C70-11.5.4.1

IALA GUIDELINE

G-XXXX

GUIDELINE ON IP (WEB SERVICE) BASED S-100 DATA EXCHANGE

Edition 1.0

Date (of approval by Council)

10, rue des Gaudines - 78100 Saint Germain en Laye, France
Tél. +33 (0)1 34 51 70 01- Fax +33 (0)1 34 51 82 05 - contact@iala-aism.org
www.iala-aism.org

International Association of Marine Aids to Navigation and Lighthouse Authorities
Association Internationale de Signalisation Maritime

DOCUMENT REVISION

Revisions to this IALA Document are to be noted in the table prior to the issue of a revised document.

Date	Page / Section Revised	Requirement for Revision

CONTENTS

1. INTRODUCTION

1.1. SCOPE

This Guideline provides guidance on the application of reliable and efficient IP (Web Service) based communication for the exchange of S-100 data. With the introduction of section 14 in the S-100 standard an alternative mechanism for efficient, fine-grained S-100 data exchange is available. This online data exchange model allows frequent transmission of data to allow continuous information exchange between e-Navigation applications and efficient usage of available (limited / expensive) bandwidth. This is an important building block for technical services for the implementation of maritime services in the context of e-Navigation.

It also facilitates the realization of service-oriented architectures (SOA) using S-100.

This guideline introduces the relevant technologies and explains the transmission of S-100 data with Web Services. In the Appendix an example of the implementation of such a Web Service for the provision of Maritime Safety Information using S-124 is shown. This includes the specification of this Web Service according to G1128 Specification of Technical Services.

This guideline is intended for service providers, system architects and developers, who are designing S-100 based technical services implementing Maritime Services in context of e-Navigation.

1.2. RELATED DOCUMENTS

IHO S-100 Standard

IALA Guideline 1128 Specification of Technical Services

MSC.467(101) on Guidance on the definition and harmonization of the format and structure of Maritime Services in the context of e-navigation

MSC.1/Circ.1610 INITIAL DESCRIPTIONS OF MARITIME SERVICES IN THE CONTEXT OF E-NAVIGATION

ISO/IEC 7491- Open Systems Interconnection – Basic Reference Model

OAuth 2.0 Framework - RFC 6749

1.3. BACKGROUND

The maritime industry is a big sector of today's economy. Hundreds of thousands of vessels are constantly underway in inland waterways, coastal waters or the open sea. To sail within their environment safely there is a continuous need for communication. This could be for example communication with surrounding vessels for collision avoidance, contacting vessel traffic service operators in port areas, obtaining weather data for the planned route or receiving navigational warnings to name only a small selection.

Until now most of these processes and services use several different types of communication channels [1]. Often the way of obtaining the above-mentioned information can also differ depending on the location of the services. This makes the acquisition of relevant information more difficult in many situations. Especially safety-relevant data can be a problem when using unsecured communication methods, in which the validity and the propriety of the data cannot be verified. In an unprotected setup an attacker could aim at injecting invalid information into navigational systems to create a misleading assessment of the environmental and navigational situation on vessels.

Contrarily, a technical trend consisting of new communication technologies for the maritime sector could be observed in the past years: IP-based technologies are increasingly rolled out and made available to the end-user. **Low Earth Orbit** (LEO) Satellite Networks, who can provide real-time IP-based communication [4] are currently emerging and are expected to find applications in several areas [5]. Also terrestrial technologies like **LTE** are

expected to play an important role for the maritime industry in the future [6]. In addition to that, satellite providers like Inmarsat are going to launch broadband IP services that would be part of the well-known **Global Maritime Distress and Safety System** (GMDSS) in the near future [7].

The fact that a set of important information can only be obtained from a lot of different sources with their own standards, channels and technologies makes the gathering of information complicated and expensive. Especially safety-relevant data like the MSI, Ship-to-Shore reporting, Vessel Traffic Management or Pilot services should be easy to distribute and easy to receive. The developments in IP-based communication for maritime applications can be seen as an opportunity to make important services easier available and more secure. The layer model of the internet protocol opens new possibilities for a separation of services and communication channel.

This paper gives guidance on how to distribute information in the maritime environment using secure IP-based communication. It can be applied to any digital maritime service.

The **Maritime Safety Information (MSI) Service** is a GMDSS service for providing information which is needed for safe navigation of vessels [2]. It is a good example for a set of data that needs to be distributed to vessels frequently with a service-bound communication-path: The service is currently realized e.g. by a specific terrestrial (NAVTEX) as well as a satellite (SafetyNET) communication channel [3]. There is no established mechanism to ensure cyber security. A basic example on how this service can be realized conforming with this guideline is presented in the ANNEX A.

2. NORMATIVE COMPONENTS

2.1. IP-BASED COMMUNICATION IN MARITIME ENVIRONMENTS

The stack of communication technologies in the maritime industry is comprehensive. Technologies like LTE, VHF, AIS, Wi-Fi, etc. are commonly used on ship bridges. The IP-Protocol is a widespread network layer protocol and abstracts from data link and physical communication layers (in the OSI layer-model). Different Technologies that are already used in maritime applications can provide the underlying layers of the IP-Protocol. Satellite communication, LTE or 802.11, for example, can be utilized for that. The abstraction from these low-level standards opens new possibilities for always available services without the need of specific implementations for several low-level communication channels.

Especially in the maritime industry IP Communication is opening opportunities for new business models, applying more standards and getting away from proprietary technologies. With the new developments in IP-providing services communication with an exhaustive availability (satellite) or with a very high bandwidth (LTE), a new set of maritime services is imaginable. These services are implemented on top of the IP-Protocol and therefore do not need to deal with low-level communication issues. These services can be reached by Wi-Fi in port areas, LTE or cellular technologies in coastal areas or satellite communication at sea to make the most efficient way of communication possible respectively.

