Onboard Maritime ICT Architecture and Standards

ISTS Report R3.1
V1.3 – 2024-11-22

MARITIME ITS

Intelligent Ship Transport System

Document information

Title	R3.1 Onboard Maritime ICT Architecture and Standards
DOI	10.13140/RG.2.2.15434.34246
Classification	Public

Editors and main contributors	Company
Ørnulf Jan Rødseth (ØJR)	SINTEF Ocean
Ørnulf Jan Rødseth (ØJRI)	ITS Norway

Rev.	Who	Date	Comment
1.0	ØJRI	27.07.2023	Final edition – only editorial changes
1.1	ØJRI	10.09.2023	Added MQTT, comment on current halt of ISO 23816, editorials
1.2	ØJRI	16.09.2023	Minor editorials after comments
1.3	ØJRI	22.11.2024	Additional editorial changes

Table of Contents

Executive Summary

This report defines an ICT architecture for the onboard computer-based systems on a ship. It gives an overview of the protocol standards and data models that are commonly in use on ships. The emphasis is on system connectivity and the ability to get information from the different systems and how to transfer information between ship and shore Cyber security is an important issue in all aspects related to information transfers between protected and unprotected networks. Physical security is part of this, but not a central aspect in this report.

The report is fairly exhaustive with regards to protocols described but it is also clear that very few ships have full connectivity between all equipment onboard. There is also a lack of uptake of already available standards that to some degree hinders data collection from ships.

Terminology and abbreviations

AIS	Automatic Identification System
API	Application Program Interface
CMDS	Common Maritime Data Structure
DMZ	Demilitarized Zone (between firewalls)
EGDH	Expert Group on Data Harmonization (sub-group of IMO FAL Committee)
FAL	Facilitation Committee in IMO
FTP	Internet file transfer protocol, secure version as SFTP
GNSS	Global Navigation Satellite System
HF	High Frequency (Short wave radio)
HTTP	Internet hypertext transfer protocol, secure version as HTTPS
IACS	International Association of Class Societies
IACS	Industrial Automation and Control Systems (not used in this document – OT used instead)
IALA	International Association for Aids to Navigation and Lighthouse Authorities
ICT	Information and Communication Technology
IEC	Standards organization International Electrotechnical Commission
IHA	International Hydrographic Office
IMO	International Maritime Organization
IP	Internet Protocol
IPV6	IP version 6 (most network today are IPV4)
IRDM	IMO Reference Data Model
ISO	International Organization for Standardization
IT	Information Technology
ITS	Intelligent Transport System
JSON	JavaScript Object Notation
Kbps	Kilobits per second
MF	Medium frequency (medium wave radio)
MIRA	Maritime ICT Reference Architecture
MSC	Maritime Safety Committee in IMO
MSW	Maritime Single Window
MQTT	A publish-and-subscribe messaging protocol maintained by OASIS
OPC UA	Open Process Control Unified Architecture
OT	Operations Technology

PKI Public Key Infrastructure

PGN Parameter Group Number (NMEA 2000)

S-100 The new hydrographic system for description of electronic chart s and overlays

SCADA Supervisory Control and Data Acquisition

SIP Strategic Implementation Plan (of e-navigation [25])

SMB Server Message Block protocol by Microsoft (distributed file system).

SOLAS IMO Convention on Safety of Life at Sea (stricter requirements to these ships)

REST Representational State Transfer (architectural style for HTTP and similar systems)

SCADA Supervisory Control And Data Acquisition

UNECE UN Economic Commission for Europe (Responsible for UN/EDIFACT maintenance)

UN/EDIFACT Messaging standard developed and maintained by UNECE.

VDES VHF Data Exchange System (extension of current AIS communication system)

VHF Very High Frequency – for ships this is approximately 156 MHz to 174 MHz

VPN Virtual Private Network

VTS Vessel Traffic Services

XML Extensible Markup Language

1 Introduction

1.1 Scope

ISTS Report R3.1 [3] gives an overview of the general concept of the ICT reference and physical architectures. This report contains a draft of a physical ICT architecture and an inventory of existing standards for onboard ICT systems. This report will not include detailed discussions on issues related to communication with off-ship parties. This will be covered in the reports on port and commercial operations. The next report in this series (R3.2) will describe land side systems and more extensively the protocols in use between ship and land. A final report (R2.1) will outline a possible maritime ICT architecture, including both ship and ship connected entities.

1.2 The physical architecture components and structure of the report

Figure 1 will be used as the basic pattern for the ICT architecture. The main contributions from this report are in the green areas while other areas will only be described on an overview level.

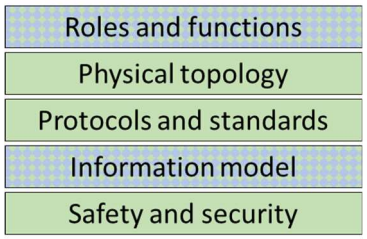

Figure 1 – The ICT architecture pattern

The main components are:

- *Roles and functions*: This will eventually be part of the reference architecture, but a first draft will be included in this report's section 2. There will also be some local roles onboard that is not necessarily transferred to the reference architecture.
- *Physical topology*: This is the actual physical architecture that represent the "typical" way data networks are used in a modern ship. Some details are presented in section 3. Safety of security in integrated systems is an essential issue and information about applicable standards are in section 8.
- *Protocols and standards*: The protocols used internally in the ship are described in sections 4 to 6. Sections 5 and 6 address different parts of the architecture, with section 4 containing more general information.
- *Information models*: These may be implicit or explicit but represents the collection of all important information elements used in the operations in the domain and their definition. Some of this will go to the reference architecture if they are of interest in other domains. Section 7 discusses this issue.
- *Safety and security*: Measures to safeguard the exchange of correct information against effects of technical faults or malicious acts. Section 8 lists applicable standards in this area.

Annex A contains a summary of all discussed standards, a snapshot of their status and the committees that develop them.

The last unnumbered section contains references. A reference to one of these entries in the text is a number in square brackets, e.g. [1].

2 Roles and functions

2.1 Some possible externally visible roles

Other documents in the R2 series will define some necessary roles for the ship. However, already at this point one may define a few that are mentioned, e.g. in international regulations.

- **Master:** Both the FAL Convention [1] and the principles for mandatory ship reporting systems [2] name the master as the one responsible for certain types of reporting.
- **Ship:** The principles for mandatory ship reporting systems [2] most commonly names the ship as the entity that is required to report. In most cases one can probably look at the master as the legal "representative" of the ship.

There are also other persons on board that may be used to represent roles, e.g. the one signing the health declaration or the chief engineer in relation to spare parts orders. However, it is expected that in most cases the master, and hence, the ship, can likely be used as the general role when the ship is seen from the outside.

2.2 The main onboard functions and roles

In some cases, particularly when looking at onboard system integration, it is necessary to refer to the functions performed onboard the ship. The actual functions implemented on a ship will vary with the ship's size and functions.

