Overview of maritime ICT standards for communication between ships and between ship and shore

ISTS Report R3.2
V1 – 2024-11-21

MARITIME ITS

Intelligent Ship Transport System

Document information

Title	R3.2 Overview of maritime ICT standards for communication between Ships and between ship and shore
Classification	Public

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

Rev.	Who	Date	Comment
0.1	ØJR	23.02.2023	Taken parts of R2.1 and converted to shore standards inventory
0.2	ØJRI	20.08.2023	First edition for review
1.0	ØJRI	21.11.2024	Final edit for publication

© 2024 ISTS CONSORTIUM

This publication has been provided by members of the ISTS consortium and is intended as input to the discussions on and development of a new maritime ITS architecture with associated standards. The content of the publication has been reviewed by the ISTS participants but does not necessarily represent the views held or expressed by any individual member of the ISTS consortium.

While the information contained in the document is believed to be accurate, ISTS participants make no warranty of any kind with regard to this material including, but not limited to the implied warranties of merchantability and fitness for a particular purpose. None of ISTS participants, their officers, employees, or agents shall be responsible, liable in negligence, or otherwise howsoever in respect of any inaccuracy or omission herein. Without derogating from the generality of the foregoing neither of ISTS participants, their officers, employees or agents shall be liable for any direct, indirect, or consequential loss or damage caused by or arising from any information advice or inaccuracy or omission herein.

The material in this publication can be reproduced provided that a proper reference is made to the title of this publication and to the ISTS project.

Contents

Executive Summary

Increasing digitalization in the society at large, including international ship operations, requires careful consideration of what communication system to deploy and how to use it. This includes basic communication basics, such as quality of service, whether the system supports fine grained API calls or only document transfers and how the system can be influenced by external factors, such as weather or geographic location. Wireless communication will be susceptible to a wide range of factors that can reduce the expected quality of service.

It is also necessary to consider how the ICT architecture is implemented in a larger system that includes the ship. In many cases, one will want to reduce direct ship to shore communication to only trusted parties on shore, e.g. only the owner or the manager.

While ships use a wide range of dedicated communication systems, most of these are used for very specific purposes and cannot be used for general internet type communication. Internet connectivity will normally be limited to various satellite communication systems or mobile data when close to shore.

When access to internet has been established, there are also several different protocol specifications that can be used. The different protocols have different features that make them suited for different applications. Some protocols may be best suited for general data acquisition, others for implementation of service APIs to service providers on shore, while other may be better for remote control and monitoring.

The data models employed by the different protocols also differ. Of particular interest is the abstract and mainly semantic IMO Reference Data Model (“IMO Compendium”) that form the sematic baseline for several other technical standards.

Terminology

Application protocol: A transport protocol that adds message header and other syntax to a transport protocol, to implement different APIs over the same API connection point.

API connection point: An endpoint for an application protocol that can accommodate several APIs over the same protocol.

Application Program Interface (API): A specific interface to transfer a defined data set over a transport protocol. This is like a remote procedure call and is more fine-grained than a document type interface.

Asynchronous: A message exchange that has a duration longer than the individual transport protocol connections.

Common Maritime Data Structure (CMDS): This is the common data model underlying the S-100 e-navigation framework.

Document type interface: This is an interface that just accepts a full data message and either accepts it or rejects it.

Hypertext Transport Protocol (HTTP): This is an internet application protocol that is commonly used by web browsers and servers [2]. It is also becoming popular in the design of API transport protocols. Normally the secure and encrypted version is used (HTTPS) [3].

IMO Compendium: This is the new reference data model maintained by the IMO Expert Group on Data Harmonization and currently implemented in ISO, WCO and UNECE standards. Part of the compendium is the IMO Reference Data Model (IRDM) [12].

Synchronous: A full message exchange that is performed during one single transport protocol connection.

Transmission Control Protocol over Internet Protocol (TCP/IP): This is a very common reliable transport protocol in the internet system [1].

Transport Protocol: The protocol, e.g. e-mail, HTTPS or TCP/IP, used to send and receive data.

NOTE: HTTPS is used by many application protocols as a transport protocol although HTTPS is an application protocol for general web services.

Transport protocol connection: For connection-oriented protocols, like TCP/IP or HTTP, a service requestor and a service provider will establish a connection before exchanging data. The duration of this connection is often shorter than the full message exchange that is needed to complete the service. Then the service requires asynchronous communication to complete.

Abbreviations

AIS	Automatic Identification System
API	Application Program Interface
ASM	Application-specific messages
CG	Correspondence Group
CMDS	Common Maritime Data Structure
DMZ	Demilitarized Zone (between firewalls in a network).
DSC	Digital Selective Calling
DSCA	Digital Container Shipping Alliance
EDI	Electronic Data Interchange
EGDH	Expert Group on Data Harmonization (sub-group of IMO FAL Committee)
EPIRB	Emergency Position Indicator Radio Beacon
FAL	Facilitation Committee in IMO
FTP	Internet file transfer protocol, secure version as SFTP
GEO	Geostationary Equatorial Orbit (satellite)
GMDSS	Global Maritime Distress Safety System
GNSS	Global Navigation Satellite System
HF	High Frequency (Short wave radio)
HTTP	Internet hypertext transfer protocol, secure version as HTTPS [2]
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
IOT	Internet of Things
IP	Internet Protocol
IPV6	IP version 6 (most network today are IPV4)
IRDM	IMO Reference Data Model (aka IMO Compendium)
ISM	Instrumentation, Scientific and Medical (open frequency bands)
ISO	International Organization for Standardization
IT	Information Technology
ITS	Intelligent Transport System

JSON	JavaScript Object Notation
kbps	Kilobits per second
LRIT	Long Range Identification and Tracking
LTE	Long Term Evolution
M2M	Machine-to-machine, automated data exchanges between computers
Mbps	Megabits per second
MF	Medium frequency (medium wave radio)
MIG	Message Implementation Guide
MIRA	Maritime ICT Reference Architecture
MMT-RDM	UNECE Multi-Modal Transport Reference Data Model
MQTT	Message Queuing Telemetry Transport
MRS	Mandatory Reporting System, where ships need to report entry and exit [6], see MSR
ms	Milli-second
MSC	Maritime Safety Committee in IMO
MSR	Mandatory Ship Reporting (as described in [6]). Part of this is MRS.
MSW	Maritime Single Window
NAVDAT	Higher bandwidth variant of NAVTEX
NAVTEX	"Navigational Telex" on MF or HF frequency bands. Low bandwidth messaging service.
OPC UA	Open Process Control Unified Architecture
OT	Operations Technology
PEPPOL	Pan-European Public Procurement On-Line
PCS	Port Community System
PKI	Public Key Infrastructure
QoS	Quality of Service (of communication links)
S-100	The new hydrographic system for description of electronic chart s and overlays
SDO	Standards Development Organizations
SIP	Strategic Implementation Plan (of e-navigation [10])
SMB	Server Message Block (protocol for shared access to files)
SOAP	Simple Object Access Protocol (serialized XML).
SOLAS	IMO Convention on Safety of Life at Sea
SSAS	Ship Security Alert System
SSL	Secure Socket Layer (depreciated in 2015 [5]).

TLS	Transport Layer Security [4].
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.
VDE	VHF data exchange
VDES	VHF Data Exchange System
VHF	Very High Frequency – for ships this is approximately 156 MHz to 174 MHz
VPN	Virtual Private Network
VSAT	Very Small Aperture Terminals (satellite system)
VTS	Vessel Traffic Services
WCO	World Customs Organization
XML	Extensible Markup Language
XSD	XML Schema Definition – defining syntax of XML messages

1 Introduction

1.1 Scope

ISTS Report R3.2 gives an overview of standards for general digital communication between ships and between ship and shore. The main subject is digital communication over internet protocols, but a brief description will also be given of other communication systems that are important in the maritime sector. Some of this communication goes over more generic carriers, such as AIS and the newer VHF Data Exchange Service (VDES).

Most of digital communication to and from ships go over wireless links, e.g. satellite and mobile data, and an overview of some of the possible problems with the wireless communication carrier is included.

The most relevant internet-based transport protocols and related data models will be described. General communication over the internet may also open the ship up for cyber-attacks. Thus, this issue is also discussed.

ISTS Report R3.1 [7] gave a similar overview of onboard communication standards.

1.2 Architecture, protocols and data models

This report will provide some insight into data models, protocols and an ICT architecture for ship-centric communication. The descriptions are based on a framework ICT architecture pattern as shown in Figure 1 [7], where the main components are:

- *Roles and functions*: Who are the parties to communication and what roles do they play.
- *Physical topology*: This is the actual physical architecture that represent the "typical" way data networks are used in ship communication.
- *Protocols and standards*: The protocols, i.e. the information transfer mechanisms that are used when communicating with the ship.
- *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.
- *Safety and security*: Measures to safeguard the exchange of correct information against effects of technical faults or malicious acts.

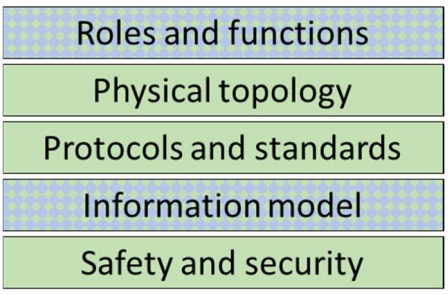

Figure 1 – The ICT architecture pattern [7]

The main subject in this report is the green areas: Physical topology, protocols and standards, and cyber security. Note that data models and protocols are sometimes integrated. This will be discussed in the relevant sections.

1.3 Structure of this report

The sections of this report are organized as follows:

1. This is the introduction and general overview to this document.
2. This section gives some basics about general communication concepts used in other parts of the report.
3. This section will go through some of the most common negative effects of wireless communication and provide an overview of how this affects ship communication for the main data carriers.
4. An overview of how one typically sets up communication facilities for ships.
5. This section provides brief descriptions on non-internet communication systems that are used by ships.
6. Similarly, an overview of systems that do support internet protocols.
7. An overview of different IMO documents that discuss communication to and from ships.
8. An overview of common protocols standards for communication with ships.
9. An overview of data models that are used by the protocols discussed in section 8.

The last section contains number references. References in the text is a number in square brackets, e.g. [1].

2 Some communication basics

This section defines some communication concepts that will be used elsewhere in the report.

2.1 Briefly on radiocommunication frequencies

Traditional radio communication frequencies are normally referred to with the following names:

- **Low Frequency (LF):** This is also called long wave and resides in the band 30 kHz to 300 kHz.
- **Medium Frequency (MF):** This is also called medium wave and resides in the band 300 kHz to 3 MHz.
- **High frequency (HF):** This is also called short wave and resides in band 3 to 30 MHz.
- **Very High Frequency (VHF):** This is the common radiotelephone frequencies in the band 30 to 300 MHz. Maritime radio uses several 25 kHz channels in the frequency range 155 to 165 MHz for VHF radio telephone, AIS and VDES.

Satellite and general terrestrial radio systems such as 4G and 5G use frequencies in the UHF band (Ultra High Frequency – 300 MHz to 3 GHz) and higher. Here, the bands have got letter-designations as follows:

- **L-band:** 1 to 2 GHz
- **S-band:** 2 to 4 GHz
- **C-band:** 4 to 8 GHz
- **X-band:** 8 to 12 GHz
- **K_u-band:** 12 to 18 GHz (K under)
- **K-band:** 18 to 26.5 GHz
- **K_a-band:** 26.5 to 40 GHz (K above)

Some new systems use even higher frequencies, but these are not yet common in civilian applications.

Most of these frequencies are licenced, i.e. you need a national permit to use equipment operating in these bands. Other frequencies are designated as “ISM” (Instrumentation, Scientific and Medical). Within certain power limits, these bands can be used freely. Communication protocols such as Bluetooth and WiFi use ISM frequencies.

2.2 Transport and application protocols

In the protocol world, the Open Systems Interconnect (OSI) model is much used. It is shown to the left in Figure 2 together with a simplified view that will be used in this report. We will not go into details on the OSI layers, but briefly explain the right-most part:

- **Transport protocol:** This takes care of moving bits and bytes between sender and receiver in a network. A typical transport protocol is TCP/IP which is used, e.g. as the transport layer in HTTP for web browsing.

- **Application protocol:** This is the protocol that implements the basic mechanisms of the application program interface, including message formatting, payload rules, digital signatures etc. A typical example is HTTP or HTTPS which allows web browsers to read complex information from web servers.
- **API data content:** The API requires both a transport protocol and some data content. The data content may, e.g. be defined in product specifications (S-100, see section 7.1.3) or as a separate data model (ISO 28005, see section 9.3).
- **Orchestration:** Finally, one also needs to define the sequence of API calls that are necessary to implement a service. This may be just a single call, but often it is a longer sequence of requests, acknowledgements, and a final service request status.

Companion standard/MIG: These are documentation that explain how the application protocol shall be used to implement a specific function. This is typically in terms of API data content and orchestration.

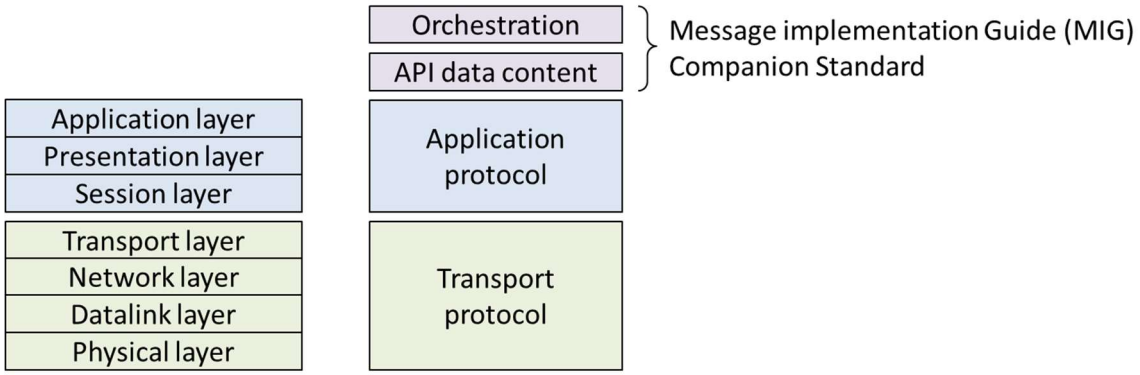

Figure 2 - OSI model and simplified representation

The divisions between layers are often a bit vague as different functions can be implemented in different layers. Most application protocols that are described in section 8 use HTTPS as a transport protocol by adding additional rules to how these protocols shall be used in a specific context.