Also, upcoming issues with cyber-security are currently relevant (see [12]). Additionally, some low-level maritime technologies, such as AIS are completely open and can be misused easily. IP-based communication enables to employ the standard security protocols built on top of IP and the layers above it (such as TCP). The IP-protocol is not the answer to all security related issues, but it provides the possibility to create secure communication channels and is a technology that needs to be discussed in the maritime industry. The MSI is a good example for a service that can be deployed as an IP-based service.

2.2. S-100 ONLINE DATA EXCHANGE

"The **S-100 Standard** is a framework document that is intended for the development of digital products and services for hydrographic, maritime and GIS communities. It comprises multiple parts that are based on the geospatial standards developed by the International Organization for Standardization, Technical Committee 211 (ISO/TC211)." [10]

The following section summarizes the data exchange sections of the S-100 standard. The proposed concept in section 3 is an implementation of the data exchange model of the S-100 standard.

The S-100 Standard allows exchanging S-100-Datasets with the S100_ExchangeSet class provided in section 4a of the Standard. An important part of the Exchange Set Model is the aggregation of Metadata and support files. A complete S-100 Dataset, typically consisting of different files such as the Feature Catalogue or digital signatures should be exchanged with its Metadata in this way (see Figure 1).

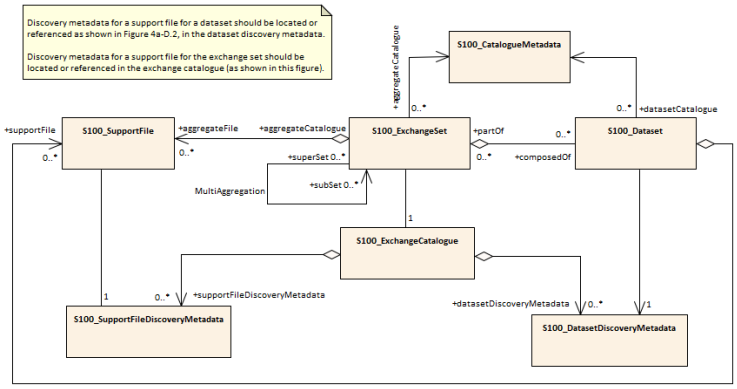


Figure 1: S100 Exchange Set Model for exchanging S-100 Datasets with their Metadata

When it comes to continuous data exchange nowadays, Webservices with publicly available APIs are often utilized for interchanging information. Webservice Technologies like REST or SOAP allow a fine-grained and efficient exchange of information. For this reason, Part 14 of the S-100 defines the usage of online services for the exchange of S-100 sets of data. Services themselves shall be modelled in a S-100 conform way (see Figure 2): The central class of the Service Data Model is the S100_ServiceMetaData which is composed of the Service Data Model including the S-100 Feature catalogue and the Service Interface which can be used to communicate with the Service.

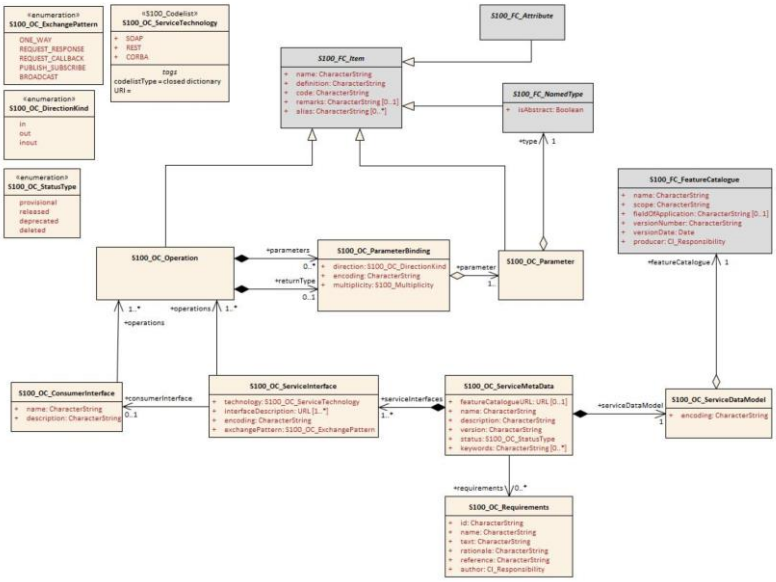


Figure 2: S-100 Part 14: Data Model to describe a Service

The Service Data Model does not contain all the fields used to describe the S100_ExchangeSet. This is due to the nature of a Service. A service is typically used to exchange multiple datasets as time passes.

Some information contained in the support files of the S100_ExchangeSet is dataset-specific and cannot be mapped to the general Service Metadata Model. A digital signature of a dataset, for example, is directly derived from the specific dataset and is different for every dataset. It has also kept in mind that a service has the possibility to reduce the amount of transmitted data. Meta-Information such as the Feature Catalogue or the available operations only need to be transmitted once when a new consumer connects to the service and opens a new session. The service can keep track of the sessions and only submit new information, that is not already known to the consumer. This makes the continuous communication more efficient and lightweight in comparison to the S100_ExchangeSet if multiple datasets need to be transmitted over time.

The two aspects mentioned above should be considered when constructing the data model of the Service: Firstly, if Metadata needs to be added to the datasets, either the data model itself needs additional fields for the description of Metainformation or a support class, similar to the S100_ExchangeSet needs to be constructed. Secondly, the Service communication scheme needs to be designed in such a way that the Service Metadata (not the dataset-specific Metadata) must be sent to the service consumer at the beginning of a session or the service metadata must be known to the consumer before. This is also prescribed by the S-100 Standard (section 14-4 to 14-6) and reduces the amount of transmitted data in comparison the S100_ExchangeSet, where Metadata such as the Feature Catalogue would be transmitted every time.