Table 1 – Overview of different network functions

Group	Example	Description
Bridge	Navigation	The navigation equipment
	Light	Lantern and deck lights controls
Safety	Fire	Fire detectors, fire doors and related equipment
	PA	Public announcement system, including general alarm
	Security	Closed circuit television, intruder detection etc.
	Watertight	Watertight doors and hatches and related equipment
	Stability	Water ingress detectors, ballast tank and pump control
Automation	Engine	Engine control, exhaust monitoring, etc.
	Power	Power generation, distribution and management
	Cargo	Cargo monitoring if in place, level measurement, cargo pumps etc.
	Deck	Deck equipment, anchor handling, hatches, cranes etc.
	HVAC	Heating, ventilation, air condition
	Hotel	Fresh, grey, and black water, galleys, laundry, food storage etc.
Administrative	Back-bridge	Equipment related to voyage planning and management
	Engineer	Systems related to ship maintenance, spare parts etc.
	Office	Other administrative systems, e.g. crewing, supplies, ISM, ISPS etc.
Public	Public	Crew/passenger data networks for general access to internet

Table 1 shows some typical networks that may be in use on a ship. These networks are also grouped into five main groups. The first three groups are related to control and monitoring of physical equipment and will involve operational technology (OT) networks. The last two groups are of the

information technology (IT) type. This table is a subset of a corresponding table developed and documented in the AUTOSHIP project [4].

This is just an example of a possible configuration. Some ships may merge some networks into one and other ships may not use networks for some of the control functions.

3 The physical architecture onboard a modern ship

Modern ships will generally have several data networks onboard, serving various functions as described in the previous section. These may also be interconnected to facilitate data transfer between different domains.

3.1 A possible physical architecture

An example of a possible physical architecture is shown in Figure 2 The structure of the physical network is typically layered with shorter distance and more specialized instrument networks at the bottom. These are networks that connect sensors and actuators to control and monitoring computers residing on the process layer. The processes are normally separated from each other to avoid that a single error in one sub-system propagates to others, but there may be special "Inter-process forwarders" (IPF) that pass some types of information between the network, e.g. to control engine speed from the navigation network. Process and instrument layers contain OT networks with high criticality for safe operation of the ship. If these are connected to other IT-networks one will need a controlled gateway (CGW) to block cyber-attacks or failures from propagating from the IT networks to the OT-networks, see section 3.4 for an example. For the same reasons, the OT-networks will normally not be connected to communication equipment that allow access to the general internet.

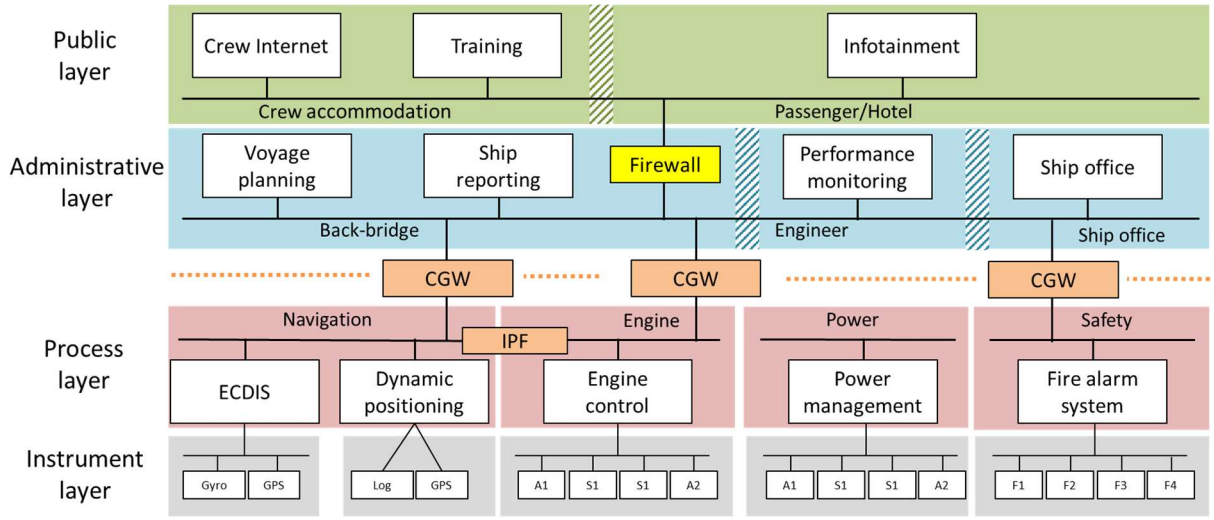

Figure 2 – A possible physical ship data network architecture

Over the process layer one will find the IT-networks. This may be "semi-controlled", such as the administrative layer where, e.g. back-bridge and ship office networks reside. These networks are less critical than the OT-networks, but still important for operation of the ship. Finally, one will find a public layer where crew and passengers may access more general onboard or internet services.

Figure 3 is a generalized diagram that show some of the typical sub-types of the ship data networks. The general requirements to such integrated networks will be addressed by ISO 16425 [5]. The figure shown here is a generalization and does not show all possible implementations of ship networks.

The networks are divided into three main groups: Those that placed in a controlled environment, ain a semi-controlled, or an uncontrolled environment.

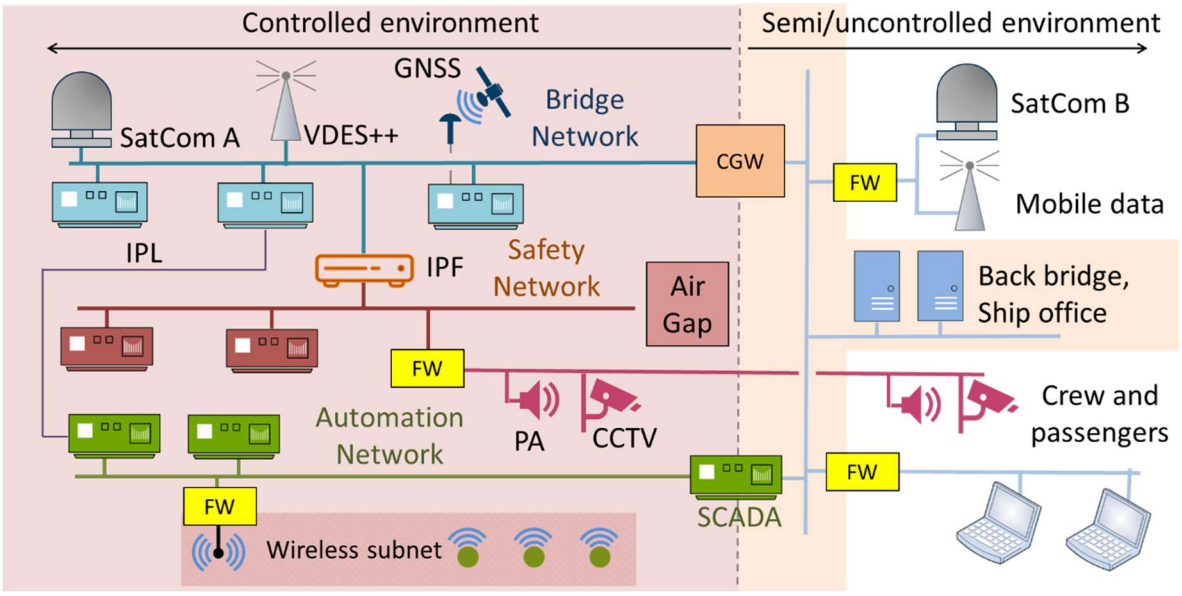

Figure 3 – A functional classification of the ship network sub-types

The use of controlled environments is mainly due to the need for protection of the OT-networks like navigation, safety, and automation from more public networks like administration or accommodation. The networks are also isolated from each other to avoid propagations of failures from one controlled network to another. Controlled environment means that these networks are protected from physical tampering as well as from cyber-attacks via the open internet or other ship networks. When connectivity is needed, this will be through special purpose "inter-process forwarders" (IPF) or direct point to point communication as shown as an "Inter-process link" (IPL).

The controlled networks can be protected from cyber-attacks through other networks by "controlled gateways" (CGW) which may include the use of firewalls and "de-militarized zones" (DMZ). Even inside these networks one also may need additional firewall (FW) functionality for wireless sub-networks or for networks that may be physically accessible in uncontrolled environments. Some networks may also be completely isolated ("air gap") from the uncontrolled networks.