2.3 Quality of Service – QoS

The quality of service (QoS) of a communication link is the overall performance of the communication link. Some important parameters for ship-related communication are:

- **Latency**: The delay inherent in the transmission of data. As an example, geostationary satellites will have a round trip delay of minimum 0.6 seconds.
- **Bandwidth**: How much data that can be delivered per time unit. This is measured, e.g. in kilobits per second (kbps) or megabits per second (Mbps). High quality video transfers will normally require several Mbps. Voice transmission may manage with as little as 8 kbps.
- **Reliability**: How likely it is that the communication is lost for shorter or longer periods. As described in section 3 there are many issues that may cause communication to fail.
- **Bit error rate**: How likely it is that data is corrupted when received. This is normally not an issue for modern communication systems as the system itself will correct errors.

However, even in this case, high bit error rates on the physical transmission will decrease effective bandwidth.

Different services may require different QoS. The exact requirements to QoS will depend on the applications that are using the communication link.

2.4 Streamed data, API or document type interfaces

Some of the communication between ships and between ships and shore parties will be voice communication over VHF. Other communication, as described in section 5, will be digital, but over dedicated wireless channels. This report will mainly focus on digital communication that uses internet protocols, and the carriers discussed in section 6. Currently most of this communication is as delimited messages that are either transmitted by EDI type interfaces or by API interfaces. These will be discussed below.

2.4.1 Streamed data

It is possible to transfer data continuously in a byte-stream, but this is less common in information exchanges that send and receive delimited units of information packages. However, continuous remote monitoring and control of ships may require this type of protocol. One example of a proposed stream-oriented protocol is described in section 8.3.3.

2.4.2 Document type interface

Ship reporting and some other forms of information exchange has for some years now been done with electronic data interchange (EDI). This is characterized by single and relatively large information packages that contain a complete data set to execute some remote service. The information package can be compared to a complete document and in this document, the term document type interfaces is used.

This has been prevalent in trades with complex cargos like containers and to some degree RORO and passenger ships. EDI has traditionally used UN/EDIFACT, sometimes XML or other types of files that have been exchanged with e-mails, FTP or other semi-manual methods. The use of document style file formats has made it difficult to create automated and more flexible interfaces directly between computers.

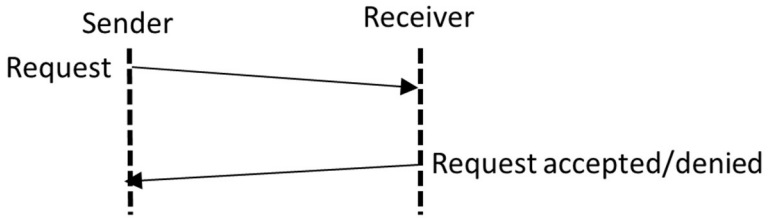

Figure 3 – EDI message sequence diagram

An example of a typical document type exchange is shown in Figure 3. The sender sends a message to a receiver and after some time gets a message back saying if the content was accepted or rejected. This is typically used to, e.g. send an arrival notification or requesting some port service. It assumes that the initial request contains all necessary information and that there is no need of other interactions between the sender and receiver. This normally require a human

to coordinate and check the message exchanges. This makes it more complicated to implement fully automated machine-to-machine communication.

2.4.3 API

An example of an API type exchange is shown in Figure 4. This particular exchange is based on the principles defined in the FAL circular on Guidelines on Authentication, Integrity and Confidentiality in Information Exchanges [13]. An API type exchange can be as simple as in Figure 3, where the top two arrows with a service request status will be the same as the exchange shown in Figure 3, but normally API exchanges are more complex.

One characteristic of an API type exchange is that it is more flexible as each arrowhead in Figure 4 can be a separate API. An API is defined by the application protocol used together with the data set transferred. Even with the same application protocol, one can easily define different APIs by changing the data set transferred. This allows the system to, e.g. send different portions of the required data at different times, possibly after feedback on what information is missing.

Another characteristic is that the sender will get an immediate response on the request, even if the request is not completely processed, as shown in the figure. The response may be an acknowledgement that the request was received, but it can also provide an immediate acceptance or reject of the response.

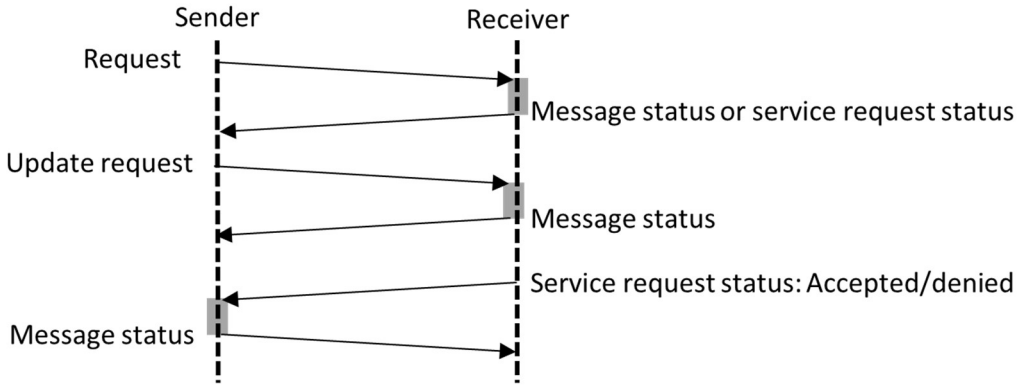

Figure 4 – An API type message sequence diagram

These two characteristics make it easier to implement M2M data exchanges, although one will also need mechanisms to ensure authentication of sender, integrity of information and confidentially.

2.4.4 API session and session context concepts

Figure 10 shows a typical nesting of API calls taken from the new ISO edition 2 of 28005-1 [35].

To the right is a single API call, here shown as one *HTTP session*. This requires one HTTP client and one server and does not allow asynchronous returns of status updates. For this, the sender and receiver must change roles and become respectively a HTTP server and client. This is shown in the middle diagram where a full exchange of messages related to a service status, i.e. a *session*, is shown. The name of the parties has been changed to sender (service requester) and receiver (service provider), and each will be either a client or server, dependent on the direction of the arrows and the placement of the arrow in the orchestration.

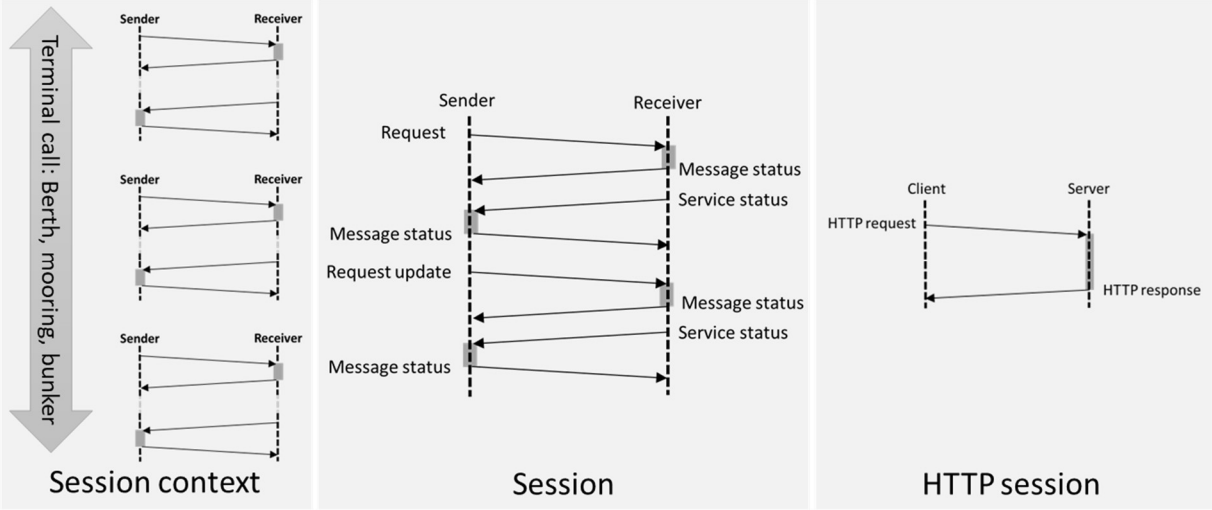

Figure 5 – Different session layers

An API type connection may also need to support more than one session at a time. This may be the case, e.g. for just in time agreements where the ship may need to agree planned arrival times with one or more terminals as well as with the port authorities. Each of the exchanges with a terminal and the port authorities will be one session, but it may be necessary to coordinate these sessions internally in the port by defining an overarching *session context* as shown to the left. The session context may also need be hierarchically nested if one must keep track of several terminals calls in the same port call or several port calls in one visit in territorial waters.

2.5 Representational state transfer: REST

This is a common design principle for the world wide web that defines best practices for using the different HTTP communication mechanisms to achieve stateless and robust web applications. However, APIs as described above, do not really lend themselves to the REST principles as there may be external processes and state changes in addition to the web transactions, e.g. as in ordering ship supplies or tugs. Also, most of the maritime APIs assume a strong coupling between the user and provider of services, which is also not in line with the REST principles.

Thus, while many of the REST principles are useful also in the design of APIs in the maritime sector, most implementations are not really REST compliant. However, they are often called REST APIs because they use some of the same protocol conventions as defined by REST.

3 Common problem with wireless communication

Communication between ships and between ship and shore is most often done over wireless connections, either via direct line of sight data links or via satellite. Even with wired communication, there are issues that can hinder communication, e.g. problems with the communication infrastructure or in the different services one tries to connect to. Limitations in available bandwidth may likewise be an issue in wired networks. See section 3.1 for a brief discussion on some of the general problems that are often overlooked when designing distributed systems.

One problem with wireless communication is that it must share the medium (the "ether") with many other users in a limited useful spectrum of radio frequencies. Other problems are related to limitations in signal strengths and losses in signal propagation. Thus, wireless communication has some of the same problems as wired communication but will be more restricted by limitations in the physical properties or the design of the system. Sections 3.2 and onwards will go through some of these issues and briefly describe possible impact on different wireless communication services.

3.1 The fallacies of distributed computing

A well-known list of "fallacies of distributed computing" has been formulated by Peter Deutsch, and later amended by James Gosling [8]. This represents common misconceptions held by designers of distributed systems that do not sufficiently understand the limitations of physical data networks. The seven fallacies are:

1. The network is reliable.
2. Latency is zero.
3. Bandwidth is infinite.
4. The network is secure.
5. Topology does not change.
6. There is one administrator.
7. Transport cost is zero.
8. The network is homogeneous.

Distributed systems are all systems that include transmission of information over a network, i.e. all systems and operations related to ship to ship and ship to shore communication. This includes wired as well as wireless systems.

3.2 Transmission delay to GEO satellites

Geostationary Equatorial Orbit (GEO) satellites are commonly used in ship to shore communication. These are often called VSAT (Very Small Aperture Terminal) systems as they normally require a stabilised and highly directional dish antenna to get sufficient signal strength.

GEO satellites have an orbital hight of about 35 000 km above the Earth's equator. The distance means that the total distance from ship to satellite and back to an Earth station approaches 100

000 km, or one third of a light second. Practical experiments have shown an expected value of ca. 0.7 to 1.5 second on roundtrip data exchanges in the far north [17]. The minimum possible roundtrip time is about 0.6 second. This gives a noticeable latency, e.g. in telephone conversations over GEO satellites. It will also cause problems for certain digital exchanges that require rapid responses, such as video based remote control of fast moving equipment.

The transmission delay also causes problems when there are high bit-error rates in high bandwidth transmission. Protocols like TCP/IP, that is commonly used in emails, file transfers and web access, will resend data if an error is reported from the receiver. As it can take minimum 0.6 second before an error can be reported, all data transmitted in this period will in principle have to be retransmitted. This means 600 kilobytes for a 1Mbps data link. However, most modern satellite systems have mechanisms in place to minimize this problem, for instance by transmission data redundancy, early data check at satellite or Earth terminal, and/or resending only the bad data.

3.3 Antenna direction

Wireless communication is dependent on good antennas for optimal gain in the sent and received signal. Directional antennas give higher gain at the cost of a smaller sector of useful signal transmission and reception. This is used in VSAT systems where a automatically stabilized and highly directional dish antenna is used to get sufficient gain. However, on a ship that moves, this can give connection problems, e.g. in bad weather as ship movements may be faster than what the antenna can compensate for. Similar problems also occur with non-stabilized directional antennas.

3.4 Shadow effects

Wireless communication generally relies on line-of-sight between sender and receiver. There are some exceptions, e.g. short and medium wave radio transmissions that can use reflections from the ionosphere for transmitting data over longer distances, mobile data coverage may benefit from reflections between buildings in cities, and certain other electromagnetic effects can extend radio coverage somewhat beyond direct line-of-sight.

The requirement for unobstructed communication has some important effects for satellite communication. One issue is that GEO satellites limit their services to below around 60-80° north and south as the satellite disappears behind the horizon beyond these limits. This limit will depend on the difference in longitude between satellite and ship. Satellites may also be obstructed by mountains in narrow fjords or by buildings and infrastructure in ports.

Shadow effects also apply to earth-bound radio communication, although reflections may reduce the problem in many cases.

3.5 Limited coverage

Most satellite systems will also have limited coverage of the Earth surface. This is usually a commercial consideration where operators point the satellite antennas to areas with the most customers. This also have the effect that the signal strength is reduced towards these area limits, and this can give rise to intermittent connection losses or reduced bandwidth.

"Real-time" satellite communication also depends on continuous connection between the ship, the satellite, and an Earth station that can transfer the radio signal onto the general internet or other land line connections. This is not a problem for GEO as they are stationary relative to the Earth surface, but other systems will only work when they can see both the mobile unit and an Earth station.

Some LEO systems, e.g. Iridium, OneWeb and Starlink, overcome this problem by putting enough satellites into orbit to completely cover the Earth. These systems use complex inter-satellite communication links to transfer signals to the satellites that are in sight of one of the Earth stations. However, this may introduce latency and complexity that may have effects on reliability and quality of service [17].

Direct radio communication like VHF and mobile data will also be limited to line-of-sight. However, mobile data will in addition have a designed-in range-limitation to increase the number of base stations and by that the total offered bandwidth in highly populated areas ("micro-cells"). In sparsely populated areas the cell sizes are much larger, but this limits the total available bandwidth in the cell as well as the capacity of each established data link. The latter is related to the frequencies used for longer distance communication and the higher required signal to noise ratio when distances get longer.