2.3. MARITIME CONNECTIVITY PLATFORM

The goal of the **Maritime Connectivity Platform (MCP)** is to enable that information can be exchanged efficiently, securely, reliably and seamlessly between authorized maritime entities across diverse communication systems. To this end the MCP consists of three core components: The Maritime Identity Registry (MIR), the Maritime Service Registry (MSR), and the Maritime Messaging Service (MMS).

The MIR compromises three components that together provide the infrastructure necessary for secure communication services today. Firstly, Identity Management: Each MCP entity obtains a unique ID in terms of a Maritime Resource Name (MRN). Secondly, Public Key Infrastructure (PKI): Each MCP entity holds an electronic identity in terms of a public/private key pair and a certificate bound to their MCP ID. And thirdly, Authentication and Authorization for Web Services: MCP entities benefit from login, single sign-on, and authorization for API access of web services, as well as secure integration of web services based on the standards OAUTH 2.0 and OpenID Connect.

3. COMPONENTS

3.1. WEB SERVICE BASED S-100 DATA EXCHANGE

In a Web service a Web technology such as HTTP — originally designed for human-to-machine communication — is used for transferring machine-readable data formats such as XML and JSON or in our case GML describing S-100 data. In practice, a Web service commonly provides a Web-based interface to a maritime technical service, utilized for example by a mobile app or bridge equipment, that provides a user interface to the end user.

The communication always consists of a request message from one machine (client) to another machine (server) and a reply message from the server to the client. The message can contain S-100 data encoded in GML. Different types of requests are named operations.

POST /Get_NW_Messages HTTP/1.1

HOST: nw-service.com

Content-Type:text/xml

Commented [JM1]: Add gml area parameter

Figure 3: Example REST-POST-Request to retrieve navigational warnings.

```
<?xml version="1.0" encoding="UTF-8"?>
 <S124:DataSet
 xmlns:xsi=http://www.w3.org/2001/XMLSchema-instance
 xmlns:gml="http://www.opengis.net/gml/3.2"
 xmlns:S100="http://www.iho.int/s100gml/1.0"
 xmlns:S100EXT="http://www.iho.int/s100gml/1.0+EXT"
 xmlns:s100_profile=http://www.iho.int/S-100/profile/s100_gmlProfile
 xmlns:S124="http://www.iho.int/S124/gml/cs0/0.1"
 xmlns:xlink="http://www.w3.org/1999/xlink">
  xsi:schemaLocation="http://www.iho.int/S124/gml/cs0/0.1 .../S124.xsd" gml:id="ds">
  <gml:boundedBy>
   <gml:Envelope srsName="http://www.opengis.net/def/crs/EPSG/0/4326">
    <gml:lowerCorner>53.602678 6.934154</gml:lowerCorner>
    <gml:upperCorner>53.922239 7.528269</gml:upperCorner>
   </gml:Envelope>
  </gml:boundedBy>
  <S124:References gml:id="references">
   <messageSeriesIdentifier>
    <nameOfSeries>Navigational Warnings</nameOfSeries>
    <warningNumber>0</warningNumber>
    <warningType>local navigational warning</warningType>
    <year>2019</year>
    <productionAgency>000</productionAgency>
   </messageSeriesIdentifier>
   <referenceCategory>in-force</referenceCategory>
   <noMessageOnHand>false</noMessageOnHand>
   <theWarning xlink:href="#preamble"/>
  </S124:References>
  <S124:NWPreamble gml:id="preamble">
```

```
<messageSeriesIdentifier>
 <nameOfSeries>Navigational Warnings</nameOfSeries>
 <warningNumber>0</warningNumber>
 <warningType>local navigational warning</warningType>
 <year>2019</year>
 <productionAgency>000</productionAgency>
</messageSeriesIdentifier>
<publicationDate>2019-05-04T18:13:51.0</publicationDate>
<generalArea>
 <locationName>
  <text>Norderney</text>
 </locationName>
 <locationName>
  <text>Langeoog</text>
 </locationName>
</generalArea>
<theWarningPart xlink:href="#warning"/>
</S124:NWPreamble>
<S124:NavigationalWarningFeaturePart gml:id="warning">
<geometry><S100:pointProperty>
  <S100:Point gml:id="pnt1">
  <gml:pos>53.731420 7.397681</gml:pos>
  </S100:Point>
</S100:pointProperty></geometry>
<warningHazardType>uncharted rock</warningHazardType>
<warningInformation>
 <headline>Uncharted Rock</headline>
 <text>An uncharted rock was discovered between Langeoog and Norderney islands...</text>
</warningInformation>
<header/>
</S124:NavigationalWarningFeaturePart>
</S124:DataSet>
```

Figure 4: S-100 gml answer to the request shown in Figure 3.

A more elaborated example of transfer of S-124 data is provided in ANNEX A.

3.2. MAKING USE OF THE SESSION CONCEPT

- What is a session in context of a WebService / Application-Layer Session: Any type of communication between service consumer and provider from initial connection to disconnection.
- Why: Efficient exchange of Metadata, Managing states of communication / interaction
- Session commands: StartSession, KeepAlive, TerminateSession, ResumeSession (bi-directional) – explain
- In session-based services, redundant transmission of Metadata can be avoided. The transmission of general service-related Metadata should be carried out at the start of a communication session.

Commented [JM2]: Write as coherent text

Commented [JM3]: Check command names

The operations StartSession, EndSession, KeepAlive and GetMetaData are the minimal requirements for a S-100 conform session-based service specification as stated in section 14-9 of the S-100 standard. Sessions are utilized to keep an internal state of which consumer has received which S-100 data. When querying the service again, the service can identify the consumer by the sessionID and for example only transmit new datasets. This is an important factor to minimize the traffic and ensure that every consumer is aware of any relevant data.