Sometimes, one can also use a Supervisory Control and Data Acquisition (SCADA) unit, i.e. a process control computer, as gateway to external networks. This will implement some form of data access gateway, e.g. based on OPC UA (see section 6.3) or on ISO 19847 (see section 4.3). This solution may have a higher risk of cyber-attacks and should be avoided for critical systems.

Satellite or mobile data gateways will normally be placed in the uncontrolled or semi-controlled networks, but there may also be specialised external gateways, e.g. on the navigation network. This can be a VDES gateway to receive special messages from other ships or from shore or satellite equipment for receiving weather forecasts or maritime safety messages. These gateways will not normally allow general internet access to or from the ship.

As modern ship operations more and more rely on data exchanges with shore entities, also in automation and navigation networks, this means that the CGW functions must have facilities for safe and secure transfer of information to or from the OT-networks.

3.2 Controlled network

Figure 3 shows a section of networks in a "controlled environment". The term is derived from "controlled network" which is defined in IEC 61162-460 [6] as a network that has been designed to operate such that it does not pose any security risks to any of its connected network nodes.

This will require certain safety and security facilities in the network implementation as well as possibly a physical protection from any unauthorized person to access network nodes or network infrastructure. Thus, the term "controlled environment".

3.3 Safety and security of field or wireless networks

As shown in Figure 3, some controlled networks may extend into areas where physical control may be challenging. One example shown is a safety network connection e.g. public announcement (PA) or CCTV equipment in public areas to the safety management system. Another example could be light or lantern control systems. These networks may be wired or wireless.

These systems may allow unauthorized persons to get physical access to equipment and network infrastructure, unless constructed to avoid such problems. This may include the use of encrypted network traffic or verification of Ethernet and IP-addresses of connected equipment.

3.4 Controlled gateway (CGW) for interconnections between critical networks

The purpose of the CGW is to avoid involuntary or intentional network attacks on functions in controlled networks while still allowing some authorized data traffic to take place. IEC 61162-460 [6] defines a 460-Gateway function for the CGW function between navigation networks and other uncontrolled or semi-controlled networks. It is illustrated in Figure 4. This variant is also specified by ISO 16425 [5] as a valid CGW for use in the more general ship network.

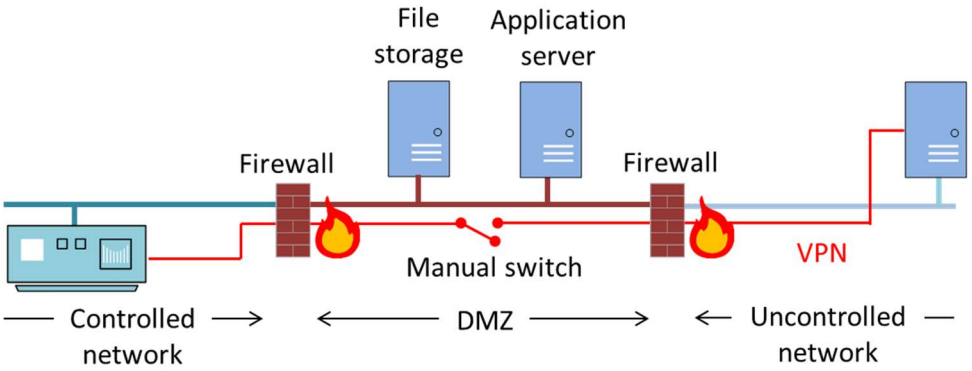

Figure 4 – Design of 460-Gateway as CGW

The 460-gateway consists of two firewalls that block all traffic other than between nodes on the external network and nodes in the DMZ. Typically, the DMZ nodes will be shared file storage or special purpose application servers, e.g. data loggers.

It is also possible to set up a direct link between nodes in the controlled and uncontrolled network, but this must use the VPN (Virtual Private Network) protocol and there must be a manual switch to allow authorized personnel to control the turning the link on and off.

3.5 External connections to the controlled network

Figure 3 shows a general ship network, including different controlled network. The figure shows four ways a controlled network can interface to other nodes or networks:

1. Via an inter-process data link (IPL) where a direct point to point data link is used to, e.g. send thrust control commands from the bridge to the engine automation.
2. Via an inter-process forwarder (IPF). This is described in the IEC 61162-460 standard as a 460-forwarder.
3. Via a controlled gateway (CGW). Section 3.4 described a controlled gateway from the navigation network to other networks. Section 4.3 discussed a general data server that can be used inside the controlled gateway.
4. Via a SCADA unit that has interfaces to both the controlled network and the external network. Unless carefully designed, this solution may increase the risk for cyber-attacks.

For the ISTS project, solutions 3 and 4 are the ones with relevance. The actual protocol for access to the data collection unit will vary. One possibility is the ISO 19847 solution (see section 4.3), another is to use, e.g. OPC UA (see section 6.3).

4 General data network and data collection standards

This section discusses some standards that are used or intended for general use onboard the ship. This includes general data network protocols and various systems for collecting data from other units or networks.

4.1 ISO 16425 – General ship network specification

ISO 16425 [5] contains definitions for ship data networks and guidelines for the installation. It gives specifications relating to such matters as the communication network-system architecture, data requirements, administration, operation, commissioning, inspection and testing.

This standard also takes into account differences between shipboard communication networks and networks that are used outside of ships and stipulates requirements and the like in clauses relating to matters unique to shipboard use.

The overall architecture that is used in this standard is similar to the one shown in Figure 2 and Figure 3

4.2 ISO 24060 – Software maintenance requirements of shipboard equipment

This standard defines a Ship Software Logging System (SSLS) for shipboard equipment software. Recognizing that maintenance of shipboard software is a major undertaking this standard initially sets base characteristics. The SSLS may be used by various users and log data from various types of equipment. It is expected that this standard will evolve over time together with related regulations and when experience on the use of the introduced concept accumulates.

Part 1 of this standard contains general requirements to the system that collects the software revision codes while part 2 contains more specific requirements for collecting the data from the equipment.

4.3 ISO 19847 – Data application server

ISO 19847 [10] defines a general-purpose ship data server that can be used as an application server in the DMZ of a CGW. A high-level overview of the design is shown in Figure 5. It consists of a data collection input function that listens in on different protocols, dependent on the type of network it is connected to. Data is stored in a database and made available to external data users through different mechanisms. FTP and HTTP shall be supported, but data users may also be able to use other protocols as exemplified in the figure.

ISO 19848 gives additional specifications for file formats, tag names and other data related issues. XML, JSON and CSV as data transmission formats for the data users are defined, but other formats are allowed. Tag names are mainly defined for machinery and automation functions.

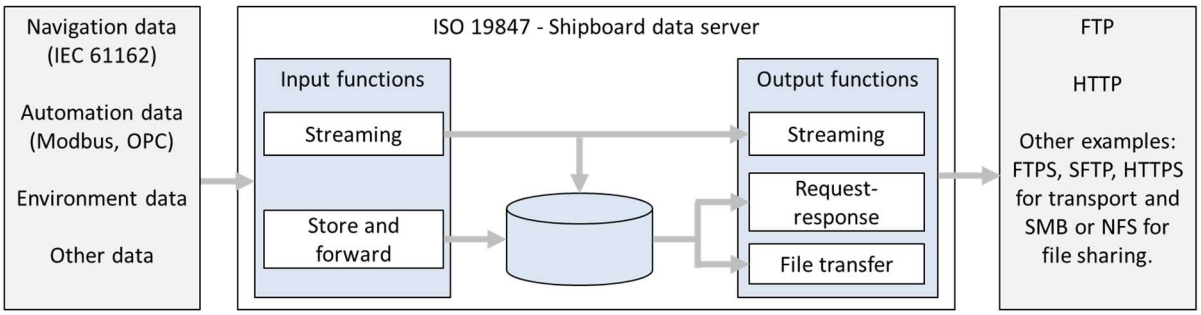

Figure 5 – The ISO 19847 general architecture

4.4 ISO 4891 – General data collection in the ship networks

Originally written as a specification of data acquisition mechanisms to the smart logbook (ISO 21745 [15]), the ISO 4891 standard [12] is now being generalized to any type of "smart applications".