3.6 Rain fade

High frequency signals, typically above 11 GHz, as is commonly used in modern communication systems, may also encounter "rain fade". This is losses related to absorption of high frequency electromagnetic signals by water. This is normally not a big problem but can cause outages in severe cases. This particularly applies in the outskirts of coverage areas, where the signal strength is lower.

3.7 Availability and cost of bandwidth

Both satellite services and mobile data operators have a physically limited total bandwidth available in each area they cover and by each frequency band they use. This bandwidth is shared between all users in the coverage area. This means that minimum bandwidth cannot be guaranteed unless the communication technology allows bandwidth reservation. Reservation will normally require that a premium is paid to the operator.

Normally, one will also have to pay a higher price to get a higher maximum bandwidth or data volume. This makes many ship operators limit the available bandwidth to save money.

3.8 Asymmetric bandwidth for send versus receive data

Traditionally, data links via many wireless (and wired) systems have been asymmetric with regards to bandwidth. This is because most users of communication pulled much more data from the internet than they pushed. Web browsing, use of social media and video or sound streaming follow this model.

With the advent of more digitalization of ship operations, this picture is still generally true. One expects that less data is sent from the ship than what is received. However, for remote control and monitoring, where large sensor data sets are being sent from the ship, this may change.

It is necessary to verify the actual available bandwidth available both on the sending and receiving side if this is a critical issue.

3.9 Jamming, spoofing and interception

All data networks are susceptible to direct cyber-attacks, e.g. by gaining physical access to network infrastructure. However, as wireless communication uses radio signals, this gives attackers additional targets.

Radio communication will always have signal strength limitations, and this also defines a necessary minimum signal to noise (S/N) ratio for a given bandwidth of digital transmissions. Higher bandwidth in the same frequency band will have a lower S/N ratio than lower bandwidths and will be more susceptible to interference. Long distances, e.g. to GEO satellites also means that signal strength is very low. In turn, this means that jamming of a radio signal is a relatively low-cost attack on the communicating systems. Jamming is basically to introduce “random” and foreign signals in the same frequency band as used by a certain service. Jamming is more difficult to do with directional antennas as they will protect the receiver from the foreign signals. Jamming have also another limitation as attack form, in that it is easy for the attacked to detect signal noise or disturbances and introduce fallback routines in the system that is using the communication facility.

Spoofing is like jamming, but here the attacker attempts to introduce a stronger signal with non-random and falsified information, and by that make the receiver believe that the false data came from the expected sender. Spoofing is much more serious than jamming as it may be able to introduce false information without the receiver noticing it.

One should also keep in mind that it is easy to intercept satellite communication, and that transmission security may be of varying quality. One should use encrypted or otherwise protected communication methods when sending information over satellite links.

4 An overview of a ship-centric communication architecture

Ships are already dependent on communication with many entities on shore, but traditionally this has been with voice communication and relatively low complexity non-voice communication, such as fax or emails. This will continue to be the case for many ships, but there is also a strong drive towards digitalization and automation of these interfaces. This section will give an overview of the parties that the ship communicates with.

4.1 Ship communication parties

There are many parties that the ship needs to communicate with during operations. However, as will be discussed in section 4.3, the actual communication may not be done by the ship itself, but by a ship representatives, such as agent, manager, or charterer. This is illustrated in Figure 6 where the ship and its representatives act as a hub in the communication with other parties, i.e. a ship-centric communication architecture.

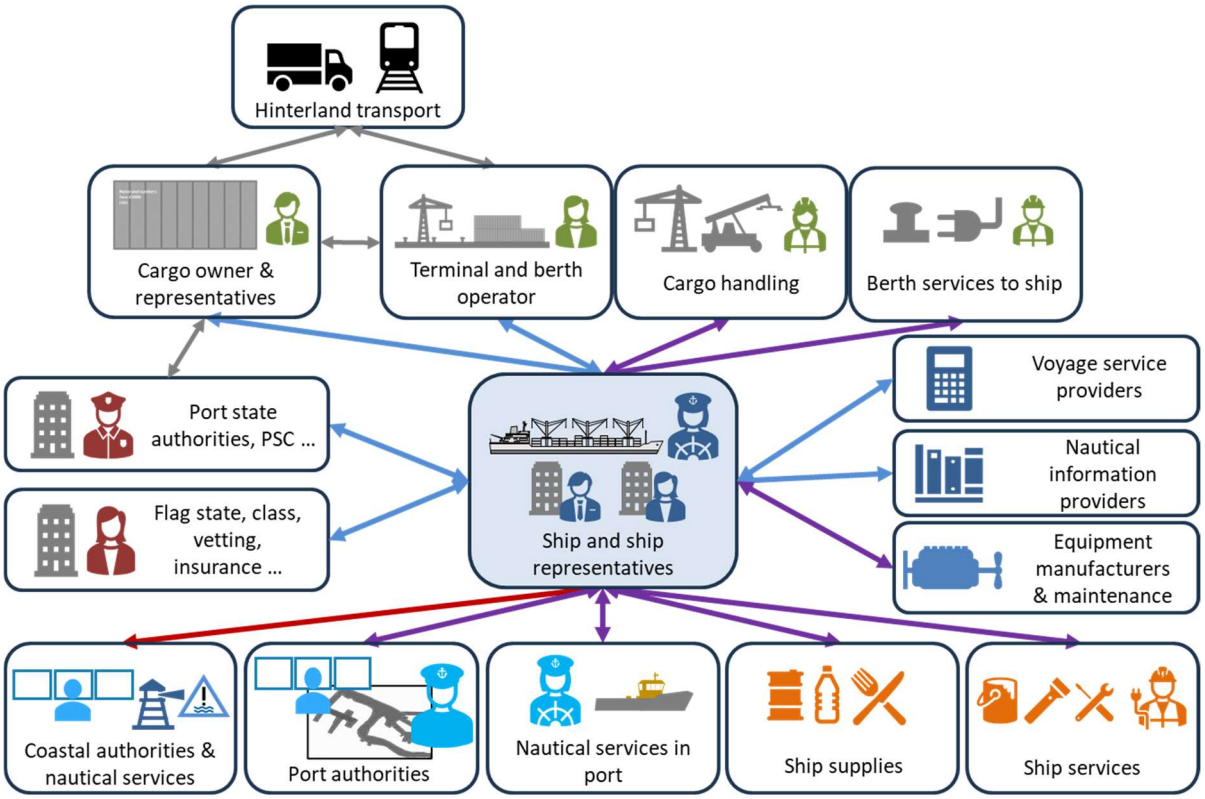

Figure 6 – Parties communicating with the ship or its representatives

This is not an exhaustive picture, but it contains the parties that most commonly are involved in communication with the ship. Hinterland transport has been added to the figure to show the importance of this part of the transport chain, although the ship is rarely communicating with those parties directly. The AUTOSHIP project made a relatively detailed breakdown of ship processes related to analysis of autonomous ship operations [9] that, if desired, can be used to give more details to this picture.

The blue arrows show communication that is mainly related to planning and exchange of information before or after a specific operation, such as a port call. Red arrows show communication that is directly linked to the execution of operations, while purple arrows show

exchanges that contain both these types. The thinner grey arrows show some of the communication that the ship does not take part in. The figure does not include direct ship to ship communications such as VHF radio or AIS transmissions.

The following paragraphs will give a brief overview of the illustrated parties.

Cargo owner and representatives: This is a party that has a decisive say on how cargo shall be handled or transported. This may include the actual cargo owner, a charterer, freight forwarder or other similar party. Communication between ship and cargo owner may include details of cargo, stowage requirements, dangerous cargo, agreement on loading and discharge times etc. This is normally related to the planning of a voyage or port call.

Terminal and berth operators: This is a party that can agree on berthing and de-berthing times for the ship. They may also handle coordination with other parties operating in the terminal or berth area. Communication between ship and terminal operators may be ship and cargo type, arrival and departure times, draught, air-draught and other information necessary to plan utilization of berths.

Cargo handling: This is a party that takes part in cargo loading or unloading. This is typically crane operators, or personnel operating hoses, pipelines and tanks. Communication is mainly operational but may also include planning if this is not handled through the terminal operator.

Berth services to ship: This is like cargo handling, but involves mooring and other services that is necessary for the ship's stay, e.g. providing gangways, cold ironing etc. Communication is mainly operational but may also include planning if this is not handled through the terminal operator.

Voyage service providers: This is a party that aids in voyage planning by providing weather forecasts, voyage optimization or similar services.

Nautical information providers: This is a party that supplies the ship and its captain with necessary nautical information, such as charts, notices to mariners, and similar information. One may also be able to get more detailed information about ports and port infrastructure from these sources.

Equipment manufacturers and maintenance: It is becoming more common to let manufacturers supervise parts of the equipment onboard to do health and efficiency analysis and to provide decision support in case of problems. This requires that information about the equipment is transmitted to shore. Shore parties may also have possibilities for real-time error and health checking of ship equipment.

Ship services and ship supplies: Ships will often order various maintenance services when in port and may also procure new supplies, such as food, fresh water, lubrication oil or bunkers. Services and supplies must be ordered, and delivery must be coordinated.

Nautical services in port: Port calls may require nautical services such as pilots or tugs. Services must be ordered and will also require communication during execution.

Port authorities: Port authorities and the port VTS must be contacted to get approval for terminal approach. The port authorities will also normally require a notification, e.g. 12 or 24 hours before port arrival.

Coastal authorities and nautical services: The coast state authorities maintain aids to navigation and sends out maritime safety information. They may also operate VTS or mandatory ship reporting areas that require reporting from passing ships.

Flag state, class, vetting and other international parties: Various certification authorities like flag state, recognized organizations, class and vetting organizations may need to communicate to keep certificates or permissions up to date or to plan inspections during port calls.

Port state authorities and port state control: The port state authorities will require arrival and departure reporting, including waste delivery, stowaways – if relevant, and other information that is needed in conjunction with a foreign port call. Port state control may also need access to ship certificates and other information. There may also be veterinary or phytosanitary authorities that requires information about cargo and permits to import or export.

4.2 A functional view

Several of the parties described in the previous subsection are involved in the same ship processes, so it may be useful to include a functional view in the architecture. Table 1 proposes a functional grouping, with some examples of applications or parties. The column named "TP" specifies if the communication mainly is over internet (IP) or over VHF or other real-time channels ("VR"). These corresponds to respectively the red and blue arrows in Figure 6.

Table 1 – Proposed functional grouping

Group	Name	Examples	TP
1	Crew and passengers	Infotainment, call home, remote training	IP
2	General navigation	VTS, MAR, MSI, weather, other ships	VR
3	Port and channel navigation	Tugs, linesmen, pilot, port authorities, terminal	VR
4	Berth operations	Linesmen, mooring, cold ironing, gangway	VR
5	Cargo operations	Cranes, pumps, lashing, RORO, ballasting	VR
6	Incident management	SAR, lost cargo, pollution, onboard incidents	VR/IP
7	Voyage management	Voyage orders, planning, optimization, reports	IP
8	Port call management	Order berth, JIT, port arrival, notice of readiness	IP
9	Ship administration	Crew, consumables, supplies	IP
10	Technical management	Maintenance, technical condition, cyber security	IP
11	Environmental performance	Fuel use, distance and speed, waste, ballast water	IP
12	National authority reporting	Ship clearance for port call, ISPS	IP
13	Certificates and safety management	Flag, crew, class, insurance, vetting, ISM	IP

This list is a compilation based on the functional decomposition in the AUTOSHIP D3.1 [9] report with some updates based on the e-navigation specifications as described in the strategic implementation plan [10]. The following subsections give a brief description of each group.

Crew and passengers: This is general and public use of social media, e-mail and web browsing. Some special applications using internet protocols may be used.

General navigation: This is communication to or from ship bridge during voyage execution. This is mainly VHF voice or other special carriers as described in section 5. It may include some parts of mandatory ship reporting (MSR)

Port and channel navigation: This is like the previous group but related to different support functions in the port. Today this is mainly voice over VHF, but VDES may play a more important role in the future.

Berth operations: Again, like the previous group, but in the future one will probably also see dedicated real-time control protocols for charging, mooring and other equipment. Some uses of such protocols are already in place, but normally as proprietary solutions and typically in the ISM bands.

Cargo operations: Like previous groups, but with cargo handling as focus. This may involve bulk loading and discharge, containers including lashing and unlashing, liquid bulk, RORO or breakbulk.

Incident management: This is special at-sea communication related to emergencies or incidents on own or other ships. This may be lost cargo including danger of pollutions, man overboard, ships in distress etc. Mainly this is handled by voice communication but there are also reporting requirements to nearest coast state, e.g. for cargo losses, and it is likely that more communication to rescue coordination centres (MRCC) also may become digitalized.

Voyage management: These are activities related to voyage planning and replanning. This may include voyage orders, voyage optimization, noon at sea reports and other similar functions that may make use of communication to shore parties.

Port call management: This is like the previous function but related to port call planning and management. This may include sending arrival notices, berth requests, just in time negotiations and similar messages.

Ship administration: Activities and reports related to management of the ship, e.g. crew wages and replacements, ordering supplies and consumables, arranging crew pickup in ports etc.

Technical management: Activities related to management and maintenance of technical systems onboard. This may include engines, cargo handling, safety systems, ICT systems and more. Today, ships are increasingly sending automated measurement reports to shore for remote maintenance monitoring. In the future one will also increasingly have to consider the cyber-security of onboard ICT systems in this context.

Environmental performance: Increasing reporting requirements on environmental performance from public and private parties goes into this group. This may include emissions from ship, fuel and energy use, voyage performance, ballast water exchanges etc.

National authority reporting: This is mainly the obligations in the FAL Convention and is related to calls in foreign ports. This includes customs, immigration, security, veterinary, and phytosanitary reporting requirements to ship, crew and cargo.

Certificates and safety management: The ship and its master need to keep all ship certificates and other documentation up to date. This includes flag state certificates, crew certificates,

various class certificates, vetting documentation, insurance, safety management documentation, logbooks and more.

4.3 Ship and ship representatives

The ship can participate itself in communication with shore parties but may also delegate this communication to other parties. Figure 7 shows the most relevant parties that can represent the ship. In addition to the parties' links to the ship (blue) these parties will also need to communicate between themselves (green) to provide a coordinated communication with external parties.

The ship representatives are:

1. **Ship owner:** The owner of the ship as registered on flag state certificates.
2. **Ship manager:** A party that has undertaken to perform some of the management functions for the ship on behalf of another party, normally the owner.
3. **Ship charterer:** A party that has paid for the use of the ship for a certain trip or period.
4. **Ship agent:** A party in the port of call that can represent any of the above within a national legal context.

