases, deduplication should be avoided and any file below 2KB in size shall not be split into parts. Files larger than 2KB can be split into parts for deduplication, depending on the structure of the file. The deduplication protocol recognizes data blocks already available on the destination client, and only sends blocks not already on the client. This is true even for binary encoded data whenever the content can be shared among other communication data. For example, binary docker images greatly benefit from deduplication due to the layers inherent in such an image. These layers are shared between multiple docker images.

5.5 Distribution

In many cases, the data to transport shall be transported to multiple destinations (such as fleet-wide documentation). In other cases, there exist multiple sources of data that shall be transported to a single destination (such as IoT sensor data from a fleet of vessels). Due to this complexity, the communication system should be able to configure tasks with multiple sources or multiple destinations.

5.6 Recovery

Satellite communication is prone to disconnections that interrupt any ongoing data transfers. The data transfer agent shall keep track of transferred data so that a recovery from signal outage does not retransmit a huge amount of data. The shore side and the data transport agent on the vessel shall agree on the point of recovery. Transporting chunks of data and keeping track of the progress of chunks makes it easy for both sides to recover from an outage.

6 Data transport agent — vessel side interface

6.1 General

A data interface on the vessel side shall be flexible enough to accommodate a wide array of applications. Asynchronous data transfers are used for document exchanges as well as machine-to-machine communication such as IoT sensor data. Vessel side should include some of the interfaces shown in 6.2, 6.3, 6.4, 6.5 and 6.6, or other interfaces.

6.2 Transportation folders

A transportation folder is where either data transmissions from shore are stored as files or where the data transmission picks up files for transportation to shore. Separate folders can be used for separate transportation tasks. If the folder is used as a destination for many sources there is a risk of naming collisions. In such cases, the system shall support the creation of subfolders for every source.

6.3 File move and sync

6.3.1 Moving files

When moving files, the semantic is that whenever the files have been transferred, they should disappear from the sending folder. The sending folder shall be monitored for any new files, and whenever they occur, they should be moved at a schedule defined by a move policy.

6.3.2 Synchronizing folders

When synchronizing folders, the semantic is that whenever a file changes in the source folder, the same change shall appear in the destination folder. This is also true for deleting files in the source folder. The destination folder is a mirror of the source folder.

6.4 Server message block

The server message block (SMB) file sharing protocol allows computers to read and write files to a remote host over a local area network. The folders on the remote host are called “shares”, and for all practical purposes behave similar to a normal folder. For data transport, this means that the agent responsible for the transportation of data shall support handling remote shares just the same as local folders. The local client shall support SMB v.2.1 or higher, to be able to store and fetch files from SMB shares.

6.5 Asynchronous message service

IoT sensors, general logging and similar time-based data streams usually can be transferred asynchronously due to lack of strict timing requirements. In such cases, message queueing technologies should be used that among other features guarantee that no messages are lost. Most IP-based sensors already support MQTT and similar protocols can be needed. The transportation system shall be able to transport message queues between ship and shore effectively, meaning that proper compression shall be in place, based on the type of messages being transported.

On the vessel side, the data transport agent shall be able to either consume or act as an asynchronous MQTT broker. These messages are then compressed and transported to shore for delivery to a receiving agent. The data shall be transported in accordance with the resolution and frequency they are received from the data sources.

The technical requirements for MQTT shall be used in accordance with ISO/IEC 20922.

6.6 API

Machine to machine (M2M) is a form of communication between two entities without human interaction. This includes the data generated from industrial instrumentation, enabling sensor data to be transported to a system for further analysis. The data transport agent shall support communication with M2M devices through an API such as HTTP RESTful, GraphQL or similar. The API shall support delivery of data to be transported, as well as receiving data in addition to monitoring and command interfaces.

For supplementary information on the input and output API which is used in the transport agent, refer to Annex C.

7 Data transport agent — shore side interface

The shore side of the data transportation is an agent responsible for handling the data received or being sent to the vessel. It shall support the same interface mechanisms as the vessel side interface, meaning the local folder, SMB, asynchronous message service and M2M API.

In addition to such an agent, the transportation system shall support delivery and fetching of data from cloud storage systems. These cloud based storage services act similar to a local folder, meaning that data available there are candidates for either moving or synchronizing with a vessel, as well as being a storage place for data received from vessels.

8 Requirements for asynchronous data management agent

8.1 General

Ship to shore communication in most cases uses either satellite communication or typical terrestrial-based services. Satellite communication differ from terrestrial-based services in that the bandwidth is limited and the cost can be high. Backup satellite communication usually has severely limited bandwidth available and often at a premium cost. Due to these bandwidth constraints, the communication shall be able to prioritize traffic types over congested networks, based on available bandwidth and/or type of carrier.

For supplementary information on the functions of asynchronous data management agent, see Annex B.