The standard specifies a network (of networks), generally outside the controlled networks that are used for safety related applications. The system is illustrated in Figure 6. The shaded modules are part of the ISO 4891 system.

The modules may or may not be equivalent to actual physical devices. The I/O units and gateways are interfaces to specific sensing or data acquisition systems. I/O units will typically communicate using MQTT but must also support UDP broadcast and HTTP to implement service discovery and trusted message transfers.

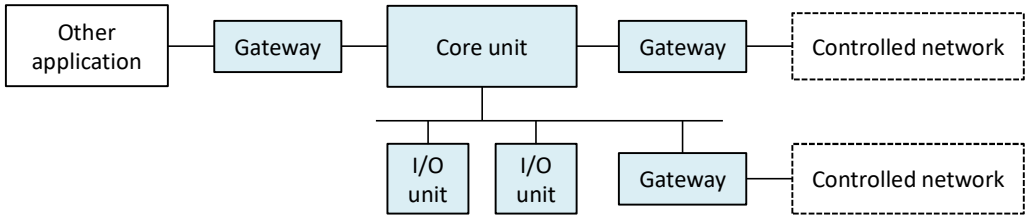

Figure 6 – Simplified illustration of ISO 4891 system

The Core unit implements several functions, namely:

1. Service discovery: First point of contact for nodes that are registering into the network. This is a combined UDP broadcast to new nodes with an HTTP API to look up available services.
2. Unit registry: Registration of I/O units and what type of data they can provide. This is done through HTTP.
3. Message broker: This is the main data distribution mechanism, using MQTT.
4. Certificate authority: This is normally implemented by the unit registry and will provide nodes on the network with public and private certificates for asymmetric encryption and digital signatures.

All nodes may also implement a direct messaging API via HTTP that allow direct access to the node from other nodes in the network.

JSON is the main format for data structures and messages in the system.

4.5 ISO 23816 – IPV6 ship network

ISO 23816 [13] is a proposed standard (start of 2022) that aims at integrating all networks on the ship in an IPV6 infrastructure. The system uses various payloads embedded in UDP datagrams. The payloads are based on existing protocol structures, e.g. various IEC 61162 message formats. There is also an application information service that can be used for device or service discovery.

The work on this standard seems to be halted for the time being. It is not clear when or if it will be resumed.

4.6 MQTT – Message Queuing Telemetry Transport

Message Queuing Telemetry Transport is an open OASIS standard that has also been made an international standard as ISO/IEC 20922 [37]. It is a lightweight publish-subscribe protocol, running

over TCP/IP and other transport protocols. It is using one message broker and any number of clients to send data between clients. The system uses hierarchical topics to publish and subscribe to different groups of data.

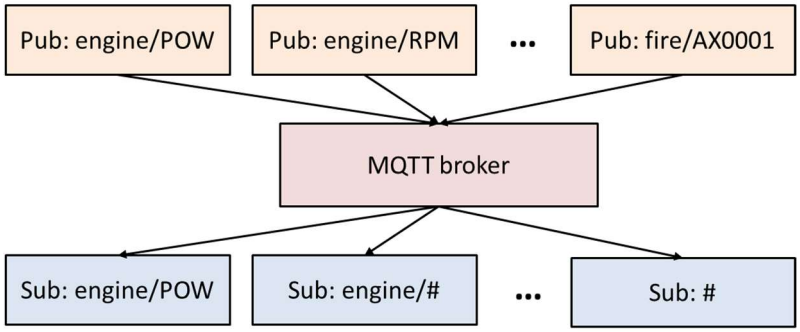

Figure 7 – MQTT overview

A client can publish (orange – "Pub:") data on a topic such as "engine/POW" or "engine/RPM" and other clients can subscribe (blue – "Sub:") to these topics or use wildcards to subscribe to all ("#") or some subtopics ("engine/#"). The single broker takes care of all administration and reduces complexity for clients. Data and management messages are sent over TCP/IP or other suitable protocols and use a binary format to reduce bandwidth overhead. MQTT does not specify any specific formats for data sent on a specific topic. This is application dependent, and the subscribers need to know the data format to read it correctly.

MQTT is increasingly popular in Internet of Things (IOT) applications due to its relative low complexity and lightweight implementation. It is also suggested as data acquisition protocols in ISO 4891 (see section 4.4).

Note that the system is dependent on a centralized broker and that this may result in too low robustness in some applications. Also, the protocol used between the broker and the clients is not suited for large volumes of data due to protocol overhead. If a system like this is used for data collection from ship to shore, one will normally add a dedicated data transmission service from the onboard MQTT broker to the data processing system on shore.

5 The navigation data network

Bridge systems are often integrated by the yard by using equipment from different manufacturers. This has driven the development of the interface standards described in this section, where the IEC 61162 series is the main standard. However, for integrated bridges one will expect to also see proprietary network solutions in parts of the bridge systems. There are also some military standards that are not described here.

5.1 IEC 61162-1/2/3 series for instrument networks

The variants of the IEC 61162 series of protocol that are commonly used on the instrument level are:

- IEC 61162-1 [16]: The definitions of NMEA text sentences for use in SOLAS ships. Serial line interface at 4800 bits per second.
- IEC 61162-2 [17]: A faster version of the IEC 61162-1, with higher baud rates.
- IEC 61162-3 [18]: A CAN bus solution, including a normative reference to NMEA 2000. However, this standard is not commonly used on SOLAS ships.

The IEC 61162 parts 1 and 2 uses a normal RS 422 serial line interface with optical isolation. Transmissions are based on text sentences as exemplified below, always with a terminating carriage return and line feed special characters ("\r\n") at the end:

```
$GPGLL,5057.970,N,00146.110,E,142451,A*27\r\n
```

This example is an output from a global navigation satellite system (GNSS) receiver with a position fix. The maximum length of such a sentence, not including CR and LF is 80 characters. Only the 7-bit ASCII character set is allowed.

5.2 IEC 61162-450/460 series for process networks

The two variants of the IEC 61162 series of protocol that are commonly used on the process level are:

- IEC 61162-450 [19]: An Ethernet version that encapsulates IEC 61162-1 sentences in UDP multicast packages for use on data networks.
- IEC 61162-460 [6]: Extension of IEC 61162-450 for higher degrees of security and safety. This standard also defines mechanisms for connecting the bridge network to other controlled and uncontrolled networks.

A network bus is constructed from network switches, and for IEC 61162-460, possibly also including an underlying mesh architecture, using spanning tree protocols to support redundancy. Logically, this will create a bus interconnecting several equipment as indicated in Figure 1Figure 8.