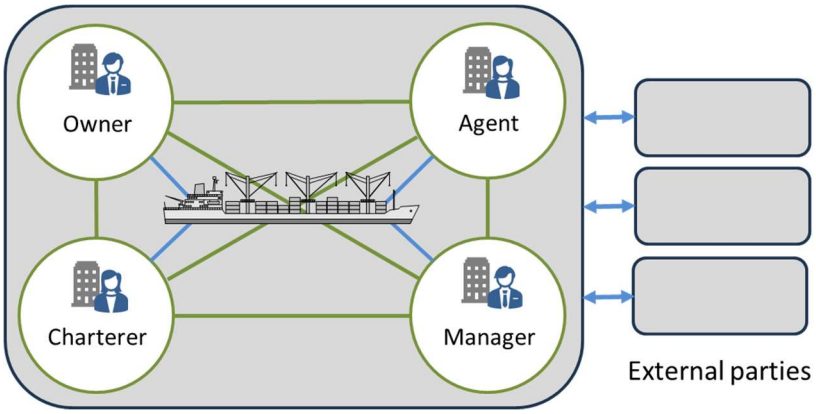

Figure 7 – Ship and ship representatives

Most of the more administrative ship-shore communication can be undertaken by the ship representatives, but exchanges very close to the captain's responsibilities, e.g. VTS or mandatory ship reporting, final just in time arrival arrangements and some issues related to voyage planning may be more effectively performed by the ship and its captain.

4.4 Port data systems

There are several data systems that can be used in conjunction with port calls, and in [14] some of these systems are identified and named. These are illustrated in Figure 8. The systems are:

- **Port Community Systems (PCS)**. If available, this is used as a federating system that can provide incoming information and request to several other systems.
- **Terminal Operating Systems (TOS)**. This is a data system used by terminal and berth operators to manage operations in the terminal, including assignments of berth.
- **VTS Information System (VTIS)**. This data system is used by VTS operators to keep track of ship in the area and relevant information about the ship. It may be connected to the MSW or PMIS.

- **Port Management Information Systems (PMIS)**. This system is used by the port authority to manage operations in port.
- **Maritime Single Window (MSW)**. System for clearance of ships for port calls.

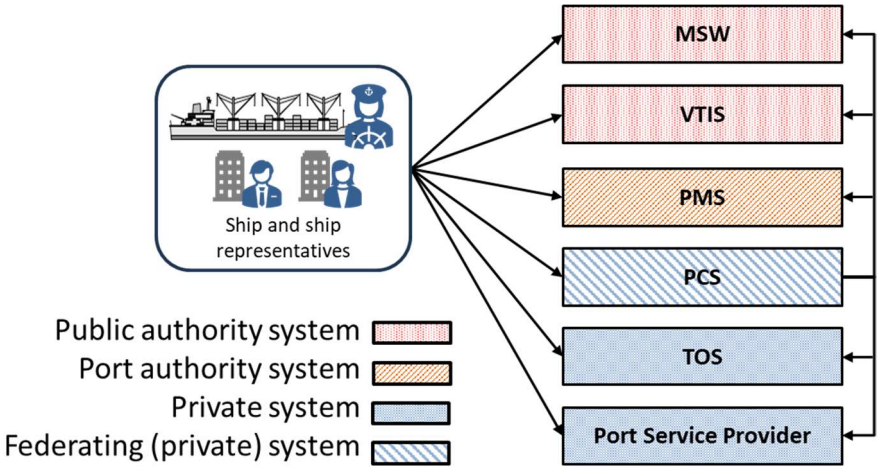

Figure 8 – Definitions of data systems in port

In addition, one will also normally see several data systems operated by different service providers.

5 Communication systems not supporting internet protocols

Ships use several different radiocommunication systems, where many are collected in the group called Global Maritime Distress Safety System (GMDSS). These systems are dedicated to specific functions and will not generally use internet protocols or internet compatible carriers. These systems will briefly be described in section 5.1. A more generic system is the automatic identification system (AIS) and the newer VHF data exchange system (VDES). These are described in section 5.2. The introduction of VDES will also define new requirements for cyber security that are discussed in section 5.4. Section 5.3 discusses some other wireless operational technology data links that are in use today.

Note that some services, VDE (section 5.2.4) in particular, could use internet protocols on top of their specified transport protocol. However, the bandwidth is limited for these services, and it will be much more effective to use dedicated binary transmission formats.

5.1 Some specialised data transmission services

This section briefly describes some common digital services that are used for specific purposes in international shipping. This is not complete as also, e.g. GNSS includes some digital information in their signals.

5.1.1 Digital selective calling

DSC is a digital service that is used, e.g. to automatically place radio calls. It is mainly used on VHF channel 70 but is also available in HF and MF and bands. It has a bandwidth of 1.2 kbps. It is also an important carrier for certain emergency messages.

5.1.2 Emergency Position Indicator Radio Beacon

EPIRB is a system for alerting of and detecting persons in distress. It is also used by aircraft and sometimes by individuals. It can be received by satellites (COSPAS/SARSAT) or by ordinary radio receivers, e.g. as mounted on rescue airplanes or helicopters. It can send a digital message at 0.4 kbps – typically used to send position and other relevant information, but it is also possible to just use the plain radio signal to determine the direction to the sender.

5.1.3 Ship Security Alert System (SSAS)/Long Range Identification and Tracking (LRIT)

SSAS and LRIT are services that are implemented by dedicated satellite short message services, originally on Inmarsat, but now also on Iridium. These are very short messages that are used to send a security alert through SSAS, e.g. for pirate attacks, or a regular position report for tracking ships at sea with LRIT.

5.1.4 NAVTEX, NAVDAT and SafetyNet

NAVTEX is a service in the MF or HF bands with a “narrow band direct printing” service distributing maritime safety information (MSI). These are short text messages sent over a 0.4 kbps data channel. NAVDAT is a NAVTEX replacement service that is still in development that can increase bitrate to up to 30 kbps, but currently referred to as having between 12 and 18 kbps [20]. SafetyNet sends the same MSI information over Inmarsat or Iridium. Iridium calls this service for SafetyCast.

5.1.5 Inmarsat C

Inmarsat C is a satellite communications system primarily used for distress alerting and reception of MSI, including shore-to-ship distress relay messages. It is a two-way store and forward system that can handle data and messages up to 32KB. Inmarsat C is also utilised for other IMO systems such as Ship Security Alerting System (SSAS) and Long-Range Identification and Tracking of ships (LRIT).

5.1.6 Digital HF

The short-wave spectrum is not much used for commercial voice communication anymore and some of the frequency bands have been allocated to, e.g. digital e-mail services such as WINLINK [18]. These have relatively low bandwidth and are sporadically used also for merchant ships.

5.2 AIS and VHF Data Exchange System

The automatic identification system (AIS) is a well-known communication channel for transmission of ship movements between ships and from ship to shore or satellite. It also has facilities for sending more general binary messages, so-called application specific messages (ASM). IALA [19] maintains an unofficial list of such messages. However, the coexistence between ASM and the more conventional AIS messages is becoming a problem as bandwidth is limited in the two AIS channels. Thus, the VHF Data Exchange System (VDES) [20] has been proposed to better support the diverse applications for shorter digital messages between ships and between ship and shore. VDES is not yet a carriage requirement for SOLAS ships, but IMO and IEC have now started work on new performance and test standards. This will in any case be a prerequisite for any carriage requirements.

Figure 9 – VDES VHF channel allocation

VDES will incorporate the existing AIS system as illustrated in Figure 9, but will also implement new higher capacity radio channels as described below. The following sub-sections will give a brief overview of the different components, including existing AIS.

Table 2 – List of some relevant AIS and VDES standards and documents

Standard	Application	Manager	Reference
ITU-R M.1371	Conventional AIS, and ASM message formats	ITU	[21]
ITU-R M.2092-1	VDES and ASM specifications	ITU	[22]
WRC-19	Channel allocation	WRC	[23]
IALA G-1017	Guideline giving an overview of VDES	IALA	[20]

The systems use VHF which typically give a range of between 30 and 120 km, dependent on antenna hights and transmission power. VHF can also be used by Low Earth Orbit (LEO) satellites, which can provide both listening and transmitting services.

Normally, a shore station will coordinate use of the different data links. It is also possible to set up ad-hoc ship-to-ship communication links coordinated locally by the ships themselves.

5.2.1 Automatic identification system – AIS

AIS has already been operational since before 2000 and is a carriage requirement on most ships. VDES proposes to relieve the current capacity problem for the main AIS channels by moving the current application specific messages (ASM) from the AIS channels to dedicated and higher capacity carriers marked as ASM in Figure 9.

The two conventional AIS channels are used for normal ship to ship and ship to shore communication. Long range AIS uses the same message formats but has a lower message repetition rate and is intended for satellite reception. The lower transmission rate reduces the problem that satellites have in that they receive AIS messages from large Earth surface areas, and this increases the probability that AIS transmissions from different ships overlap in time, interfere with each other and decreases signal quality.

AIS bit rate is 9.6 kbps and about half of this is effective bandwidth for payload. Today, ASM as described in section 5.2.3, is sent on the existing AIS channels with the same modulation and bandwidth as AIS messages. When ASM has been moved to the new frequencies (see below), AIS will not be available for ASM messaging.

There are several different conventional AIS message types defined, but the most common are the position message, sent rapidly to give a ships position, heading and speed, and the static message, which provides some static ship parameters such as name, destination, size etc.

5.2.2 Satellite AIS

These are normal AIS channels where message update rates have been reduced to reduce interference and to simplify satellite reception of the signals. Satellite or “long-range” AIS is also in use today.

5.2.3 Application specific messages – ASM

When VDES comes into common use, the ASM messages will be moved to new channels added to VDES (see Figure 9) to relieve the existing AIS channels from ASM messages. They have a more complex modulation, allowing 19.2 kbps raw bandwidth. Data payloads in each message can theoretically be up to 172 bytes, dependent on message type, forward error correction and other parameters.

It is expected that VDES ASM may be more available to general messaging than AIS ASM messages, so it may be interesting for certain control functions. However, one cannot rely on other ships having the possibility to receive and send ASM before the system has been approved by IMO as a carriage requirement. It may be more likely that base stations implement ASM, making it interesting for vessel to do VTS messaging. However, see section 5.4 for a discussion on cyber security issues.

5.2.4 VDE – VHF Data Exchange

VDE is the new "high capacity" component of VDES. It can use up to four 25 kHz channels to achieve up to 307.2 kbps raw bandwidth in a concurrent transmit and receive configuration. Additional VHF channels are allocated, mainly to avoid crosstalk between VDE and other VHF channels. VDE supports three different modulation schemes to also cater for longer distance communication when signal-noise ratios would otherwise make high-capacity communication unreliable. Table 3 shows the different specified variants. For details of modulation scheme, refer to the protocol specification [22].

Table 3 – Raw VDES bitrate (kbps) for different modulations and channel widths [22]

Modulation scheme	25 kHz	50 kHz	100 kHz
MCS-1 (π/4 QPSK)	38.4	76.8	153.6
MCS-2 (8 PSK)	57.6	115.2	230.4
MCS-3 (16 QAM)	76.8	153.6	307.2

Frame formats include various administrative information that will reduce the raw bitrate with up to about 25% in the lower capacity variants. Relative reduction will be smaller for the higher capacities. Forward error correction can further reduce the available bandwidth.

The VDE service can be implemented both as streaming data and as packet data. This depends on the protocol used. However, the total available bandwidth will be shared between all users within listening range of each other.

5.2.5 Satellite services

Both ASM and VDE includes provisions for communication with LEO satellites. The principles are similar as that described in previous sections, but the capacity of the data links will be lower. Long-range AIS is already a dedicated satellite service.

5.3 OT communication in port

With increasing automation in ports, also including support for autonomous ships, there will be an increasing need for digital real-time interfaces between ship and port equipment. There are no relevant standards in this area yet, but some manufacturers have their own proprietary solutions, e.g. based on WiFI or other protocols in the ISM bands. It may also be interesting to look at 5G as a common solution for this, e.g. by using a private 5G network in the port. Some possible applications are briefly outlined below.

Automatic mooring: Mooring systems need to communicate with ship to determine when to activate mooring. Dependent on system, there may also be a need to move mooring with tide or other physical changes.

Cold ironing and charging: Electric batteries become more common and charging systems will be needed in many ports. These will also need to be steered from ship to connect to connectors and to control current. The same applies to shore support of power or "cold ironing".

Cranes: Automated cranes may also need to connect to the ship to control the cargo loading or discharge process. This may be control of cranes on ship or short, with communication to the opposite side.

Local positioning systems: There may also be access to local positioning services, e.g. based on GNSS corrections, radar range finders or other systems. These may also need local communication.

5.4 Cyber security for narrow band radio communication

Most of the systems described in this section have limited protection against cyber-attacks. It is relatively easy to spoof most of the services and the bandwidth in many is too limited to allow, e.g. the inclusion of digital signatures. This may be a manageable problem if messages are intended for human use, where the human operator can do sanity checks on the information or verify the received information by other means.

However, if the communication is used in automated machine-to-machine communication, cyber-attacks become more critical. One known problem is that AIS to some degree is used in automated target tracking, e.g., in cooperation with radar detected targets. As it is easy to spoof AIS, one can introduce false targets in electronic displays used by the navigator, and this can cause problems in limited visibility. However, radar echoes can still be used to verify AIS targets.

The new ASM messages may have space for introduction of digital signatures to verify authenticity and integrity of the received information. An acceptably secure elliptic curve cryptographic signature is 64 bytes long [22] and this could in principle be used for the longer messages.

VDE have sufficient capacity to accept the overhead of introducing digital signatures. Special VDE management (“bulletin board”) messages have already allocated 64 bytes for this purpose.

6 Communication systems supporting internet protocols

This section will briefly describe some of the most common communication systems used in ship to shore communication where the internet protocol is commonly used as transport layer.

6.1 VSAT systems

VSAT is the most common system in use today. It uses a stabilized dish antenna that points to a GEO satellite. The satellite typically has several spotbeam transceivers that can be directed to different areas of the world that is viewable from the satellite. Dependent on the position over Equator, each satellite will typically have a view of about one third of the world, more limited as the view goes north- or southward from Equator. The SATBEAM web site [24] provides a good visualization of the coverage of many of these systems.

Within the spot beam, there is a fixed bandwidth available for all customers. The available bandwidth for each user is normally limited by how much is paid for the subscription. It is not uncommon to have relatively limited bandwidth available onboard, e.g. down to 256 kbps.