Note that GetMetaData returns the ServiceMetaData instance, defined in Figure 2. Hence, GetMetaData is the only command that must be known to the consumer to discover the services capabilities.

3.3. AUTHENTICATION MECHANISMS TO ENSCURE CYBER SECURITY

To secure the exchange of the S-100 data, two options are available. One option is to require that each dataset is digitally signed by the originator of the warning. Thereby it is possible to guarantee origin and message authenticity without any trust assumptions on intermediary communication points, but care has to be taken to prevent replay attacks. The second option is to ensure that the communication between the consumer and service is carried out via a secure connection, e.g. via TLS. The TLS Protocol is very common in Webservice communication and provides no further overhead. However, the consumer has to trust that the service provider distributes authentic and timely S-100 data only, and it lies with the service provider to ensure this. The two options can of course also be used in combination.

Both solutions require the existence of a Public Key Infrastructure (PKI) including a certificate authority (CA) that issues certificates for the participants of the proposed communication pattern. A consumer-defined lookup-table can be configured with a list of CAs that are trusted by the consumer. Suitable PKIs are currently set up by operators of the MCP.

As it is not always possible or intended to contact the CA for each message that is broadcasted by the service provider, the consumer which is typically a vessel at sea is recommended to update the local certificate store whenever in charge of a good connection. This aims to optimize the usage of the potentially limited bandwidth at sea.

If support metadata such as digital signatures needs to be transmitted with each dataset, additional changes need to be made to the transmitted data. An approach for that is shown in Figure 5: The Streamable_Exchange set complements the ServiceMetaData with dataset-specific information such as a digital signature that is directly derived from the dataset and therefore needs to be generated for each dataset individually. The Streamable_ExchangeSet is inspired by the SupportFile-section of the ExchangeSet model of the S-100 standard. It can easily be extended with additional dataset-specific metadata without making changes to the S-XXX data models.

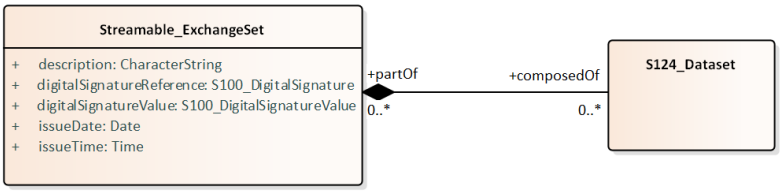


Figure 5: Streamable Exchangeset as (Signature-)Metadata-Container for S124-Datasets.

Commented [JM4]: Change to S-XXX

In S-100 section 15 the mechanism for assigning digital signatures to files is described. The approach described here makes use of its features (S100_DigitalSignature, S100_DigitalSignatureValue) but the signatures are assigned to datasets. In addition, to ensure the timeliness of S-100 datasets the data set must also contain a timestamp (i.e. date and time) so that the receiver of the dataset can check whether the data is up to date. Otherwise an attacker could eavesdrop and record a signed dataset and replay it later on, perhaps in a context when the data will cause misinformation or confusion. It is crucial that the signature spans both the dataset and the timestamp. Otherwise replay attacks will still be possible: The attacker could extract the signed dataset from the overall message and combine it with a timestamp valid for the intended time of replay. Also note that separately signing the dataset and the timestamp is not sufficient because the attacker could eavesdrop on any current message, extract its signed timestamp, and combine the current signed timestamp with an earlier signed dataset. Hence, it is crucial that S-100 dataset and timestamp are cryptographically bound together.

Moreover, it is crucial for security that the clocks of the sender and receiver are synchronized and that the time window in which the receiver accepts a message as valid is sufficiently precise. The first is easy to realize since in the maritime context we can assume that senders and receivers are equipped with GPS. The choice of the time window for acceptance is less straightforward to determine. Different types of datasets might come with

different margins of when it might become unsafe to accept and act upon them. In our context of IP-based communication we also must keep in mind that the routing of messages does not come with any real-time guarantees. We recommend that the time window will be defined specifically for each type of S-100 dataset following a safety impact analysis.

It is highly recommended to implement IP based communication in such a way that no TCP/UDP-Ports are opened at the service consumer side at any time. Also, the usage of HTTPS instead of HTTP as a communication protocol always has to be preferred as is fulfills all of the proposed recommendations. As an additional measure of security, a VPN network can be used.

3.4. USING MMS

The Maritime Messaging Service (MMS) is an information broker as part of the Maritime Connectivity Platform (MCP, see section 2.3) for exchanging messages via different communication channels in a maritime environment. It is a more comprehensive approach than web services because it supports multiple communication patterns. It provides an abstraction Layer from low-level communication technologies and is – as it uses a HTTP Interface – based on IP-technology. The MMS uses MRNs to identify and authorize service consumers and service providers. It acts as a middleware between the service consumers and services and supports features like group- or geocasting of messages. Furthermore, the use of MRNs and the architecture of the MMS solve the problem of switching between different communication technologies and allow a continuous communication.

To use the MMS as a service provider, an MRN for the service is required. The service must register its MRN in the Maritime Identity Registry (MIR) which is also a part of the MCP. The registration of the service's MRN in the MIR is required later to authorize messages from the service. The service consumer, which is typically a vessel, also must use a registered MRN to communicate with the service via the MMS. In application, messages are then transmitted via HTTP with custom headers containing the MRN of the message source and destination. A service consumer can obtain the MRN of a Service via the Maritime Service Registry (MSR) of the MCP. Figure 6 shows the message layout of a message that is sent via the MMS.

HTTP Header		
Field Name	Description	Example
srcMRN	MRN of a sender	srcMRN: urn:mrn:smart:service:instance:mof:S11
dstMRN	MRN of a receiver	dstMRN: urn:mrn:smart:vessel:imo-no:mof:12
HTTP Payload		
Message that a sender want to send. Ex) Hello World!		