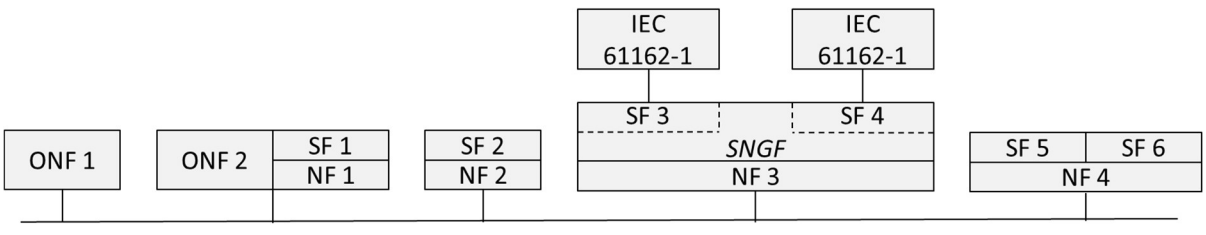

Figure 8 – An IEC 61162-450 network

Each device can have zero or more logical system function (SF) block. Each SF is assigned an SF identification code consisting of two letters and four digits. The SFs use a network function (NF) block to communicate with each other. A range of UDP multicast addresses are used to send messages to a group of listeners. Each UDP datagram can contain a number of IEC 61162-1 sentences including additional plain text formatting to specify, e.g. source and destination SF.

An example of a possible payload is shown below. VSI is a type of sentence that is used by AIS base stations:

```
\g:2-2-34,s:AB0001*39\$ABVSI,r3669961,1,013536.96326433,1386,-98,,*14
```

The leading text between backslash ('\') characters represent the additional formatting used. Here it contains a sentence grouping command (g:) and a sender identification code (s:). Several such lines can be sent in one UDP datagram, up to the maximum size of 1466 characters of payload. The grouping parameter allows sentences in different datagrams to be grouped together.

The protocol also allows the use of "Other Network Function Block" (ONF) that use other protocols, e.g. HTTP, to distribute information that is not in the form of IEC 61162 sentences. A special function block called a SNGF (Serial Network Gateway Function) is used to translate IEC 61162-1 serial line protocol to IEC 61162-450 datagrams.

The IEC 61162-450 protocol is very simple, and implementation should only take a few days. However, specifications are somewhat ambiguous and more complex use of the standard can be expected to be difficult to make interoperable with other implementations.

5.3 NMEA Networks

The following are commonly known standards from NMEA. They are not normally used onboard large seagoing vessels, so they are not listed in the annex table, but are included here for reference.

5.3.1 NMEA 0183 – Equivalent to IEC 61162-1/2

NMEA 0183 [7] is a superset of the IEC 61162-1 standard discussed above. NMEA 0183 contains additional sentences for use in AIS networks, including the Transport, Annotate and Group (TAG) function.

This standard is not relevant for larger ships as these ships are required to refer to IEC 61162-1.

5.3.2 NMEA 2000 – Equivalent to IEC 61162-3

NMEA 2000 [8] is a CAN based bus-solution with a bit rate of 256 kbps. This specification contains the definition of the transport protocol as well as a library of protocol data blocks (PGNs). NMEA 2000 is referenced by IEC 61163-3 with additional requirements to redundancy and other characteristics required for SOLAS use.

5.3.3 NMEA OneNet

OneNet [9] is a high-capacity network protocol based on UDP datagrams and IPV6. Payloads are based on the NMEA 2000 PNGs. This makes it relatively easy to implement. The specification has to be bought from NMEA together with certification tools and other services. Prices are significantly higher than for IEC specifications.

The primary features and goals of OneNet are as follows [9]:

- NMEA 2000 data transfer over IPv6 in a standard format.

- High-bandwidth applications such as radar, video and more that are not possible via NMEA 2000.
- Support Ethernet and TCP/IP at 1 gigabit and faster speeds.
- Utilize standardized connectors (RJ-45 and X Coded M12) depending on installation.
- Robust, industry-standard cybersecurity requirements.
- NMEA 2000 gateway compatibility.
- Mandatory device & application certification by the manufacturer, then verified by NMEA.

This specification is rarely used on larger seagoing ships. The alternative is normally IEC 61162-450.

6 Automation and safety networks

Automation and safety systems are commonly from a single manufacturer and has in this context less need for standardization. However, there are some standards on the instrument level bus solutions and on the interfacing between automation systems and other systems.

6.1 IEC 61158 – Instrument level fieldbus

On the instrument level there are several fieldbus standards that can be used. Some of these are standardized through the IEC 61158 [20] series of standards. These standards define 28 different "Communication Profile Families" (CPF) covering, e.g. Foundation Fieldbus, Profibus and many more. Profiles for traditional instrument level communication as well as for Ethernet variants are included.

These networks will normally be connected to a supervisory control and data acquisition (SCADA) unit on a process network. Thus, they are of relatively low interest in the scope of ISTS project.

6.2 IEC 61784 – Additional instrument level fieldbus

IEC 61784 [21] series of standards define additional communication profiles based on the specifications in the IEC 61158 series.

These networks will normally be connected to a supervisory control and data acquisition (SCADA) unit on a process network. Thus, they are of relatively low interest in the scope of ISTS project.

6.3 OPC UA – General automation interface

OPC UA is a general, flexible and open specification for a client-server system for collection of automation data, including subscription to changes in data objects. It can run on numerous transport protocols and transfer data in different formats. It is also standardised as IEC 62541 [22]. The specification is also openly available from the OPC web site [23] and various implementations are also available, some in the public domain.

Peer-to-peer communication and hierarchical systems can be designed by combining servers and clients in different configurations.

OPC UA can run over a number of data transmission protocols, e.g.:

- TCP/IP
- HTTPS
- WebSocket

For a newer publish/subscribe service, other protocols can be used, e.g.:

- UDP
- AMQP or MQTT

Data can likewise be transferred in several formats:

- XML
- UA Binary
- JSON

Services are available in the following main types:

- General data access: Basic client-server operations.
- Alarms and conditions: A subscription service based on the client-server principle.
- Historical access: Time series.
- Publish/Subscribe: This is an alternative to the basic client-server-model.

Most services can operate on single data elements or aggregates.

OPC UA is both used internally on process networks as well as a gateway between SCADA equipment and other networks.

6.4 MODBUS – Simple device interfacing

Modbus [27] is a serial communications protocol that was originally developed for use with programmable logic controllers (PLCs) in industrial control systems. It is now commonly used for communication between a wide range of devices in industrial automation and control systems, including PLCs, remote terminal units (RTUs), and supervisory control and data acquisition (SCADA) systems. Modbus is available in several variants including Modbus TCP/IP which is used over Ethernet and Modbus RTU over serial lines.

Modbus only transfers 16 bit maps or values and has no facility for naming data object other than its index number in the slave unit.

6.5 Shipdex F – Maintenance data

Shipdex (see section 7.6 and [11]) also contains a protocol for transfer of maintenance data that may be relevant for other uses onboard. This is called Shipdex F.

7 Information models

This section will discuss some existing data models used in digital data exchanges onboard ships. Many of these are implicit in protocol specifications, e.g. IEC 61162-1 others are more abstract, such as the IMO reference Data Model.

7.1 IMO Compendium – IMO Reference Data Model (IRDM)

The IMO reference Data model [25] was developed in a cooperation between WCO, UNECE and ISO to cover the semantic definition of the data elements that were referenced in the FAL Convention. It has later been extended to other areas, such as ship certificates and just in time arrival in ports.