6.2 MEO systems

Today there is only one commercial Medium Earth Orbit (MEO) system in operation. This is the O3B (originally called “Other 3 Billion” – referring to people without ordinary internet access) satellite system that can provide low latency and high bandwidth coverage between 50° north and south and more limited service up to 62°. The orbit is around 8000 km above the Earth which gives a significant lower latency than GEO systems. The directional antenna has the added complexity of following the movement of the satellites, but this is not a big problem on a ship that in any case needs a stabilized antenna to track GEO satellites when the ship moves. A lower orbit can also give a better signal strength than GEO.

6.3 LEO systems

There are several systems in Low Earth Orbit, best known is probably Iridium and Starlink. Iridium is an older system with 66 active satellites that operate in L-band. It provides different services, including safety services in the GMDSS service set. It can also provide voice communication over small handsets as well as digital connectivity with the help of special mobile stations and antennas.

Starlink has currently around 4000 satellites that operate in K_a and K_u bands, and currently only provide digital connectivity. Both systems use inter-satellite communication to be less dependent on ground stations. Iridium can provide up to 700 kbps receive and 176 kbps send speeds. Starlink can provide more than 100 Mbps speeds for their users, but there is a subscription determined limit to how much data one can transmit at the guaranteed speeds. As for all other systems, the bandwidth will also have to be shared by subscribers in each coverage area.

A third system, OneWeb, is also in operation. It has around 700 satellites in LEO orbits. It provides a similar service as Starlink. While StarLink sells services directly to users, including the general public, OneWeb is targeting mainly business, governments and similar user groups.

The benefit of LEO systems is low latency and shorter distances between satellite and ground station. However, LEO has some drawbacks, e.g. more space debris and more drag from the thin

atmosphere. This will normally limit the lifetime of the satellites as they need to use fuel to adjust orbits. As many more satellites are used, this will lead to a relatively high rate of replacement of satellites which in turn increases operational costs.

6.4 Mobile data: LTE - 4G - 5G

Mobile data services are referred to as Long Term Evolution (LTE), 4G, or 5G (fourth or fifth generation mobile telephone systems). In principle these terms specify gradual developments towards higher capacities and lower latencies. LTE is not well defined and can mean different things when used by different vendors. Normally, LTE means an extension to 3G technology and has capabilities below that of real 4G.

Mobile data will normally be available in ports and in areas close to the coast where there is a sufficient population density to make a business case for building out the base stations. Communication is normally with low latency and relatively good bandwidth, although these factors vary with the deployed system and how many users are accessing the network. Also, distance to base stations will have an impact as lower signal strengths normally means lower bandwidth as the complexity of modulation has to be reduced.

Starlink (see section 6.3) is doing experiments with direct communication between 5G cell phones and some of the satellites in the system.

6.5 Wireless networks

Some ports may also offer WiFi or WiMax connectivity, although this is probably being superseded by mobile data such as 5G.

6.6 Cyber security for satellite communication

Most satellite communication is relatively easy to jam, listen in on or even spoof. This is probably getting better in more modern systems, but one should make sure that cyber-security measures are taken as needed. This type of attack requires proximity to the ship.

Internet connections as provided by all the services described in this section also potentially opens the ship for cyber-attacks from remote locations. This means that the internet access point on the ship needs to be protected.

7 IMO guidelines on digital information exchange

As this report covers maritime communication to and from ships, it may be useful to give a brief overview of some of the documents that has been published by IMO on this subject. This section will focus on general requirements and guidelines for electronic communication.

One should keep in mind that IMO has a dualistic view on digital and electronic communication that has yet to be fully reconciled. The concept of e-navigation, which is closely related to safety of navigation, is handled by the maritime safety committee (MSC) and its sub-committee on Navigation, Communication, Search and Rescue (NCSR). Most of the development work is undertaken by IALA and IHO in the framework of IHO's S-100 specifications. Other types of more operational communication, including MSW, is handled by the Facilitation Committee (FAL).

Traditionally, these have been separate developments with little coordination. However, as FAL now has established the Expert Group on Data Harmonization (EGDH) that is responsible for the further development of the IMO Compendium, IHO is now working on harmonization of the S-100 data model with the IMO Compendium. It is expected that can be the start of further standardization of the e-navigation developments.

7.1 E-navigation strategic implementation plan (SIP)

The development of the e-navigation concept in MSC led to a strategic implementation plan that was last updated in 2018 [10]. This gives details of the planned development and applications within the e-navigation framework. The SIP has identified five specific e-navigation solutions:

- S1: Improved, harmonized and user-friendly bridge design;
- S2: Means for standardized and automated reporting;
- S3: Improved reliability, resilience and integrity of bridge equipment and navigation information;
- S4: Integration and presentation of available information in graphical displays received via communication equipment; and
- S5: Improved communication of VTS Service Portfolio (not limited to VTS stations).

Of these, it is mainly S2 and some other parts of the other solutions that are relevant for the discussions in this report. This will be discussed in the next sub-section. In addition, the last sub-section will briefly introduce the concept of maritime services.

7.1.1 E-navigation sub-solutions

Table 4 lists some of the sub-solutions within e-navigation that has the most direct relevance to the topics discussed in this report. The "solution" column refers to sub-solution codes in the SIP. The "function" column refers to the function groups in section 4.2.

Table 4 – Sub-solutions of e-navigation solution 2

Solution	Description	Function
S2.1	Single-entry of reportable information in single window solution.	12
S2.3	Automated or semi-automated digital distribution/communication of required reportable information, including both "static" and "dynamic" information.	2, 12

Solution	Description	Function
S2.4	Standardized digital reporting formats based on recognized internationally harmonized standards	CMDS
S4.1.1.	Implement a Common Maritime Data Structure (CMDS) for Maritime Service Portfolios (MSP) and include parameters for priority, source and ownership of information.	CMDS
S5	Improved communication of VTS service portfolio (not limited to VTS stations)	2, 3

The rows marked "CMDS" refers to the "common maritime data structure". Currently, this is implemented in the S-100 framework but there is a need to harmonize that with the IMO Compendium. This issue will be discussed further in section 9.

7.1.2 Maritime services

As part of the improved provision of services to vessels through the identified e-navigation solutions, maritime services have been identified in the SIP as the means of providing electronic information in a harmonized way. The proposed list of Maritime Services is presented in Table 5. The "No" column represents the service number as specified in the SIP and the "function" column refers to the function groups in section 4.2. Note, however, that this mapping is indicative and not necessarily fully correct.

Table 5 – Overview of maritime services

No	Name	Function
1	VTS Information Service (INS)	7
2	Navigational Assistance Service (NAS)	2
3	Traffic Organization Service (TOS)	2, 3
4	Local Port Service (LPS)	2, 3, 8
5	Maritime Safety Information Service (MSI)	2
6	Pilotage service	3
7	Tug service	3
8	Vessel Shore Reporting	12
9	Telemedical Assistance Service (TMAS)	6
10	Maritime Assistance Service (MAS)	7
11	Nautical Chart Service	7
12	Nautical Publications Service	7
13	Ice Navigation Service	2, 7
14	Meteorological Information Service	2, 7
15	Real-time hydrographic and environmental information Service	2
16	Search and Rescue Service	6

A Maritime Service Portfolio (MSP) is a set of operational Maritime Services.

7.1.3 S-100 product specifications and messages

Each of the e-navigation services will eventually be defined as a S-100 product specification. Examples are S-421 for route exchange and S-131 for port infrastructure. Part of the product specification is a data model that represents the information content required to implement the

service. This data model can in turn be converted to messages between service users and providers. The data models and messages will be designed according to the S-100 reference data models that are maintained by IHO (see section 9.2).

7.2 FAL Guidelines on setting up an MSW

FAL.5/Circ.42/Rev.1 [11] gives a general overview of the maritime single window and how it can be designed and put into operation. It does not specify any specific standards to be used but mentions some of those that are available and partly in use. This is the basic guideline underlying much of IMO's work on MSW. One of the figures from the document is redrawn in Figure 10.

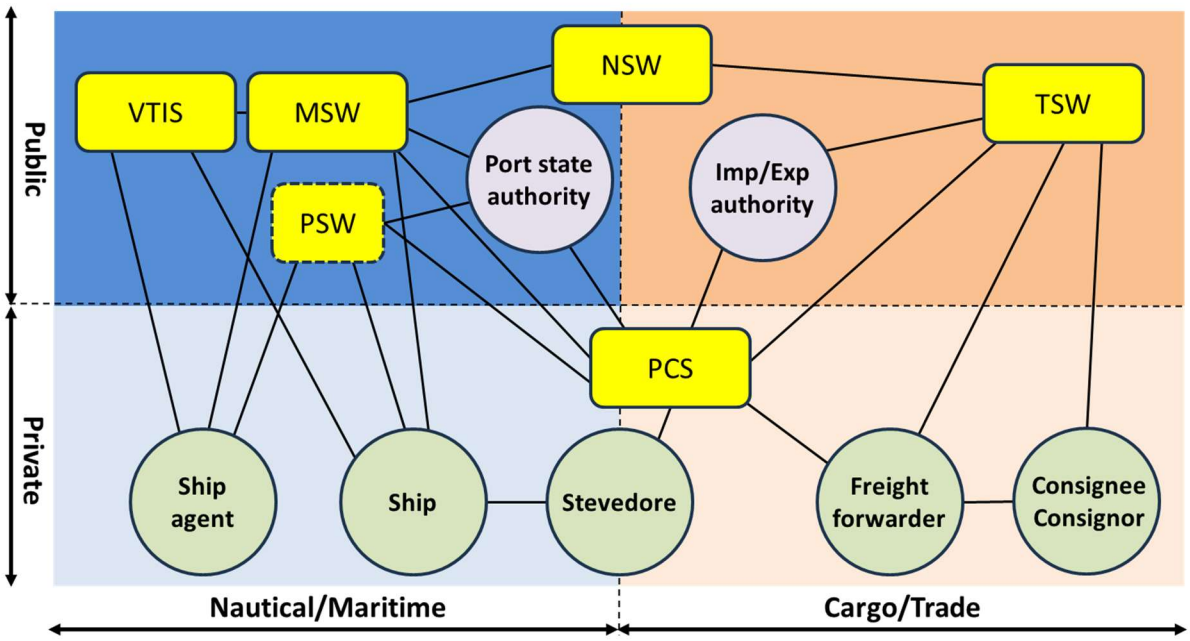

Figure 10 – Different types of communication hubs in ports

This shows some of the same systems as was identified in section 4.4, but puts them into a private/public and maritime/trade grid system. New systems in this figure are PSW (Port Single Window), NSW (National Single Window) and TSW (Trade Single Window). These are reporting portals for a single port, for national reporting requirements, and for trade import and export respectively. The parties in the pink circles are examples of some of the potential operators and back-offices of the systems. Green circles are private users of the systems.

7.3 The IMO Compendium

The IMO Compendium used to be published as a printed guideline that exemplified the digital implementation of an MSW with the help of a set of UN/EDIFACT messages. However, as it became more complicated to maintain the guideline and as it became clear that one also needed to include other standards, e.g. from ISO and WCO into the mapping, the compendium was converted into an on-line reference data model [12].

The IMO Compendium is basically a data reference model that is an agreed-on naming and description of several sets of data objects that have been extracted from various IMO instruments and other data exchange requirements. It is the IMO expert group on data

harmonization (EGDH) that does the definition work which in turn is approved by the IMO FAL committee.

International standards development organizations (SDO) like ISO, WCO and UNECE then make sure that their specific standards are aligned with the definitions in the IMO Compendium and produce a mapping table from the objects in the IMO Compendium to their relevant standards. IHO is also working on a similar process to align their S-100 data model (see section 9.2) with the IMO Compendium. The process is illustrated in Figure 11.

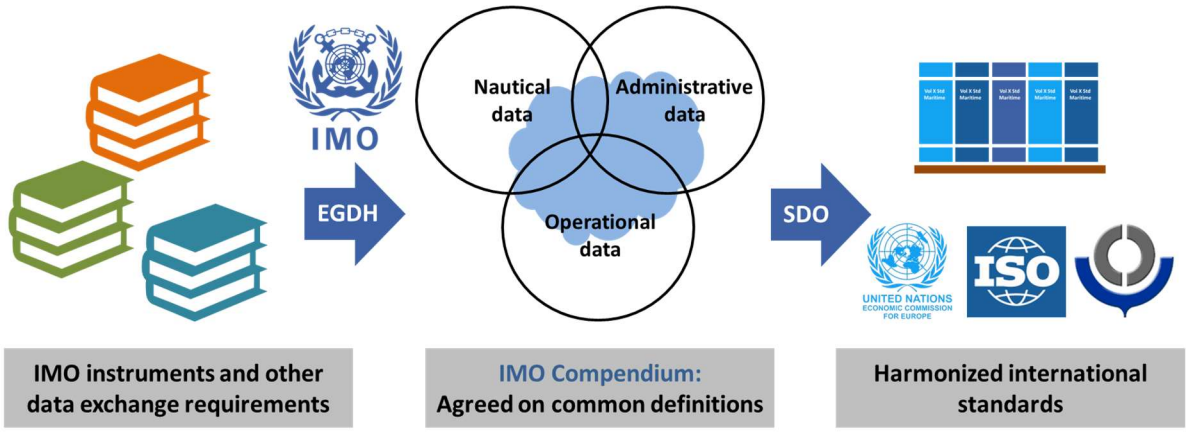

Figure 11 – The principle of the IMO Compendium

This process will ensure a level of interoperability between the standards which allows, e.g. container cargo manifests in UN/EDIFACT to be used in parallel to ISO 28005 XML messages that provides, e.g. pre-arrival messages. The first IMO instrument to be used in this mapping was the FAL convention and its FAL forms, that specifies some of the reporting requirements for the MSW.

The IMO reference data model is discussed in more detail in section 9.1.

7.4 Guidelines on Authentication, Integrity and Confidentiality

IMO FAL.5/Circ.46 [13] provides guidelines on the use of digital signatures in electronic message exchanges. This document also interduces some general concepts for message exchanges using APIs that can be used as reference in standards and specifications. Figure 12 is a redraw of figure 4 in the document that illustrates some of these concepts.