Figure 6: Layout of an MMS-Message. [13]

As every message is directly addressed to its receiver, the Webservice only needs a single interface that receives the messages addressed to its MRN. Additionally, the service needs to send MMS-HTTP requests to the MMS broker, to answer a consumer's request. Since the service only has one MRN, the selection of the operation required by the client needs to be wrapped into the message payload. A simple json-like structure with the attributes: "operation", "type" and "content" that refer to the corresponding attributes of the S-100 service model is proposed. A basic message exchange with the wrapped operations is shown in Figure 7.

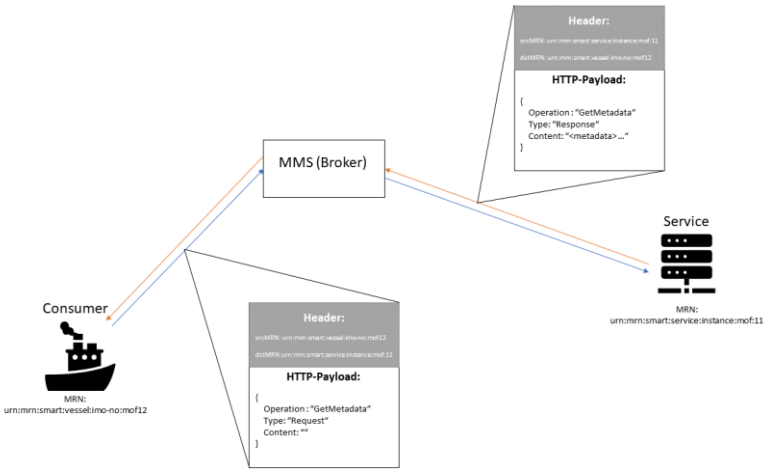


Figure 7: Simple exchange of messages using the MMS with a json-wrapper for the operations and types.

This usage of the MMS results in some changes that must be made to the instance of the S-100 model proposed in section 3.1 and 3.2: As the consumers can now be identified by their MRN, which is known to the service, the session operations are not mandatory anymore. However, these commands can be kept for keeping track of consumers interests to receive new datasets.

If the MMS is within the trust boundary of the client, the MMS could be used as a push-service gateway which enables the client to receive messages right after they arrive. When the MMS is trusted by service providers, the MMS could also be used as service-call proxy. Endpoint URLs of service providers do not need to be exposed to the client leading to better security. More on the MMS can be found in the high-level description document of the Maritime Messaging Service[1]. [13]

1 https://maritimeconnectivity.net/docs/MMS_Specification_0.8.3.pdf

ANNEX A IP BASED EXCHANGE OF MSI (S-124)

This section is an example on how to implement a reliable and efficient IP based service following this guideline.

1. NORMATIVE BACKGROUND

1.1. GMDSS

The Global Maritime Distress and Safety System (GMDSS) was designed to alert rescue authorities as well as near vessels in case of an emergency event. The goal is to provide help to the ship in distress as fast as possible. It is also used for the distribution of Maritime Safety Information (MSI) and was introduced by the SOLAS Convention in 1992. [8]

The GMDSS uses several different communication methods realized by satellite or terrestrial services. Radar transponders and emergency position indicating radio beacons are also used sometimes for locating survivors after an accident. Depending on the location of the ship in distress, different channels are used for an automated establishment of communication. [9]

The addition of IP-based communication to the GMDSS via satellite is a recent development and opens the possibility to reach ships in distant locations via an IP-connection [7]. As a part of GMDSS these services must fulfil the approved safety and security standards regulated by the SOLAS Convention too.

1.2. MSI

As defined by the Resolution A.705 by the International Maritime Organization (IMO), the Maritime Safety Information Service is

"[…] an internationally coordinated network of radio broadcasts containing information which is necessary for safe navigation, received in all ships by equipment which automatically monitors the appropriate frequencies and prints out in simple English only that information which is relevant to the ship". [2]

The MSI service is also a part of the GMDSS. In addition to providing information about navigational warnings, the MSI service is used for the distribution of meteorological forecasts and warnings or other safety-related information. The process of the distribution is visualized in Figure 8: The MSI is sent to an abstraction layer of the available broadcast service. Depending on the location of the affected ships either NAVTEX or SafetyNET is selected to transmit the information. The GMDSS-equipped ship needs separate equipment for receiving the MSI either by satellite (SafetyNET) or terrestrial (NAVTEX) communication channels. [3]

1.3. S-124 STANDARD

The **S-124 Standard** is a product specification of the S-100 family, managed by the International Hydrographic Organization (IHO). It standardizes the Navigational Warnings with a S-100 conforming Data Model. Its intention is to describe and encode navigational warning data for the usage in navigation. The standard aims at its usage in the above described mediums (NAVTEX and SafetyNET). [11]

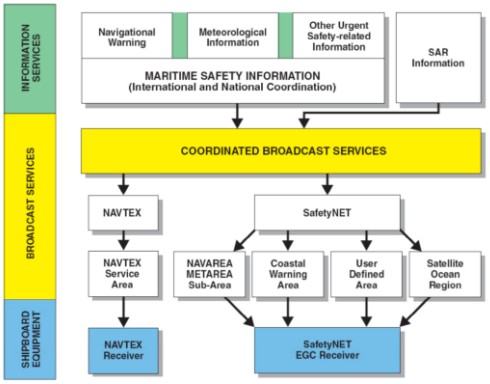


Figure 8: Today's Distribution of the MSI - Information, Broadcast Services and Shipboard Equipment [3]

2. REALIZATION OF A WEB SERVICE FOR MARITIME SAFETY INFORMATION

The following section describes the realization of a navigational warnings service. The service specification is an instance of the S-100 Service Data Model as introduced in section 2.2. Figure 9 shows the instantiation of the model. The ServiceMetaData provides the central structure and provides information about the service itself. The ServiceInterface in combination with the ConsumerInterface specifies the way consumers can interact with the service. The data model of the service can be described by the (XML-) Feature Catalogue of the S-124 Standard.