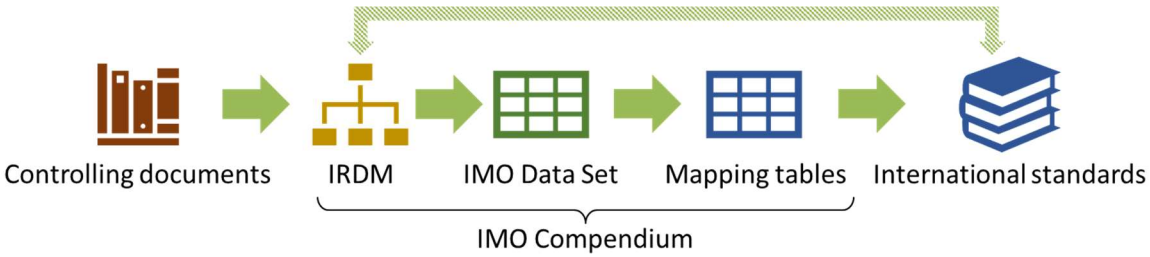

Figure 9 – Systematic view on IMO Compendium

The compendium is developed incrementally by adding new controlling documents to the system. Examples of this is the FAL Convention for the maritime single window and other IMO resolutions or circular for, e.g. mandatory ship reporting. Each document will normally add new elements to the reference data model, but the goal is to reuse as much of existing elements as possible. The individual elements in the model are given an identification number in the IMO data set and this is the basis for several mapping tables, currently to ISO, UNECE and WCO data models. These data models are the basis for the development or harmonization of the specific international standards. The participating standards organizations will ensure that the definitions in the standards and the IRDM is harmonized.

The IRDM and the IMO data set are maintained by the Expert Group on Data Harmonization (EGDH) which is a sub-group of the FAL Committee of IMO. The standards organizations also participate in EGDH to ensure correct match to their specific data models.

7.2 S-100 – Common Maritime Data Structure (CMDS)

The CMDS was defined as the underlying data model in the e-navigation SIP [26]. It was later decided to use the IHO S-100 infrastructure [36] to implement the CMDS. However, this causes some problems for non-geographic elements as S-100 does not have a systematic approach for organizing any operational attributes to the first order objects, which are the geospatial elements. This is now being to some degree remedied through the introduction of the concept register.

The components of the IHO Geographic Information registry (GI Registry) are shown in Figure 10. The different parts are:

- *Concept register:* A general collection of definition of terms identifying an object, information or phenomena of nature without any relation to other concepts.
- *Data dictionary register:* List of object names and definitions. Sub-set of concepts.
- *Portrayal register:* Different graphical objects used to assemble chart overlays (products).

- *Meta data register*: Empty for the time being.
- *Product specification register*: List of product specifications.
- *Producer code register*: List of approved producers of product specifications.

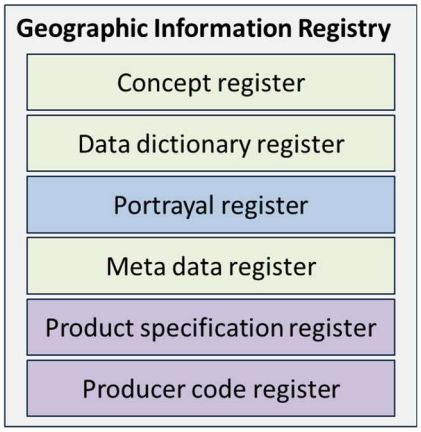

Figure 10 – The IHO Geographic Information Registry

Today harmonization to IMO Compendium is handled by ad hoc adding S-100 data elements to the IMO Reference Data Model. A more formal cooperation between IHO and IALA and the EGDH is being established.

7.3 ISO 28005 – Electronic Port Clearance

The ISO 28005 series of standards [14] has been developed as a protocol for ship-centric communication between ships and their agents and administrative or operative parties on shore. The series define a HTTP message structure consisting of a header, a body and various other components as shown in Figure 11.

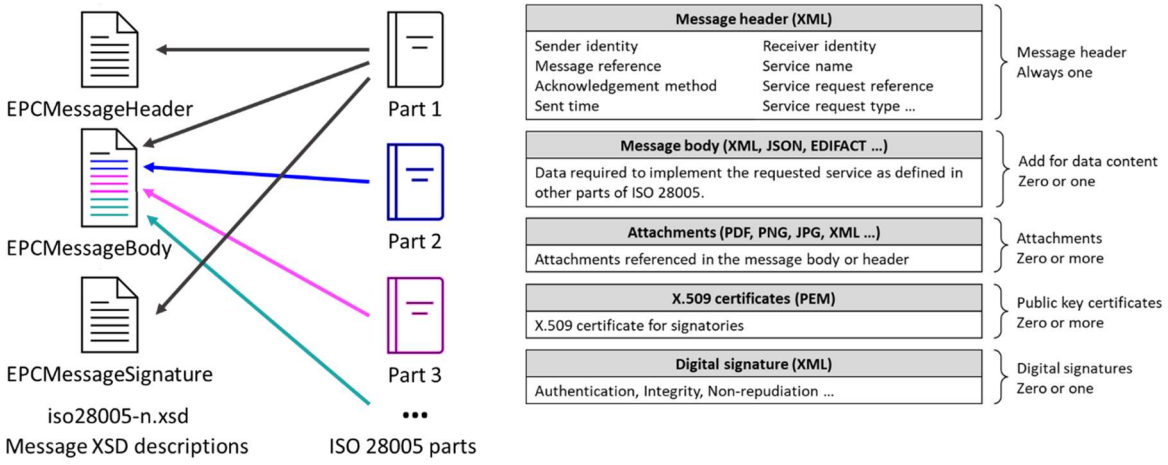

Figure 11 – Structure of ISO 28005 messages

The standard defines a data model that is converted into individual core data elements similarly to that what is done in the IMO Compendium. However, the models are not identical, although core elements can be mapped between them. The core elements can be put into a message body as shown in the figure to define different APIs. All APIs will us ethe same protocol and basic message structure. The content of the header and the body will define the specifics of the API.

The data model currently covers all data elements defined in the FAL Convention as well as additional elements for other IMO instruments, for just in time arrival and for other operational purposes. The model is available as XSD file at https://standards.iso.org/iso/28005/-2/ed-2/en/, together with a mapping to the IRDM. The data model is also available as an Enterprise Architect compliant file.

7.4 IEC 61162-1 – Navigational data model

IEC 61162-1 defines a form of implicit data model for data that is transmitted on a bridge network. The transmission format is sequences of data elements in a "sentence", normally representing output from some instrument or other equipment (see section 5.1).

There is no formal underlying data model, although the same data format and semantics seem to be reused where possible.

IEC 61162-3 has a more structured approach where data elements are defined separate from the structures they are used in and organized in numbered parameter groups (PNG – Parameter Group Number). The PNGs are the basis for constructing CAN bus messages. The PNG database is only available as purchase from NMEA.

7.5 ISO 19848 – Automation data

ISO 19848 [24] defines unified rules for developing machine and human readable identifiers and data structures for shipboard machinery and equipment, with the objective to facilitate exchange and processing of sensor data from ships. This includes a data channel concept and a time series concept. A data channel is a description of a specific data source, a time series is a collection of data sampled at specified times.

The standard gives rules for naming of time series and channels and also file formats for describing their properties.

Furthermore, the standard provides two ways to tag measurements, one based on the JSMEA (Japan Ship Machinery and Equipment Association) rules which is included in the printed standard, and one based on DNV VIS naming system. The latter is described here: https://data.dnv.com/.

There are also some standards from the general automation domain that may be used to name data objects, but these are of limited value on ships.

7.6 Shipdex D – Maintenance data

Shipdex [11] was originally a format and specification for delivery of equipment and maintenance documentation but has also been extended with a protocol for transfer of maintenance data between parties in the shipping industry. It consists of two main protocols:

1. Shipdex D: The specification for electronic maritime technical documentation.
2. Shipdex F: The specification for transfer of maintenance data.