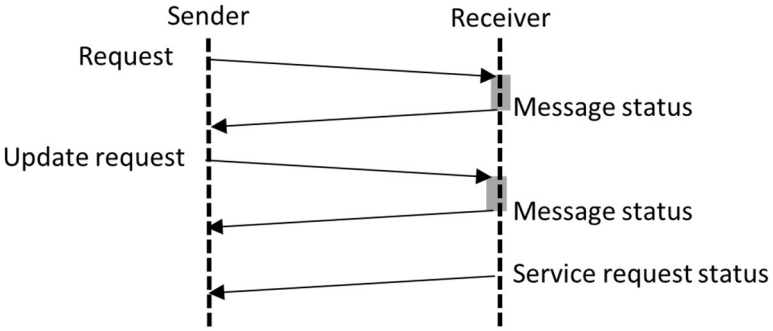

Figure 12 – Some communication concepts from [13]

The main group of definitions are:

1. The terms “sender” and “receiver” to denote service requestor and service responder. This is because communication normally will be asynchronous with service request status messages possibly arriving several hours or even days after the request. This means that the sender may have to be both client (for the request) and server (for the status message).
2. The naming of general message types, such as “request”, “message status”, “update request” and “service request status”. The document also adds some semantics to the different message types.
3. Some definitions for content in a message header, covering requirements from the FAL convention as well as for the message exchange semantics defined in the guidelines.

In addition to these definitions, the document also suggests a suitable cryptographic standard for use in communication between ships and shore. It also discusses requirements to a public key infrastructure in the maritime domain, where lack of internet access is one element and the need for minimal bandwidth use is another. The latter particularly applies to digital signatures on VDES messages.

7.5 Guidelines for communication related to port calls

FAL has also published a guideline for communication with ports in relationship to port calls [14]. This document is based on the ITPCO’s port call guide [15] as well as other industry guidelines. It basically rephrases the business processes, parties and information exchanges defined in the ITCPO document as an IMO publication. It also provides part of the mapping between the ITCPO data objects and the IMO Compendium, and it also suggests the port ICT architecture described in 4.4. Thus, this is in effect a link between different industry guidelines and documents, and the maritime digitalization principles underlying the work in IMO FAL.

8 Application protocols for communication between ship and shore

As ships become more connected, digital information exchanges between ship and shore become more common. Except for special communication as described in section 5, the communications are normally set up as internet connections via satellite or mobile data links. They can in principle also used fixed internet lines when the ship is in port or when agents communicate on behalf of the ship.

Communication to or from the ship over internet can be in different forms and each of the following sub-section will describe one of these forms. Traditional document type transfers, e.g. ftp or e-mail will not be included in the discussions (see section 2.4.2).

8.1 Data replication

Data replication solutions copy data between onboard systems to a centralized system ashore. Dependent of type of replication systems, the onshore system may be a general-purpose gateway to other shore systems or used as a data base for different service providers.

8.1.1 ISO 23807 Asynchronous data transfer

ISO 23807 [16] specifies requirements for a file replication type data transfer between ship and shore. The concept is illustrated in Figure 13.

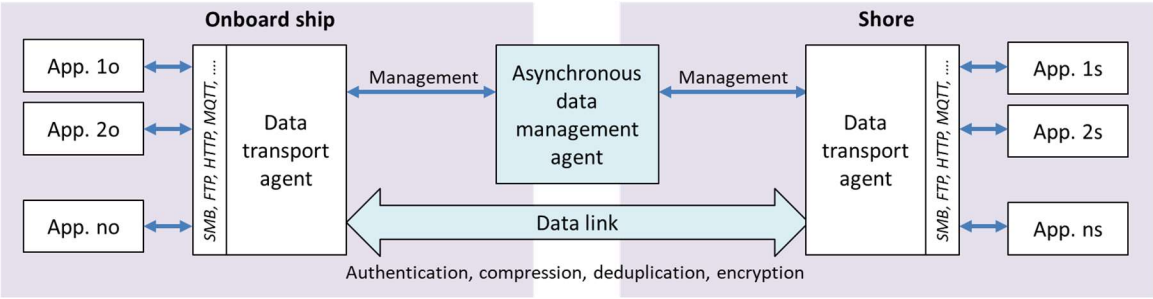

Figure 13 – File replication according to ISO 23807

Onboard applications communicate with a data transport agent via one of the indicated protocols or others, as shown in the figure. A ship side application can, e.g. be an ISO 19847 Data application server [7].

The transport agent is in contact with a similar agent ashore and together, via a data management agent, they control data replication between ship and shore. The transport management will handle prioritization, delayed transfers, bandwidth use and other issues that may need to be controlled on an expensive satellite data link.

The standard does not specify any protocol to use between the transport agents or between transport and management agents. As this is assumed to be a proprietary transfer mechanism, this can be left to implementors of such systems.

This solution is attractive as it is relatively easy to manage both with respect to cyber security and system maintenance. Applications on the ship or shore will interface to the replication system with common computer supported interfaces, including transparent file shares, and need little special adaption to interfaces or protocols. The system can also optimize use of satellite resources to keep costs under control while some data transfers still can be prioritized.

The main drawback is that this system cannot be used to implement more complex APIs, e.g. as is suggested in the port interface guideline [14]. If this functionality is needed and the replication principle is to be used, the APIs must be implemented in a shore-side application.

8.1.2 Proprietary data replication solutions

There are already commercial and proprietary solutions available for asynchronous data transfer like that described in section 8.1.1. Most ship electronics manufacturers have some form of communication solutions that is used for monitoring of own equipment, but which in many cases also can support more general information management. External parties may or may not be able to access data collected on shore. Two examples of proprietary systems are ABB Ability OneBox [28] and Kongsberg Kognifi [29]. Other systems are available.

8.2 International Data Spaces

With the use of proprietary data storage solutions on shore, one will rapidly encounter the issue of determining who has ownership of the data and how to grant access to it. This report will not go into any discussions on the legal and contractual aspects but will briefly describe the possibility of implementing a "maritime data space" that can be used to control access to data and data ownership.

The International Data Spaces Association (IDSA) [30] is a not-for-profit organization that develop specifications for a shared and distributed data space where ownership and access rights can be managed by internationally standardized mechanisms.

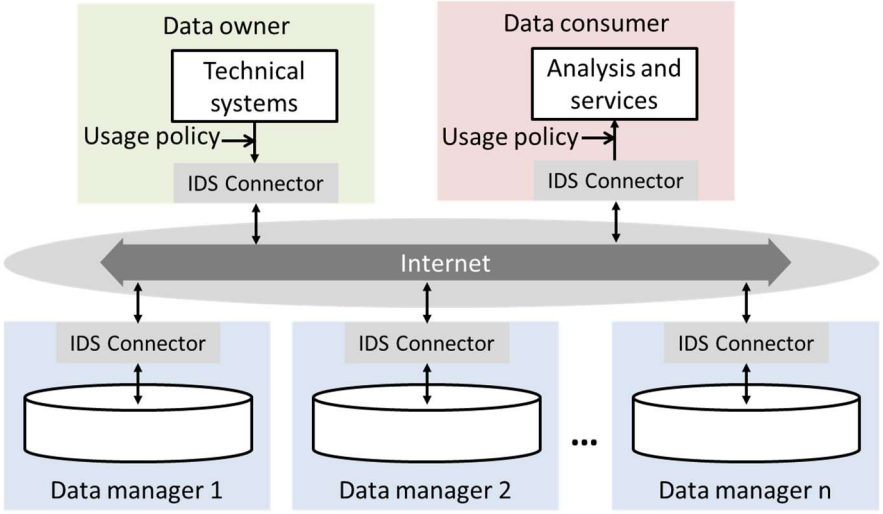

Figure 14 – Conceptual view of IDS system

Figure 14 shows a conceptual view of the IDS system. It is implemented by adding IDS connectors to data input and output paths. The connectors must be adapted to the local application but use standardized protocols for communication with each other. This allows the data owners to retain ownership of data regardless of where it is stored and to grant third parties access to this data without involving the data manager. The system may also include various service functions, e.g. as broker of services or for identity management.

A research project running from 2019 to 2021 [31] investigated the use of IDS for maritime applications as a "maritime data space". GAIA-X [32] is also one of the users of IDS and several

other projects in the transport sector is investigating and specifying a federated EU data space for transport and trade.

It is also important to note that IDS may be used to change the conventional "push" mechanism, where declarants send various mandatory reports to the authorities, to a "pull" mechanism, where authorities are allowed to access the data they need through the IDS, without giving additional work to the declarants.

8.3 Streaming or pseudo-streaming

On the opposite end of the performance scale from data replication, is data streaming. Here, the point is to transfer data as rapidly as possible so that the two sides of the communication link have always approximately the same information. This can be used for remote monitoring and control of the ship, e.g. as may be necessary for maritime autonomous surface ships (MASS) or for decision support to crew, which is becoming more common in certain cases. Typical applications for the latter are shore assistance on passenger ships during emergencies or interventions after failures in technical subsystems. Remote pilotage is also an application that will need streaming of data.

Another variant of streaming is near real-time transfer of measurements ("pseudo-streaming"). Here, one will tolerate some delays, e.g. on the order of ten seconds, but will still require that data is mostly transmitted without longer-term buffering.

8.3.1 Remote control

A special case is various forms of remote control where operators on shore fully or partly control ship processes. This is a relevant situation in conjunction with the development of autonomous ships or for crew assistance in special operations. The latter may e.g. be crane operations, operation of remotely operated vehicles for underwater operations, or launch and recovery of other crafts etc.

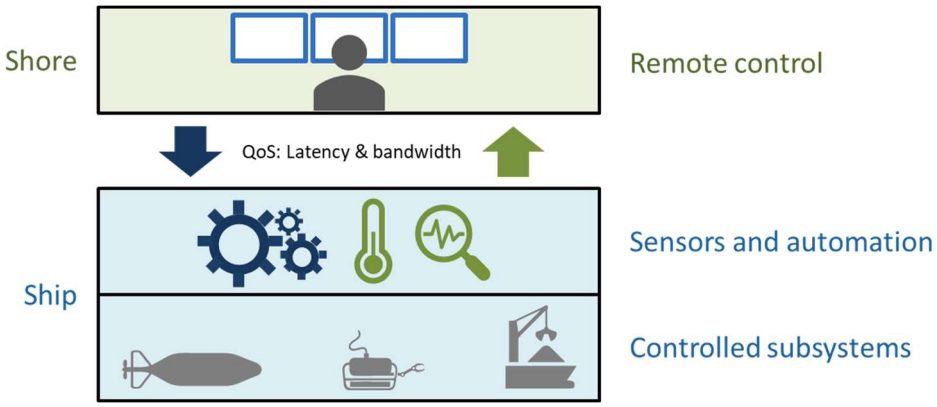

Figure 15 – Hierarchy of remote control

Remote control operators will normally rely on sensor readings, e.g. video to determine their actions. However, there will also be some form of sensor and automation system associated with the controlled assets. The requirements to the communication link (QoS – Quality of service) will be determined by the complexity and time constants related to the asset control as well as the type of control the operator need to exercise and what assistance he or she gets from the automation system.

As an example, it is virtually impossible to directly remote-control launch and recovery of smaller crafts via a GEO satellite link. The movement of the ship and the craft to be recovered will usually be faster than the delay over the GEO satellite link. However, if the automation system can assist in the time critical operations, it is still possible for the operator to provide a higher level of control that is less time critical.

This report will not go into further detail on this type of communication. No maritime standards have been established yet, so currently, proprietary protocols are used.

8.3.2 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 [26]. 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 distribute data between clients. The system uses hierarchical topics to publish and subscribe to different groups of data.

MQTT is increasingly popular in Internet of Things (IOT) applications due to its relative low complexity and lightweight implementation. It is also increasingly being used onboard and is one of the suggested data acquisition protocols in ISO 4891 [7].

For ship to shore use, MQTT is not directly to be recommended. However, technically one may construct a system like that of the white boxes shown in Figure 16. The grey boxes represent an alternative solution that will be discussed below.

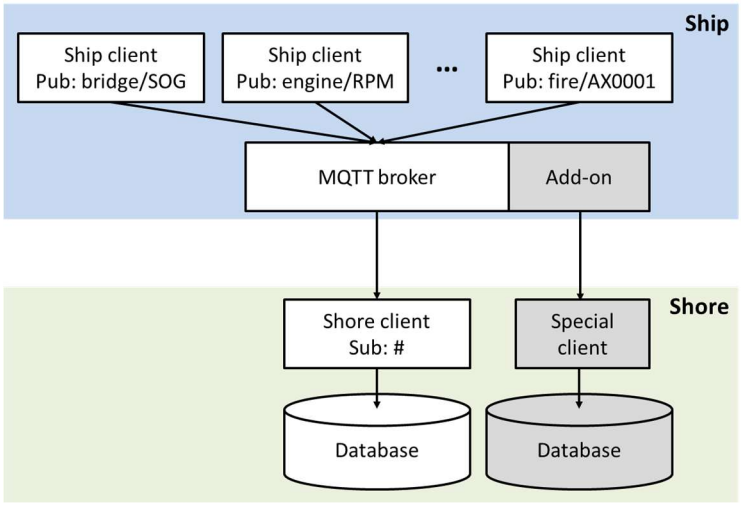

Figure 16 – Possible MQTT setup for ship-shore communication

The suggested setup will deliver all published data (bridge/SOG, engine/RPM and fire/AX001) to the shore client each time their value changes, as the client subscribes to the general wildcard "#". See ISO 18131 (section 9.7) for a possible standard for naming of topics in the maritime domain.

However, the data will be delivered in individual MQTT messages for each data item, which will create a relatively high communication overhead and computational load on the broker as well as on the shore client.

A better solution is to add functionality to the onboard MQTT broker and send the collected and compressed data by other means to shore. This is relatively easy to do and could, e.g. be done by using the ISO 19847 data formats [7]. The proposed solution is illustrated with the grey boxes.

8.3.3 ISO 18131 - Publish-subscribe architecture

ISO 18131 [27] is currently under development in ISO TC8/WG10. It is a requirements specification for asynchronous data transfer between parties at sea and shore without specifying any protocol to use.

The underlying architecture is very similar to that of MQTT (see section 8.3.2) and it proposes to use similar topic naming system. The specification also defines a naming structure for the topics that fit the maritime domain.

The main application seems to be data exchanges between external stakeholders and the ship. This may include flag state, class, port state and others. Thus, it is probably intended for a more macro-level distribution than MQTT which is basically an IOT standard.

8.4 API type protocols

API type protocols allow senders and receivers to engage in more complex message exchanges, e.g. to negotiate a just in time arrival in port [15]. An API can also be used to transfer a single document in a single exchange, like a document type interface. The API type protocols will normally include mechanisms for message formatting, digital signatures, management of API call sequences and more.

8.4.1 ISO 28005-1

The first edition of this standard was published in 2013 [35], but it is now under revision and will be published as edition 2 in early 2025. This will modify much of the general message appearances and definitions. The standard specifies a transport protocol for a generalized API based on HTTPS and an application protocol with a general message structure that allow different APIs to be easily constructed once the general protocol framework has been implemented.