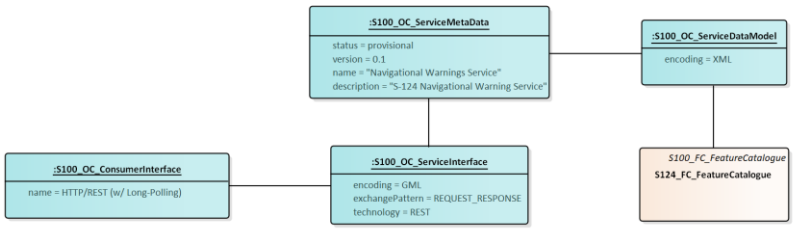


Figure 9: Service Specification of the Navigational Warnings Service

The operations of the service, which are also instances of the Service Data Model are illustrated in a separate diagram for the sake of clarity. Please note, that for demonstration we only implement a subset of the proposed operations in the S-124 Standard, section 11.2.2.

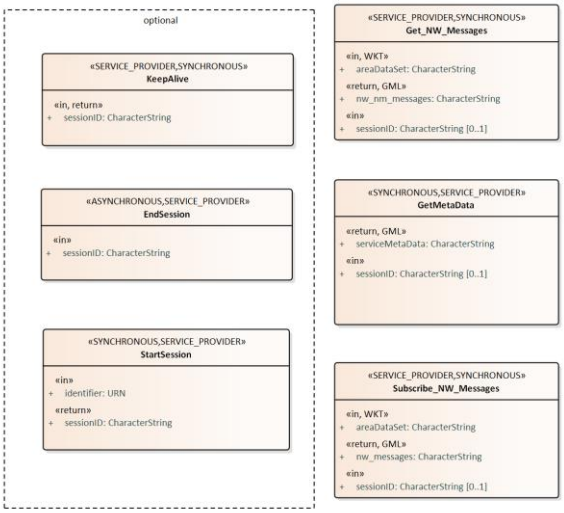


Figure 10: Available Operations of the Navigational Warning Service

The operations StartSession, EndSession, KeepAlive and GetMetaData are the minimal requirements for a S-100 conform **session-based service** specification as stated in section 14-9 of the S-100 standard. Sessions are utilized to keep an internal state of which consumer has received which warning. When querying the service again, the service can identify the consumer by the sessionID and only transmit new navigational warnings. This is an important factor to minimize the traffic and ensure that every consumer is aware of any relevant warnings.

Note that GetMetaData returns the ServiceMetaData instance, defined in Figure 9. Hence, GetMetaData is the only command that must be known to the consumer to discover the services capabilities.

Operations Description

StartSession, EndSession, KeepAlive and GetMetaData are implemented as described in S-100 section 14-9.

Get_NW_Messages

OPERATIONTYPE: SYNCHRONOUS

OPERATIONOWNER: SERVICE_PROVIDER

Role Name	Name	Description	Mult	Type	Direction	Encoding
Operation	Get_NW_Messages	Provides Navigational Warning messages for a specific area	-	-	-	
Parameter	sessionID	To identify the active session	1	CharacterString	in	
Parameter	areaDataSet	The area definition	0..1	CharacterString	in	WKT

Parameter	nw_nm_messages	The messages returned for the area	1	CharacterString	return	GML

Subscribe_NW_Messages

OPERATIONTYPE: SYNCHRONOUS

OPERATIONOWNER: SERVICE_PROVIDER

Role Name	Name	Description	Mult	Type	Direction	Encoding
Operation	Get_NW_Messages	Opens a long-polling Subscription. The service provides Navigational Warning updates as Response.	-	-	-	
Parameter	sessionID	To identify the active session	1	CharacterString	in	
Parameter	areaDataSet	The area definition	0..1	CharacterString	in	WKT
Parameter	nw_nm_messages	The messages returned for the area	1	CharacterString	return	GML

The implemented operations open the possibility for keeping track of the consumers by the service via the session id.

Communication Patterns

The described operations allow two communication patterns between service and consumer. The first pattern (shown in Figure 11) is a simple polling pattern. After starting the session and transmitting the metadata, the consumer can use the Get_NW_Messages command to receive all navigational warnings for the specified area. This could be for example a polygon containing the planned route. The Service can keep track of the messages that are known to the consumer via the session ID and only submit messages updates, when the client repeats the Get_NW_Messages command in fixed periods.

The second possible pattern is the long-polling pattern (shown in Figure 12). After opening the session and receiving the metadata, the consumer executes Get_NW_Messages once, to get the current set of Navigational Warnings. After that, the consumer opens a long-polling request with Subscribe_NW_Messages. This is a simple request that is answered by the server only after an update of the Navigational Warnings set is published. This solution ensures that the consumer immediately gets notified, when an update is available. That means there is no fixed time period which must pass before a new request is executed as realized by the polling pattern. After an update was received, the consumer directly starts a new Subscribe_NW_Messages command to wait for the next update.