Shipdex is a not-for-profit cooperation between several companies. Membership is required for commercial use of specifications.

8 Security of shipboard systems

8.1 Introduction

Safety requirements to equipment and network will depend on the criticality of the functions implemented. This document will not go into detail on this issue, but normally one will need to protect critical functions by providing redundancy or alternative ways to execute the function. Some of the standards discussed in preceding sections contain various safety provisions, normally by supporting some form of network or equipment redundancy.

Security is generally understood as protection against malicious digital attacks from external parties. This can take place via the internet, as virus on memory sticks or various other forms. This section will give an overview of some of the relevant standards for this area.

There are various general standards for security in critical networks, such as the IEC 62443 series [35] that covers much of the life cycle for such equipment. This section will go through some of the specific standards that are developed for use in the maritime domain.

The standards listed in section 8.2 are mainly addressing risks to the physical systems. However, it is also necessary to consider risks associated with data that is used by the systems. This is discussed in section 8.3.

Sections 3.2 - 3.5 also discuss specific safety issues related to the protection of controlled networks from network access from other systems on the ships.

8.2 Physical system cyber security standards

8.2.1 IACS E26 – Cyber resilience of ships

This standard [31] defines general principles and methods for protection of the ship against cyber-attacks. It will be a minimum requirement for classed ships from January 2024.

8.2.2 IACS E27 – Cyber resilience of on-board systems and equipment

This standard [32] defines more specific requirements to computer-based equipment and systems. It will be minimum requirements from January 2024.

8.2.3 ISO 23806 – Cyber safety risk assessment system

MSC-FAL.1/Circ.3 [29] puts down requirements to ship's safety management system to also include cyber security in the risk assessment. ISO 23806 [30] translates these requirements into more concrete guidance for cyber risk assessment and avoidance.

The standard gives requirements for establishing, implementing, maintaining and continually improving a cyber safety risk assessment system within the context of the company’s SMS.

The standard gives the specification to be met for the specific requirements to effectively identify and protect for cyber safety to provide assurance that these aspects are suitable within the overall SMS and to be compliant to the ISM and/or ISPS code as applicable, as well as any additional requirements of the company.

8.2.4 ISO 23799 – Assessment of onboard cyber safety

ISO 23799 [34] establishes the elements of onboard cyber risk assessment and the requirements for assessment process, assessment preparation, risk identification, risk analysis and risk evaluation.

This document applies to the risk assessment of onboard cyber systems based on network technologies as specified in MSC-FAL.1/Circ.3 [33], such as bridge systems, cargo management systems, propulsion and machinery management and power control systems, access control systems, passenger or visitor servicing and management systems, passenger-facing networks, core infrastructure systems, administrative and crew welfare systems, communication systems, etc.

8.2.5 IEC 63154 – Cybersecurity for navigation bridge equipment

IEC 63154 [28] specifies requirements, methods of testing and required test results to provide a basic level of protection against cyber incidents (i.e. malicious attempts, which actually or potentially result in adverse consequences to equipment, their networks or the information that they process, store or transmit) for equipment on the navigation bridge. Equipment approved according to IEC 63154 will be compliant with IACS E27.

8.2.6 IEC 61162-460 – Security in navigational networks

This standard (see section 5.2) specifies additions to IEC 61162-450 to ensure cyber-secure implementation of navigational bridge networks. This includes various requirements to the equipment itself as well as to the implementation of controlled gateways (see section 3.4) and similar network equipment. Work is under way on a new edition of IEC 61162-460 to include provisions for IACS E27 compliance.

8.3 Risks associated with data manipulation

Standards in section 8.2 intends to harden systems and networks against attacks, either physically onboard the ship or through data networks.

However, one may also have attacks on data transmissions, aiming to falsify information that is used by onboard systems to do critical tasks.

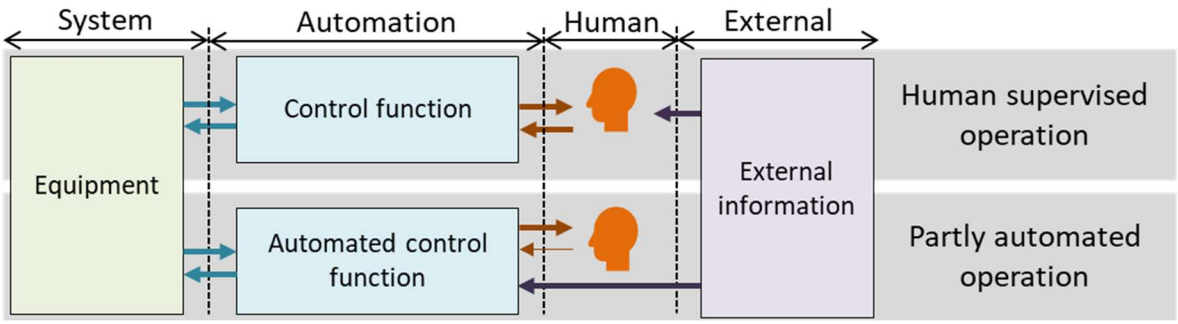

Figure 12 – Automation with or without human quality control

The problem is illustrated in Figure 12 where it is indicated a low (top) and high (bottom) automation case for the same control problem. In the low automation case, all external information is passed through the human which can do at least some form of sanity and quality control of the information before it is used in the control process.

In the high automation case, information is passed directly to the automatic controller without human control. While the first case is also susceptible to manipulation of external data, the second case is much more critical as quality control must be performed by automation. This may be possible in some cases, e.g. by defining static or dynamic bounds on received information, it will in general require digital signatures on the information to ensure that authenticity of sender can be verified and also that the actual data has not been tampered with.

This issue will be returned to in report D3.2 on ship to shore data communication but interested readers can have a look at IMO FAL.5/Circ.46, Guidelines on Authentication, Integrity and Confidentiality in Information Exchanges [38].

The FAL Circular addresses data received from sources outside the ship, but in principle, this problem also applies to external data received from other shipboard sources, unless these are placed in controlled networks and the transfer of information is safeguarded by encryption of physically protected data transmissions.

References

[1] The Convention on Facilitation of International Maritime Traffic, as amended.

[2] IMO Resolution MSC.433(98) Guidelines and Criteria for Ship Reporting Systems, adopted on 16 June 2017.

[3] ISTS Report R2.1 Introduction to the Maritime ICT Architecture, 2023-01-16, available from http://ists.mits-forum.org/.

[4] Rødseth Ø.J., Faivre J., Hjørungnes S.R., Andersen P., Bolbot V., Pauwelyn A.S., Wennersberg L.A.L. "AUTOSHIP deliverable D3.1: Autonomous ship design standards", Revision 1.0, June 2020.

[5] ISO 16425 Ed. 2 Ships and marine technology — Specification for the installation of ship communication networks for shipboard equipment and systems (DIS voting by February 2022).

[6] IEC 61162-460 Maritime navigation and radiocommunication equipment and systems – Digital interfaces – Part 460: Multiple talkers and multiple listeners – Ethernet interconnection – Safety and security.

[7] NMEA 0183 description: https://www.nmea.org/nmea-0183.html

[8] NMEA 2000 description: https://www.nmea.org/nmea-2000.html

[9] NMEA OneNet description: https://www.nmea.org/nmea-onenet.html

[10] ISO 19847 Ships and marine technology — Shipboard data servers to share field data at sea.

[11] Shipdex descriptions: https://ww2.shipdex.org/

[12] ISO 4891 Ships and marine technology — Interoperability of smart applications for ships (under development).