8.4.1.1 Conformance with IMO guidelines

The ISO 28005 series are designed to be conformant to IMO FAL guidelines and specifications:

- The data model used in all standardized message components conform to the IMO Compendium (section 7.3).
- The message types and patterns are conformant to the guidelines on authentication, integrity and confidentiality (section 7.4).
- Relevant parts of the port related definitions are conformant to guidelines for communication between ship and shore (section 7.5).

Future editions and parts of the standard will likewise ensure conformance with these and other relevant guidelines. The protocol is not designed with general e-navigation services in mind (see section 7.1). However, ongoing work in IMO will harmonize S-100 data models with the IMO Compendium and by that also ensure compatibility between the systems. Also, one may include S-100 messages as payload in ISO 28005 messages.

8.4.1.2 Transport protocol

The data transport is using HTTP over TLS (HTTPS). The transport layer is not patterned on the REST architecture and specifies a plain HTTP interface where the HTTP protocol is completely decoupled from the application protocol. This allows a layered implementation as illustrated in Figure 17.

The figure shows the resulting layering for an ISO 28005 service provider implementation. A service user implementation will look similar but will mainly implement the client part to exchange synchronous messages to the service provider. However, also a service user can implement a HTTP server to receive asynchronous responses. Alternatively, asynchronous responses can be fetched by the user by polling the service provider.

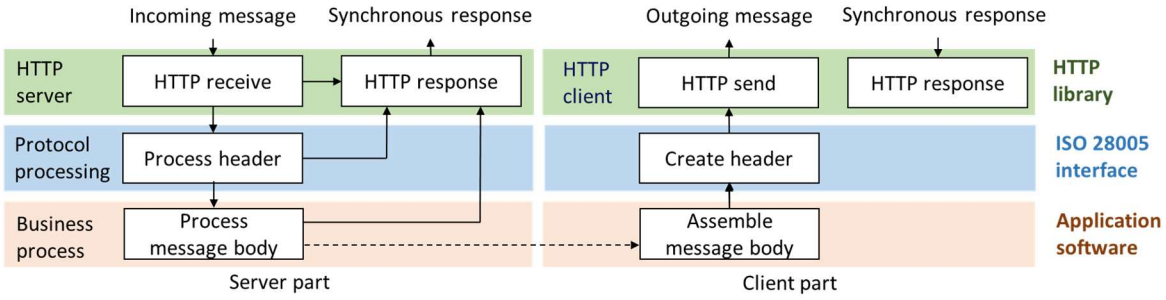

Figure 17 – ISO 28005 transport and application protocol layering

In principle, the two top layers can be off-the-shelf software while the bottom layer needs to be adapted to implement the actual business logic.

8.4.1.3 Message payload

The application message uses the HTTP multi-part format to support different types of data messages and attachments as illustrated in Figure 18.

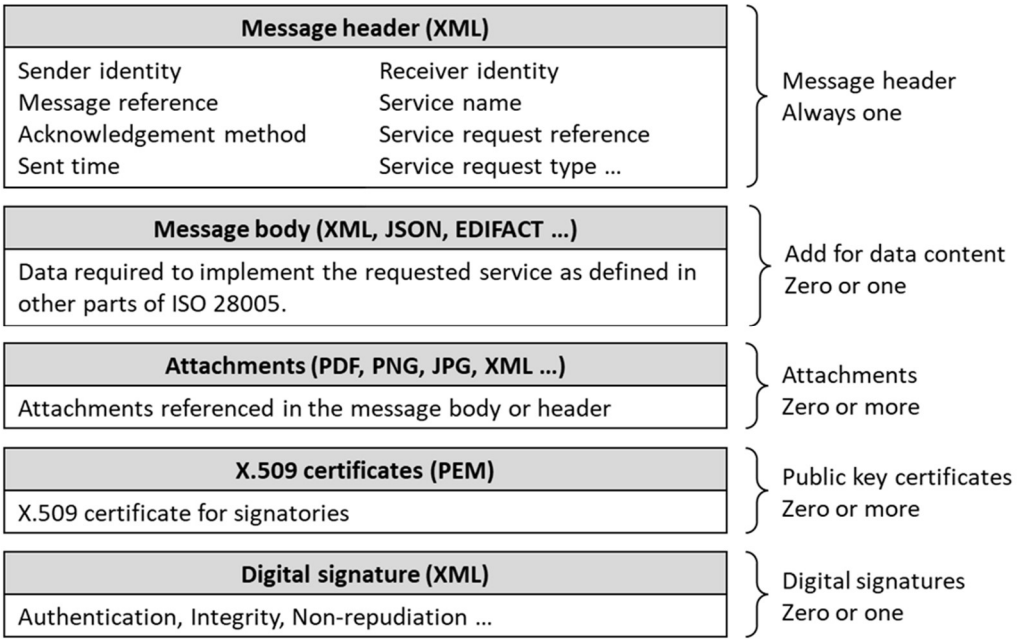

Figure 18 – HTTP multi-part message format

The XML message header has a fixed format with optional attributes that are used as required. It contains enough information to do generic processing of the message and pass the payload on to the correct business logic as illustrated in Figure 17.

The ISO 28005 message body is also defined by a single XSD specification and can be parsed for syntactic correctness by the generic transport interface software. The actual data objects included will be dependent on application and is specified in a message implementation guide for the application. The full content of the message body corresponds to the defined data objects in the IMO Compendium (see section 7.3).

Attachments are additional stand-alone files, normally references from the message body. This may, e.g. be PDF data sheets or pictures. Encrypted parts of the message body, e.g. passenger or crew lists or maritime declaration of health, may also be included as attachments.

One may also include public key certificates in the message, in case some of the sender identities are not yet included in a general PKI or if a suitable PKI is unavailable.

A list of digital signatures is included as the final part. This allows different parties to sign different parts of the message.

One can also use other file formats in the message body or in the attachments, e.g. UN/EDIFACT. This allows legacy systems to include complex manifests, bills of lading or passenger lists in native formats. This requires that the receiver understands these formats.

8.4.1.4 Generalized message sequence patterns – non-repudiation

ISO 28005-1 defines four general message exchange patterns. The patterns are used for all types of service requests, where service may include sending a mandatory report, retrieving some information, or requesting a physical service such as linesmen or tugs.

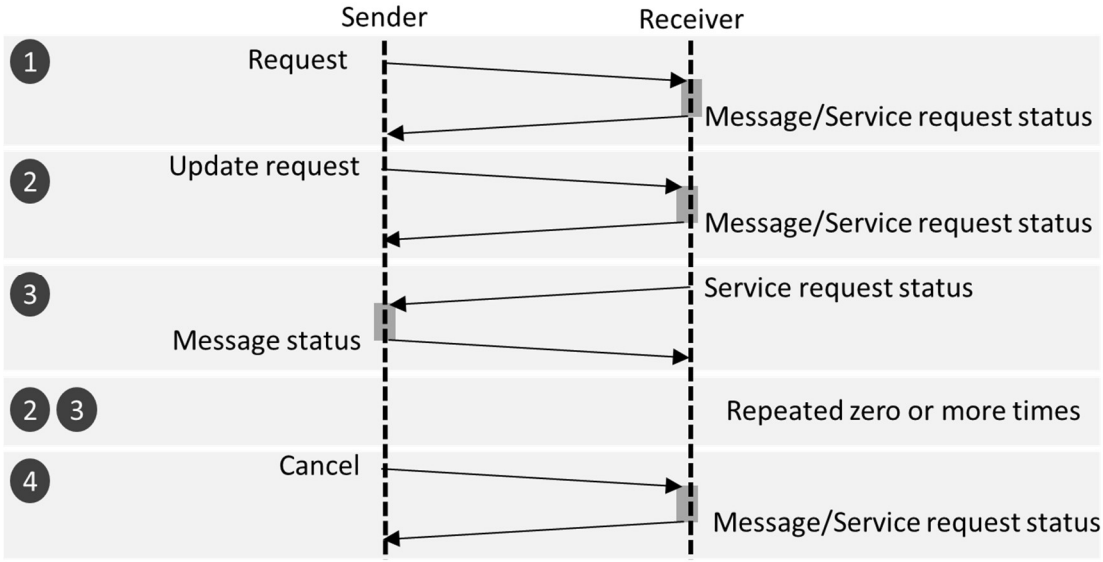

Figure 19 – General service request pattern

Figure 19 shows the most general service request and update pattern. The three other patterns are status poll for service user to ask for status on service; simple information fetch for atomic and non-modifiable requests for information; and subscription. All these patterns are based on the general service request.

All messages shall cause an acknowledged to be returned to sender. This can be used to prove that the message was received and read (non-repudiation).

8.4.1.5 Integrity, authentication, confidentiality, and non-repudiation

The use of HTTPS will secure message transfers from third party interference. There is also a possibility for further encryption of message parts to protect certain information from being accessed by non-authorized users in intermediate software systems such as a PCS or MSW. This may be relevant for protection of personal information such as passenger lists or the maritime health declaration.

The use of digitally signed message parts will provide integrity checks and authentication. The standard also requires full acknowledgements on all messages and service requests, which can be used to implement non-repudiation. Acknowledgements are also generally necessary for automated machine-to-machine message exchanges.

ISO 28005 does not specify any particular PKI to be used or specific interfaces to the PKI.

8.4.1.6 Flexible API design – message implementation guides

The standard XML message body will contain all data objects defined in the IMO compendium. All of these are optional. By modifying the message body content, different APIs can be easily created, and it is also trivial to define APIs with variable number of data objects, if that is desired.

Message implementation guides (MIG) will be published in the different parts of the standard, covering the applications that is defined in the IMO Compendium. Other MIGs can be created as needed.

8.4.1.7 Access authorization and service discovery

The standard includes a MIG for access authorization and the implementation is by including an access token in the message header. The access authorization API can also return a list of services that the token applies to, and this may be used as a simplified service discovery. No other service discovery mechanism is defined by the standard today.

8.4.2 IEC 63173-2 SECOM for S-100 based products

IEC 63173-2 [33] is also called SECOM for “secure communication”. It was developed in IEC TC80 as a carrier for S-421 messages as specified by IEC 63173-1 [34]. The latter standard covers route exchanges between ships and between ship and shore. However, SECOM is intended for all S-100 type product specifications and can be viewed as a general-purpose document type interface specification. It is claimed to be compatible with the relevant IHO specifications for exchange of S-100 product specifications.

SECOM contains five main components as illustrated in Figure 20. The blue parts are defined by SECOM, the dashed grey parts are outside the specification.

Technically, SECOM is quite like ISO 28005-1. It is based on HTTPS and a REST-type interface. However, as discussed in section 2.5 it will often be impossible to implement the full REST semantics due to connections into external processes beyond the context of the interfaces and their processing. SECOM is also implementing REST principles by embedding several instructions to the server in the URL. SECOM is also strongly integrated in the HTTP/REST framework by using

HTTP return codes also for SECOM diagnostics. It supports asynchronous deliveries of acknowledgements or other responses to received messages.

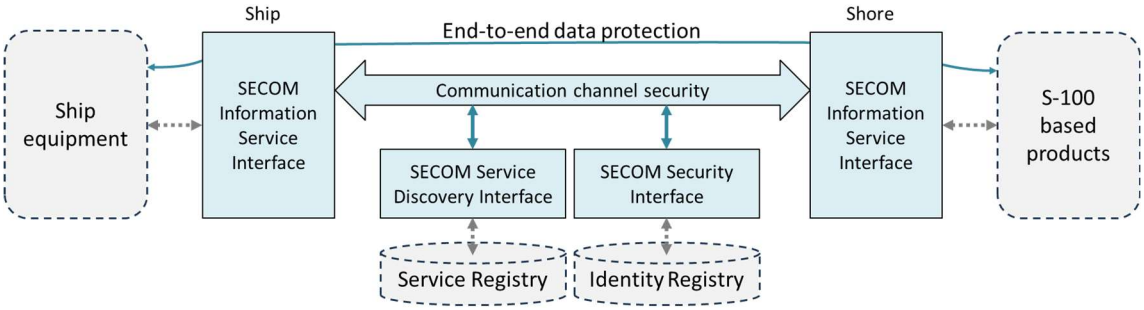

Figure 20 – SECOM components and structure

8.4.2.1 Information service interface

The service interface provides several services as listed in Table 6. This report will not go into further detail on these services.

Table 6 – Overview of SECOM communication services

Service	**Description**
Upload	Interface to send (push) information to consumer
Upload link	Interface to send (push) a link to information for a consumer to get
Acknowledgement	Interface to send acknowledgement asynchronously
Get	Interface to get (pull) one or more data sets from a service provider
Get Summary	Interface to get (pull) information about available datasets from service provider
Get by link	Interface to get a link to data sets from service provider (uses Upload link)
Access	Interface to request access to data sets
Access Notification	Interface to grant or deny access
Subscription	Interface to request subscription to data sets (uses Upload to send data)
Remove subscription	Interface to cancel a subscription
Subscription notification	Interface to receive information on the status of subscriptions
Capability	Interface to query service provider for details of available services
Ping	Interface to ask for technical status of specified services
EncryptionKey	Interface to exchange temporary symmetric encryption keys
PublicKey	Interface to exchange public key certificates.

8.4.2.2 Communication channel security and SECOM PKI

Communication security is provided by HTTP over TLS. It is implied that public key certificates from the SECOM PKI is used in HTTPS.

8.4.2.3 End-to-end data protection

To ensure end-to-end integrity and authentication, SECOM also uses digital signatures over the contents of messages. This is like what ISO 28005 does.

Encryption is done by symmetric keys and requires that client and server exchanges keys before the message is sent. The key is temporary and is used only for one data transmission.

8.4.2.4 SECOM security interface

SECOM provides its own interfaces to a public key infrastructure. However, most of the interfaces are designed according to commonly used standards. Table 7 lists the available interfaces.

Table 7 – Overview of SECOM PKI services

Service	Description
CSR	Certificate signing request
GetPublicKey	Get a public key certificate from the PKI based on certificate thumbprint
CRL	Get a certificate revocation list
OCSP	Check revocation status of certificates with the OCSP protocol.
Revoke	Revoke a certificate

This report will not go into further details of these functions.

8.4.2.5 SECOM service discovery

SECOM allows any number of service registries, but provides a standard interface to each. This interface allows the consumer to search for S-100 services based on standardized service descriptions from the S-100 framework.