8.2 Size restrictions

Volume-based satellite carriers are commonly used as backup communication channels. It can still be desirable to transport certain small files, while blocking other larger files. The client on the vessel shall be able to restrict transportation of data based on the combination of size and available carriers.

8.3 Prioritization of data

The communication between ship and shore contains traffic types of different importance. Some of the data are vital for the operation of the vessel, as other data are of minor importance. The data transport agent shall be able to differentiate the data and put constraints on it based on the policy set forth.

Due to the inherently different characteristics of the various communication carriers available to a vessel such as available bandwidth and cost, the data transport agent shall be able to prioritize different traffic types based on the available carrier. For instance, low bandwidth backup carriers can be candidates which shall prioritize the communication of important operational data.

8.4 Carrier status

The software platform on the vessel shall have knowledge about which carrier is currently in use for the specified data transport. This information is vital for the data transportation agent to apply the correct bandwidth management policy.

8.5 On-demand data request

In addition to scheduled data transports, the data transport agent shall be able to initiate data transport whenever data are ready. For instance, when data are available on the shore-side, the agent on the vessel can initiate on-demand a transport of that data. Likewise, data available on vessel side should be able to be transported on-demand outside of scheduled time. Meta information about the data available on vessel-side should be available to shore-based system.

8.6 Delayed transmission

In many cases, there is a huge benefit from delaying transmission to instance fixed intervals. Huge data transfers can be delayed until the pressure on the satellite carrier is low and certain data such as IoT and text-based log lines gain a bigger benefit from compression when more data are collected over time.

8.7 Resume on interrupt

Satellite carriers are prone to frequent errors and disconnects, which can make problems for large data transfers. To overcome this, the data transport agent shall keep track of what data has already been transferred before such an interruption, and then be able to continue without resending a lot of data. This is true even if there is a carrier change during the interruption. Based on priority settings, some data transfers can be put on pause if the carrier is changed to another type that does not allow that traffic type.

8.8 Monitoring

The data communication shall be monitored and the progress shall be fed back to the system.

As the communication link is usually over slow satellite links, the data transfer can take a long time to complete. As such, it is important to monitor the following:

- how much data that currently has been transferred to which destination;
- how much data are left to transfer;
- when data are available at source;
- when data are delivered to destination;
- carrier status;
- whether the vessel is online or not.

9 Requirements for security of data transmission

9.1 General

It is necessary to establish enough trust in the transportation so that there is no unintended data leakage and no need to double-check the data transferred. Transmission failures can also have safety or security consequences with the severity being dependent on the criticality of the data contained in the transport.

The following general mechanisms shall be in place to establish proper trust in the transportation.

- Integrity: The content of a transportation cannot be tampered with.
- Authenticity: The identity of the originator of the transportation can be verified.
- Confidentiality: The contents of the transportation cannot be read by others than the intended receiver.

Depending on the data within the transportation, it can be necessary to provide proof that the data was delivered to the intended receiver system. In such cases, it is necessary to add:

- Non-repudiation: Providing proof that the data was delivered to the recipient.

9.2 Transport security

In general, all data transmissions should be adequately protected by encryption.

The appropriate encryption method and key exchange method should be selected considering the importance and usage of the data.

Due to the compromise of cryptography by the improvement of computer performance, the appropriate algorithm can change over time, and the best practice algorithm at the time of implementation should be adopted.

ISO/IEC 18033 and NIST SP 800 are examples of related standards that should be referenced. It is also desirable to use secure encryption and cryptographic key management methods recommended by public organizations in each country at the time of implementation.

Data encryption uses the symmetric key cryptography AES, and its key sharing is recommended to be DH, DHE, ECDH or ECDHE for public key cryptography, and PSEC-KEM for hybrid cryptography.

Also, TLS1.3 specifies the use of AES GCM, AES CCM or ChaCha20-Poly1305 for encryption, DHE or ECDHE for key exchange, RSASSA-PSS, RSASSA-PKCS1-v1_5 or ECDSA for digital signature, and SHA-256, SHA-384 or SHA-512 for hash functions.

All transportation should include a timestamp or sequence number to avoid that the traffic is intercepted and resent, at a later time, by hostile parties, and by that interfere in the same or a different session.

All transportation of any importance can be electronically signed. The signature should protect the integrity of every important data elements, including an eventual timestamp.

The meta information regarding transmission of outgoing and incoming data shall be kept as proof of transmission and reception.

Different security encryption strategies can also require consideration, to take into account the importance of the data and the intended use.

9.3 Data security

To ensure confidentiality, the content of the data shall be encrypted with a sufficiently strong encryption key.

Transmission of data over a secure channel provides confidentiality, without having the data source to encrypt the data content itself. However, it can still be necessary to encrypt the data content if it requires protection from being read by some parties that can get access to the data at either the receiving or intermediary (cloud relay) side.