[13] ISO 23816 Ships and marine technology — Secured ship network based on IPv6 Ethernet network (under development).

[14] ISO 28005 Ships and marine technology — Electronic port clearance (EPC) - several parts.

[15] ISO 21745:2019 Electronic record books for ships — Technical specifications and operational requirements.

[16] IEC 61162-1 Ed. 5: Maritime navigation and radiocommunication equipment and systems - Digital interfaces - Part 1: Single talker and multiple listeners

[17] IEC 61162-2 Ed. 1: Maritime navigation and radiocommunication equipment and systems - Digital interfaces - Part 2: Single talker and multiple listeners, high-speed transmission

[18] IEC 61162-3 Ed. 1.2: Maritime navigation and radiocommunication equipment and systems - Digital interfaces - Part 3: Serial data instrument network

[19] IEC 61162-450 Ed. 2: Maritime navigation and radiocommunication equipment and systems - Digital interfaces - Part 450: Multiple talkers and multiple listeners - Ethernet interconnection

[20] IEC 61158: Industrial communication networks - Fieldbus specifications.

[21] IEC 61784: Industrial communication networks – Profiles.

[22] IEC 62541: OPC unified architecture.

[23] OPC UA website: https://opcfoundation.org/about/opc-technologies/opc-ua/

[24] ISO 19848 Ships and marine technology — Standard data for shipboard machinery and equipment.

[25] The IMO Compendium on Facilitation and Electronic Business, The IMO Reference Data Model, https://imo.org/en/OurWork/Facilitation/Pages/IMOCompendium.aspx

[26] IMO MSC.1/Circ.1595, E-Navigation Strategy Implementation Plan – Update 1, 25 May 2018.

[27] MODBUS specifications at https://modbus.org/.

[28] IEC 63154 Maritime navigation and radiocommunication equipment and systems - Cybersecurity - General requirements, methods of testing and required test results.

[29] MSC-FAL.1/Circ.3 Guidelines on Maritime Cyber Risk Management. July 2017.

[30] ISO 23806 Ships and marine technology — Cyber safety

[31] IACS Unified Requirement UR E26 Cyber resilience of ships, April 2022.

[32] IACS Unified Requirement UR E27 Cyber resilience of on-board systems and equipment, April 2022.

[33] MSC-FAL.1/Circ.3, Guidelines on maritime cyber risk management, July 2017.

[34] ISO 23799 Ships and marine technology — Assessment of onboard cyber safety.

[35] IEC 62443 Security for industrial automation and control systems (series)

[36] S-100 Introduction, http://s100.iho.int/home/s100-introduction.

[37] ISO/IEC 20922 Information technology — Message Queuing Telemetry Transport (MQTT) v3.1.1, Ed. 1 - June 2016.

[38] IMO FAL.5/Circ.46, Guidelines on Authentication, Integrity and Confidentiality in Information Exchanges via Maritime Single Windows and Related Services, June 1st 2022.

Annex A– Overview of standards and groups

The table lists the standards mentioned in this report with their full name. The status field gives the status of the specification as of time of writing (see revision field at cover page):

- Ed. N: Published as edition N
- Rev: Currently under revision by committee
- CD: Currently as Committee Draft
- CDV: CD for Voting
- WD: Currently as working draft
- DIS: Draft international standard
- IS: International standard, may be in maintenance in later editions
- Continuous: Continuously updated, available online.

Note: This status will rapidly be outdated, so this is only to be seen as an indication of status of the respective standards.

The colouring is as follows:

- Green: Data networks.
- Blue: Data models
- Grey: Cyber security

Table 2 – Overview of standards and their status

Standard	Name	Committee/Group	Status
IEC 61158	Industrial communication networks - Fieldbus specifications	IEC TC65/SC65	IS
IEC 61162-1	Maritime navigation and radiocommunication equipment and systems – Digital interfaces - Part 1: Single talker and multiple listeners	IEC TC80/WG6	IS Ed. 5
IEC 61162-2	Maritime navigation and radiocommunication equipment and systems – Digital interfaces - Part 2: Single talker and multiple listeners, high-speed transmission	IEC TC80/WG6	IS Ed. 1
IEC 61162-3	Maritime navigation and radiocommunication equipment and systems – Digital interfaces - Part 3: Serial data instrument network	IEC TC80/WG6	IS Ed. 1
IEC 61162-450	Maritime navigation and radiocommunication equipment and systems – Digital interfaces - Part 450: Multiple talkers and multiple listeners - Ethernet interconnection	IEC TC80/WG6	IS Ed. 2
IEC 61162-460	Maritime navigation and radiocommunication equipment and systems – Digital interfaces - Part 460: Multiple talkers and multiple listeners - Ethernet interconnection – Safety and security	IEC TC80/WG6	IS Ed. 2
IEC 61784	Industrial networks – Profiles	IEC TC65/SC65	IS
IEC 63154	Maritime navigation and radiocommunication equipment and systems - Cybersecurity - General requirements, methods of testing and required test results	IEC TC80/WG6	IS 2021

Standard	Name	Committee/Group	Status
ISO 4891	Ships and marine technology — Navigation and ship operations — Smart logbooks for shipping (proposed new title: Interoperability of smart applications for ships)	ISO TC8/WG10	CD
ISO 16425	Ships and marine technology — Guidelines for the installation of ship communication networks for shipboard equipment and systems	ISO TC8/SC6/WG16	DIS Ed. 2
ISO 19847	Ships and marine technology — Shipboard data servers to share field data at sea	ISO TC8/SC6/WG16	IS Ed. 2
ISO 23816	Ships and marine technology — Secured ship network based on IPv6 Ethernet network	ISO TC8/WG10	WD
ISO 21745	Electronic record books for ships — Technical specifications and operational requirements	ISO TC8/WG10	IS
MODBUS	Public domain specification from Modicon	n/a	n/a
OPC UA	OPC Foundation, Unified Architecture (also IEC 62541)	OPC/IEC	IS
Shipdex F	Maintenance data transfer	Shipdex	1.0
MQTT	Message Queuing Telemetry Transport (ISO/IEC 20922)	OASIS/ISO/IEC	1.0
S-100 CMDS	Common Maritime Data Structure (S-131, S-211, S-421)	IHO/IALA	Continuous
IMO Compendium	IMO Reference Data Model/IMO Compendium	IMO FAL	Continuous
IEC 61162-1	Maritime navigation and radiocommunication equipment and systems – Digital interfaces - Part 1: Single talker and multiple listeners	IEC TC80/WG6	CDV Ed. 6
ISO 19848	Ships and marine technology — Standard data for shipboard machinery and equipment	ISO TC8/SC6/WG16	IS Ed. 2
ISO 28005-2	Ships and marine technology — Electronic port clearance (EPC) — Part 2: Core data elements	ISO TC8/SC6/WG2	IS Ed. 2
ISO 28005-3	Ships and marine technology -- Electronic port clearance (EPC) -- Part 3: Part 3: Technical standard for administrative and operational data exchanges	ISO TC8/SC6/WG2	IS 2025
Shipdex D	Equipment and maintenance data models	Shipdex	2.3
IACS UR E26	Cyber resilience of ships	IACS	Apr 2022
IACS UR E27	Cyber resilience of on-board systems and equipment	IACS	Apr 2022
IEC 63154	Cybersecurity - General requirements, methods of testing and required test results	IEC TC80	IS 2021
ISO 23806	Cyber safety	ISO TC8/WG10	IS 2022
ISO 23799	Ships and marine technology — Assessment of onboard cyber safety	ISO TC8	IS 2024