8.4.3 ISO 15000-2 – Applicability statement AS4

ISO 15000-2 [38] is identical to the ebMS AS4 profile [39]. These specifications are profiles of the more general ISO 15000-1 or ebMS 3.0 Web Services B2B messaging. The AS4 profile reduces options and make implementation less complex. The standards are part of the OASIS ebXML framework and is a modernized version of the similar applicability statement AS2 [40]. AS4 is used in the European eDelivery framework [41], which includes Peppol [42], the European federated electronic procurement system for use across different jurisdictions. The Peppol system is increasingly being used outside the EU and associated states. The Open Peppol association has also started a project to include logistics in the Peppol framework [43].

Program code for an AS4 access point is available as several open-source implementations. These are mostly written in Java.

8.4.3.1 Four-corner architecture

AS4 is based on a "four corner" architecture as shown in Figure 21. However, it can also be used in a direct point-to-point configuration if both parties implement the AS4 specification. Otherwise, it is expected that the interface between the sender and receiver and the access points is by some specialised and application and/or region-specific protocol.

Each user of the system must have an access point (AP) that converts between the user's native document format and the AS4 protocol. The access point can be implemented inhouse or provided by third parties. In some cases, there may also be a network of intermediaries between the two access point corners.

The AS4 network may implement various registries, e.g. for authentication of senders and receivers or for service discovery. This depends on the application. For the European Maritime Single Window environment (EMSWe), the plan is, e.g. to create a central registry of declarants and also to implement various validation services in the network. This is planned to be done in corner 3, in the EU-supplied reporting interface module (RIM).

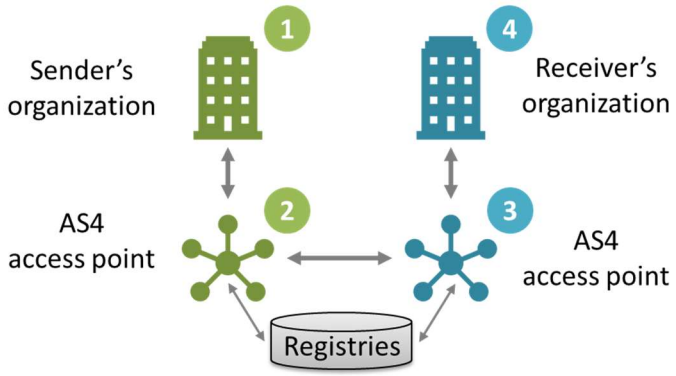

Figure 21 – AS4 4-corner model

The AS4 profiles include one full profile with both message pull and push for both sender and receiver as well as simpler profiles where the sender does not need to support push from receiver.

8.4.3.2 Transport via HTTP, web services and SOAP

The payload is a SOAP message over HTTP, i.e. an XML message defined according to the web service standards. The SOAP message may either contain a single XML message, containing the full transaction information or it can also be a multi-part MIME-compliant message to transfer additional information that is not in XML format. The latter may also be used when the payload is compressed.

8.4.3.3 Header block

The SOAP message contains a header which structure is defined by ebMS 3.0. The header is payload agnostic and contains information used in the management of the transaction, e.g. information necessary to route the message to the correct destination.

8.4.3.4 Non-repudiation

The messaging protocol can require that a receiver of a message returns an acknowledgement which can be used to prove that the message was received and read.

8.4.3.5 Security

The transport layer is HTTP, optionally secured with TLS, SSL or equivalent. As SSL has been depreciated [5], TLS or equivalent should be used.

The messaging protocol can also use standard web security components to include signatures and optionally public key certificates in the message.

8.5 Third party connectivity providers

Peer-to-peer communication do not use third party connectivity providers, except for basic internet access. This is illustrated in Figure 22.

There are generally two types of third-party connectivity providers. A four-corner service is shown in Figure 21. It consists of the sender (service requestor) at corner 1 and the receiver (service provider) at corner 4. In between are the access points, where service users and providers use third party access points. In this model the access point will also often contain additional services such as accounting.

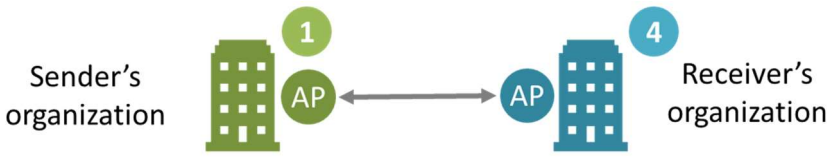

Figure 22 – Peer-to-peer communication

Another type is the hub-and-spoke system where a single service provider does the routing between requestors and providers. This is illustrated in Figure 23. Here the connectivity provider may also supply identity management and various directory services.

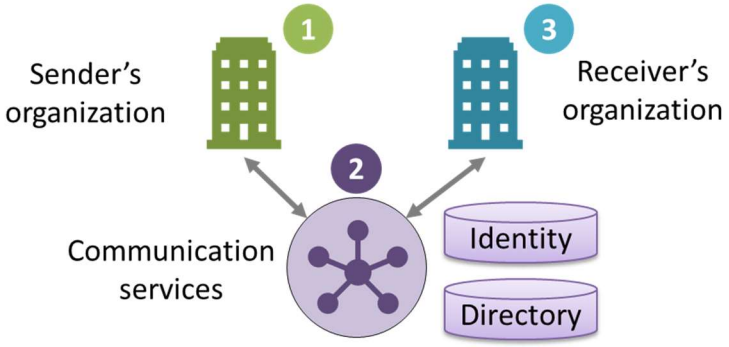

Figure 23 – Hub-and-spoke communication system

This section will give a brief description of different connectivity providers that implement such third-party systems.

8.5.1 Peppol – Pan-European Public Procurement Online

Peppol uses the AS4 protocol (section 8.4.3) to transport data between access points. There are several different providers of access points, and these providers will usually also provide other

services to the users, such as accounting with automatic billing or payments through the Peppol network. A Service Metadata Locator (SML) is provided by OpenPeppol, a non-profit international association of access point providers and others.

Despite the European origin, OpenPeppol has at the time of writing members from 43 different countries, e.g. Australia, USA, Singapore and Japan [42]. It has currently around 475 registered access point providers.

At the time of writing, Peppol is mainly used for e-procurements, including purchase orders, invoices and other documents. However, there is also work ongoing to extend Peppol to use in logistics. This work started in 2023 and has a decision point in Q3 of 2023 to establish the services.

8.5.2 EMSWe – European MSW environment

EMSWe will use a similar system as Peppol. Each EU state will implement an access point for its national users. This is the RIM (Reporting Interface Module). These access points can then route messages to other states' access points. As Peppol, EMSWe will also implement identity and possibly digital signature repositories.

8.5.3 MCP – Maritime Connectivity Platform

MCP [44] is today a hub and spoke system with one commercial implementation, Navelink. In principle MCP can be implemented as a system of independent connectivity providers which will be more like the four-corner model of Peppol. MCP uses the SECOM protocol (see section 8.4.2) for connection to end users but is in principle protocol agnostic. The main functionality is to provide an identity register associated with a PKI and a service discovery function.

8.5.4 Navelink

Navelink [45]is a not-for-profit, but commercial operation, implementing the MCP system in one single instance. It is owned by Wärtsilä and Kongsberg. However, Navelink plans to shut down operations in December 2024.

9 Data models

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

9.1 IMO Reference Data Model – IRDM

The IMO reference Data model 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. The data model is available from this link:
https://imo.org/en/OurWork/Facilitation/Pages/IMOCompendium.aspx

The model has mapping to the corresponding data models used in ISO 28005-2, in UNECE MMT-RDM and the WCO data model. The latter two is not discussed further in this document but are focusing on governmental data structures and electronic trade respectively.

The IRDM is maintained by the Expert Group on Data Harmonization (EGDH) which is a sub-group of the FAL Committee of IMO.

9.2 CMDS/S-100 - Common Maritime Data Structure

The CMDS was defined as the underlying data model in the e-navigation SIP [10]. It was decided to use the IHO S-100 infrastructure to implement the CMDS. The S-100 Geospatial Information registry contains data elements defined in S-100 [46].

There is also a currently unformal cooperation between IHO and IALA and the EGDH to make sure that S-100 as far as possible is kept aligned with the IRDM.

9.3 ISO 28005-2/3 – ISO 28005 data model

ISO 28005-2 [36] is a data model for electronic port clearance that has been harmonized with IRDM. It currently covers all data elements defined in the FAL Convention as well as some additional elements for other IMO instruments. 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.

ISO 28005-3 [37] will soon be published and will extend ISO 28005-2 with new definitions from the IRDM, including also messaging guidelines for port call optimization or just in time arrival.

9.4 UNECE Multi-Modal Transport Reference Data Model

This is the UNECE variant of the IRDM. It contains several data elements with corresponding definitions, suitable for multi-modal transport information exchanges [47].

9.5 IEC 61162-1 – Navigational data

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.

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. However, the model is only available as purchase from NMEA.

9.6 ISO 19848 – Automation data

This standard 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 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/

9.7 ISO 18131 - Publish-subscribe architecture

ISO 18131 [27] is currently under development in ISO TC8/WG10. It is a requirements specification to asynchronous data transfer between parties at sea and shore without specifying any protocol to use. It is planned to go out as a draft standard in late 2023. The underlying architecture is like that of MQTT (see section 8.3.2) and it proposes to use similar topic naming system. The specification also defines a naming structure for the topics that fits the maritime domain.

References

[1] Internet Society, RFC 9293, Transmission Control Protocol (TCP)

[2] Internet Society, RFC 2068, Hypertext Transfer Protocol -- HTTP/1.1.

[3] Internet Society, RFC 9110, HTTP Semantics

[4] Internet Society, RFC 8446, TLS version 1.3.

[5] Internet Society, RFC 7568, Deprecating Secure Sockets Layer Version 3.0, June 2015.

[6] IMO A.851(20), IMO Assembly Resolution A.851(20), General Principles for Ship Reporting Systems and Ship Reporting Requirements, including Guidelines for Reporting Incidents involving Dangerous Goods, Harmful Substances and/or Marine Pollutants. Adopted on 27 November 1997.

[7] ISTS Report R3.1: Onboard Maritime ICT Architecture and Standards, V1.0 – 2023-07-27

[8] Rotem-Gal-Oz, Arnon. "Fallacies of distributed computing explained." *http://www.rgoarchitects. com/Files/fallacies. pdf* 20 (2006).

[9] 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.

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

[11] IMO FAL.5/Circ.42/Rev.1, Guidelines for Setting Up a Maritime Single Window, July 1st 2021.

[12] IMO Compendium, approved by FAL 47 on March 28th 2023, and as amended. Available from https://imo.org/en/OurWork/Facilitation/Pages/IMOCompendium.aspx.

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

[14] IMO FAL.5/Circ.52, Guidelines for Harmonized Communication and Electronic Exchange of Operational Data for Port Calls, 31 March 2023.

[15] ITPCO - International Taskforce on Port Call Optimisation https://portcalloptimisation.org/.

[16] ISO 23807:2023 Ships and marine technology — General requirements for the asynchronous time-insensitive ship-shore data transmission, March 2023.

[17] Rødseth, Ø. J., Kvamstad-Lervold, B., & Ho, T. D. (2015, May). In-situ performance analysis of satellite communication in the high north. In *OCEANS 2015-Genova* (pp. 1-6). IEEE.

[18] WINLINK web pages (short wave email): https://www.winlink.org/

[19] IALA Collection of regional applications for AIS Application Specific Messages, https://academy.iala-aism.org/asm/

[20] IALA Guideline 1117 "VDES Overview", https://www.iala-aism.org/product/g1117/

[21] Recommendation ITU-R M.1371-5, Technical characteristics for an automatic identification system using time division multiple access in the VHF maritime mobile frequency band, February 2014.

[22] Recommendation ITU-R M.2092-1, Technical characteristics for a VHF data exchange system in the VHF maritime mobile band, February 2020.

[23] World Radiocommunication Conference 2019 (WRC-19), Final Acts, ITU Publications 2020.

[24] SATBEAMS web site: https://satbeams.com/

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

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

[27] ISO 18131 Ships and marine technology — General requirements for publish-subscribe architecture on ship-shore data communication, Working Draft, May 17. 2023.

[28] ABB Ability OneBox: https://new.abb.com/marine/systems-and-solutions/digital/abb-ability-onebox---marine-signals-monitoring

[29] Kongsberg Kognifi: https://www.kongsberg.com/digital/resources/news-archive/2017/kongsberg-launches-kognifai/

[30] International Data Spaces Association – IDSA: https://internationaldataspaces.org/

[31] Maritime Data Space: https://internationaldataspaces.org/maritime-data-spaces-provides-trusted-environment-for-industry-data-sharing/

[32] GAIA-X: https://internationaldataspaces.org/we/gaia-x/

[33] IEC 63173-2:2022, Maritime navigation and radiocommunication equipment and systems - Data interfaces - Part 2: Secure communication between ship and shore (SECOM).

[34] IEC 63173-1:2021, Maritime navigation and radiocommunication equipment and systems - Data interfaces - Part 1: S-421 route plan based on S-100.

[35] ISO 28005-1:2013, Security management systems for the supply chain — Electronic port clearance (EPC) — Part 1: Message structures.

[36] ISO 28005-2:2021 Ships and marine technology — Electronic port clearance (EPC) — Part 2: Core data elements

[37] ISO 28005-3 Ships and marine technology — Electronic port clearance (EPC) — Part 3: Data elements for ship and port operation

[38] ISO 15000-2:2021, Electronic business eXtensible Markup Language (ebXML) — Part 2: Applicability Statement (AS) profile of ebXML messaging service

[39] AS4 Profile of ebMS 3.0 Version 1.0. 23 January 2013. OASIS Standard. http://docs.oasisopen.org/ebxml-msg/ebms/v3.0/profiles/AS4-profile/v1.0/os/AS4-profile-v1.0-os.html.

[40] RFC 4130, MIME-Based Secure Peer-to-Peer Business Data Interchange Using HTTP, Applicability Statement 2 (AS2), July 2005.

[41] European eDelivery framework: https://ec.europa.eu/digital-building-blocks/wikis/display/DIGITAL/eDelivery

[42] PEPPOL - Pan-European Public Procurement Online, see Open Peppol at https://peppol.org/

[43] Peppol logistics specifications https://openpeppol.atlassian.net/wiki/spaces/RR/pages/3123642381/2023.07.07+Peppol+Logistics+specifications

[44] Maritime Connectivity Platform, https://maritimeconnectivity.net/

[45] Navelink, https://www.navelink.org/

[46] IHO Geospatial information registry, https://registry.iho.int/fc/list.do.

[47] UNECE Multi-Modal Transport Reference Data Model, https://unece.org/trade/uncefact/rdm, https://unece.org/trade/documents/2018/01/standards/multi-modal-transport-reference-data-model-brs