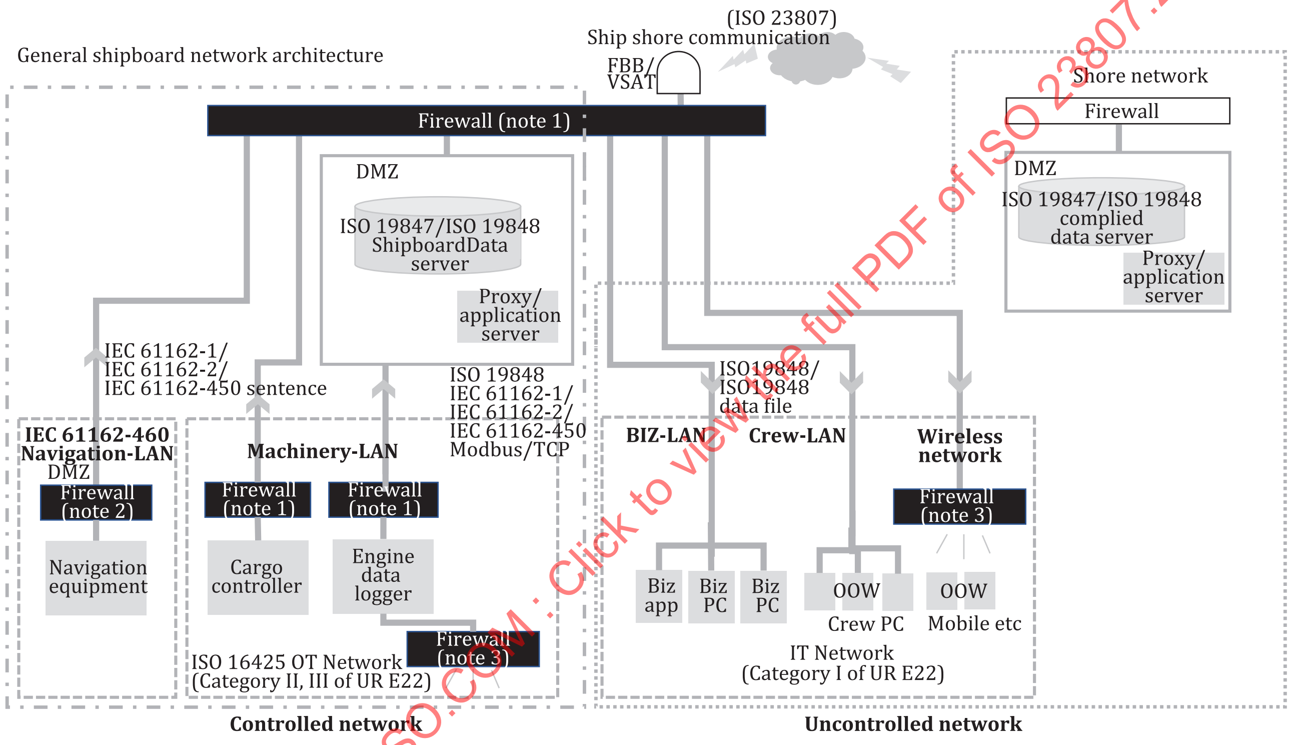
Common electronic signature systems often rely on public-key cryptography and asymmetric keys which cannot be suitable for encryption of larger data. An electronic signature system shall, if necessary, contain provisions for the generation and exchange of tools such as symmetric keys that can be used to encrypt data of maximum size used between senders and receivers.

Annex A
(informative)

Correlation chart

A.1 General

Figure A.1 shows the correlation between this document and other relevant standards such as ISO 16425, ISO 19847, ISO 19848 and IEC 61162-1, IEC 61162-2, IEC 61162-450 and IEC 61162-460.



NOTE 1 The firewall is part of the 460-Gateway or 16425-Gateway. The 16425-Gateway can consist of L3, UTM and etc.

NOTE 2 The firewall complies with the requirements of the 460-Gateway. The 460-Gateway can consist of L3, UTM and etc.

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

Figure A.1 — Correlation chart

Annex B
(informative)

Functions of asynchronous data management agent

B.1 General

This annex provides supplementary information on the functions of asynchronous data management agent in 8.1 of this document.

B.2 Concepts

- Task: a data transmission job defined with name, type, sources, destinations and data locations.
- Source client: a data transport agent from where data are transmitted. A task should have one or multiple source clients configured.
- Destination client: a destination client is a data transport agent to where data are transmitted. A task should have one or multiple destinations.
- Data location: a location storing sending or receiving data on a source client or destination client.

B.3 Clients registration

All clients should be registered in the asynchronous data management agent and the agent manages all clients registered.

B.4 Task configuration

B.4.1 Create task

All tasks should be created and registered in the asynchronous data management agent with following information:

- type of task;
- one or multiple source clients;
- one or multiple destination clients;
- data location on the source client;
- data location on the destination client;
- task name;
- options such as file type filter, delay, overwrite/rename when the same name data exists, carrier select;
- eventual carrier restrictions, such as not allowed to transfer data over volume priced and low-bandwidth carriers.