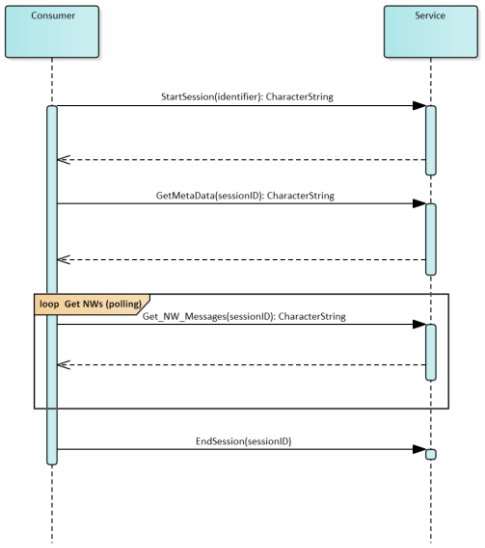


Figure 11: Polling of the Navigational Warning Messages

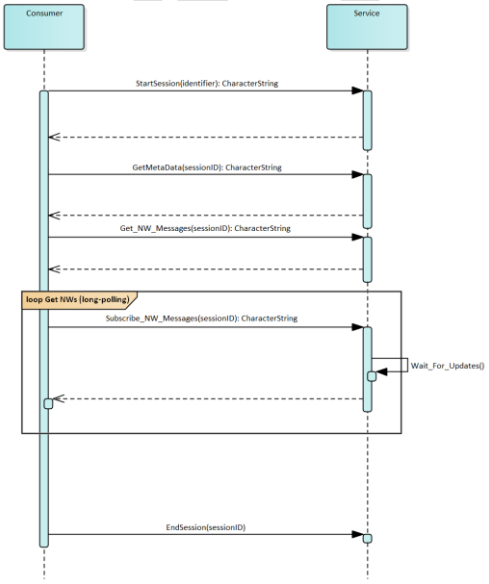


Figure 12: Long-Polling of the Navigational Warning Messages

Both patterns are mandatory for the service. Although the long-polling is preferable because of the immediate notification, it is not always possible to realize such a long lasting connection on the client side. Bad connections can be a cause of connections failures. Also, the polling method is an easy way to keep implementations of the consumer component simple.

Note that both patterns can also be used session-less (without executing the session commands) theoretically to provide a more lightweight communication pattern. In this case the service does not keep track of the transmitted warnings and the information state of the consumer.

3. SERVICE SPECIFICATION OF THE TECHNICAL SERVICE

Commented [JM5]: Appendix

The MSI technical service is specified in the following form according to G-1128.

3.1. SERVICE IDENTIFICATION

Name	Navigational Warning Service
ID	urn:mrn:iala:service:specification:msi:1230.1 (to be assigned)
Version	0.1
Description	This service delivers Maritime Safety Information (MSI) / Navigational Warnings to its consumers.
Keywords	MSI, maritime safety information, navigational warnings, s-124, warnings service
Architects	Axel Hahn, Sibylle Fröschle, Julius Möller
Status	provisional

3.2. OPERATIONAL CONTEXT

For a high-level description of the service see ANNEX A section 2.

Please note, that for demonstration we only implement a subset of the proposed operations in the S-124 Standard, section 11.2.2.

Requirements

Requirement Id	**NWS-RQ1**
Requirement Name	Get Datasets
Requirement Text	The service must provide a list of current navigational warnings.
Rationale	

Requirement Id	**NWS-RQ2**
Requirement Name	Get Metadata
Requirement Text	The service must provide metadata for the navigational warning datasets.
Rationale	

Requirement Id	**NWS-RQ3**

Requirement Name	Subscribe Warnings
Requirement Text	The service must provide an interface for subscription of navigational warnings. The service consumer needs to be notified when a new navigational warning is created.
Rationale	

Requirement Id	**NWS-RQ4**
Requirement Name	Message signing
Requirement Text	Navigational warning datasets must be signed.
Rationale	Security

Operational Nodes

Operational Node	**Remarks**
Vessels	Vessels at sea.
NW-Service providers	Service providers that publish MSI.
Certification Authorities	Certification Authorities that issue certificates to sign the datasets.

3.3. SERVICE OVERVIEW

The following diagram gives an overview of the main elements of the service.

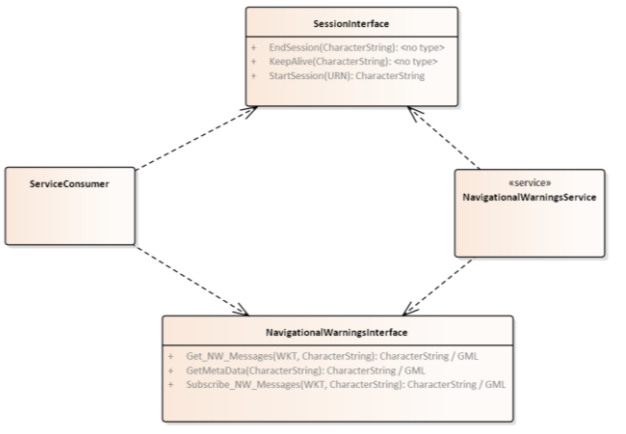


Figure 13: Navigational Warnings Service Interface Definition Diagram.

Service Interface	Role (from service provider point of view)	ServiceOperation
SessionInterface	provided	StartSession, EndSession, KeepAlive
NavigationalWarningsInterface	provided	Get_NW_Messages, Subscribe_NW_Messages, GetMetadata

3.4. SERVICE DATA MODEL

The service uses an external data model, which is described by the S-124 standard. Additions to the S-124 data model regarding security are discussed in section 3.3.

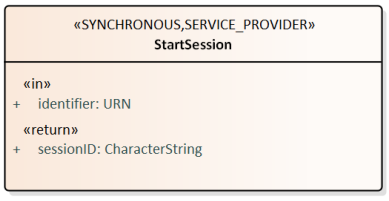
3.5. SERVICE INTERFACE SPECIFICATIONS

SERVICE INTERFACE SessionInterface

The session interface provides functionalities for starting, ending or keeping alive a session. Sessions are used for keeping track of the current information state of each consumer of the service. The use of sessions is not mandatory, but it can help minimizing the traffic between service and consumer.

OPERATION StartSession

Commented [JM6]: Use MRN instead of URN



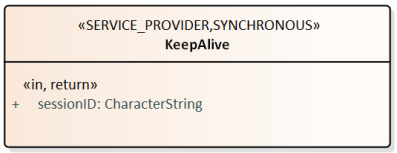
OPERATION FUNCTIONALITY: Starts a new session.

OPERATION PARAMETERS:

Parameter	Type	Direction	Description
identifier	URN	In	An URN (MRN) identifying the consumer of the service.
sessionID	CharacterString	Out	An ID to identify the new session.

Commented [JM7]:

OPERATION KeepAlive



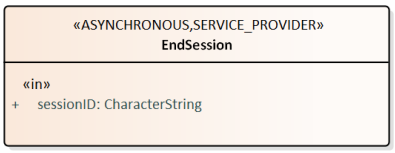
OPERATION FUNCTIONALITY: Keeps the current session alive. The service session time-out is reset.

OPERATION PARAMETERS:

Parameter	Type	Direction	Description

sessionID	CharacterString	In	The current session ID.
sessionID	CharacterString	Out	The current session ID.

OPERATION EndSession



OPERATION FUNCTIONALITY: Ends the current session.

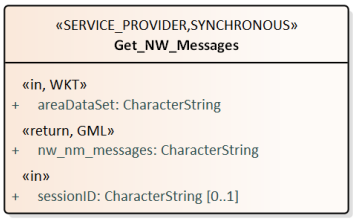
OPERATION PARAMETERS:

Parameter	Type	Direction	Description
sessionID	CharacterString	In	The current session ID.

SERVICE INTERFACE NavigationalWarningInterface

The NavigationalWarningInterface provides the core functionality of this service. Consumers can request a list of Navigational warnings or subscribe to navigational warning updates. An operation for obtaining MetaData is also available.

OPERATION Get_NW_Messages

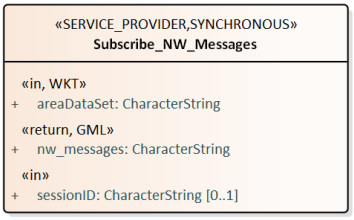


OPERATION FUNCTIONALITY: Returns a list of navigational warnings for a specified area.

OPERATION PARAMETERS:

Parameter	Type	Direction	Description
areaDataset	WKT	In	The requested area for navigational warnings.
sessionID	CharacterString	In (optional)	The current session ID.
nw_nm_messages	CharacterString	Out	A S-124 Dataset with navigational warning, encoded in gml.

OPERATION Subscribe_NW_Messages

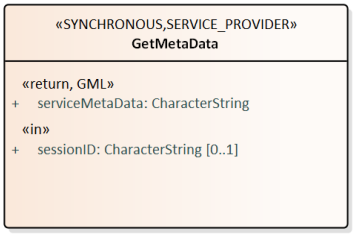


OPERATION FUNCTIONALITY: Subscription to updates on navigational warnings.

OPERATION PARAMETERS:

Parameter	Type	Direction	Description
areaDataset	WKT	In	The requested area for navigational warnings.
sessionID	CharacterString	In (optional)	The current session ID.
nw_nm_messages	CharacterString	Out	A S-124 Dataset with navigational warning, encoded in gml.

OPERATION GetMetaData



OPERATION FUNCTIONALITY: Provides Metadata for the service.

OPERATION PARAMETERS:

Parameter	Type	Direction	Description
sessionID	CharacterString	In	The current session ID.
serviceMetaData	CharacterString	Out	An S-100 (Part 14) metadata instance for the navigational warnings service encoded in gml.

3.6. SERVICE DYNAMIC BEHAVIOUR

The service dynamic behaviour is described in section **Error! Reference source not found.** ("Communication Patterns").

4. REFERENCES

[1] F. Bekkadal, 'Emerging maritime communications technologies', Oct. 2009.
[2] 'Resolution A.705(17) - Promulgation of Maritime Safety Information'. International Maritime Organization, 06-Nov-1991.

[3] 'Manual on Maritime Safety Information (MSI)'. International Hydrographic Organization, Jul-2009.
[4] G. Maral, J.-J. de Ridder, B. G. Evans, and M. Richharia, 'Low earth orbit satellite systems for communications', *International Journal of Satellite Communications*, 01-Jul-1991. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/sat.4600090403. [Accessed: 08-Jul-2019].
[5] H. Tsunoda, K. Ohta, N. Kato, and Y. Nemoto, 'Supporting IP/LEO Satellite Networks by Handover-Independent IP Mobility Management', *Sel. Areas Commun. IEEE J. On*, vol. 22, pp. 300–307, Mar. 2004.
[6] I. Maglogiannis, S. Hadjiefthymiades, N. Panagiotarakis, and P. Hartigan, 'Next generation maritime communication systems', *IJMC*, vol. 3, pp. 231–248, Jan. 2005.
[7] 'Inmarsat receives IMO approval for Fleet Safety', *Inmarsat*. .
[8] K. Korcz, 'GMDSS as a Data Communication Network for E-Navigation', *TransNav Int. J. Mar. Navig. Saf. Od Sea Transp.*, vol. 2, no. 3, Sep. 2008.
[9] E. Tzannatos, 'GMDSS Operability: The Operator-Equipment Interface', *J. Navig.*, vol. 55, pp. 75–82, Jan. 2002.
[10] 'THE S-100 UNIVERSAL HYDROGRAPHIC DATA MODEL', 2017. [Online]. Available: http://s100.iho.int/S100/. [Accessed: 05-Sep-2019].
[11] International Hydrographic Organization, 'IHO Geospatial Standard For Navigational Warnings - Special Publication No. S-124 (Working Draft)'. 31-Oct-2018.
[12] L. Jensen, 'Challenges in Maritime Cyber-Resilience', *Technol. Innov. Manag. Rev.*, vol. 5, pp. 35–39, Apr. 2015.
[13] Maritime Connectivity Platform, 'MMS: Concepts, Design and Usages'. .