e-NAV13 Information paper

Agenda item 10

Task Number 18

Author(s) / Submitter(s) Jens K. Jensen, Danish Maritime Authority

Information on draft e-Navigation technical infrastructure test-bed

# Summary

The ANNEX of this paper provides a draft of a technical infrastructure test-bed under consideration for the ACCSEAS project in the North Sea Region of Europe.

## Purpose of the document

The draft is provided as information and inspiration. It is a non-final document to inspire comments from the community. The considerations contained within are targeted to be input to the IMO e-Navigation correspondence group at a later date, after maturing the draft with comments from the communication working group.

The communication working group is requested to comment as appropriate.

# Background

The ACCSEAS project will deliver a regional test bed for e-Navigation services. To accommodate sea trials for different e-Navigation services, a test-bed infrastructure needs to be constructed. This infrastructure will be a test-bed in itself. Experience from these test bed trials are intended to be fed into the IMO e-Navigation process.

# Action requested of the Committee

The Committee is requested to note the document.

e-Navigation technical infrastructure test-bed

- supporting seamless information flow

# Introduction

This document is a conceptual description of the considerations on developing a technical infrastructure that supports seamless information flow, in order to support a test-bed for practical e-Navigation services. This technical infrastructure will constitute an architectural test-bed in itself.

We aim to introduce a high level abstraction of a technical infrastructure called ‘the e-Navigation cloud’, including generic and basic key elements, describing how they work together to provide seamless access to information by relevant actors:

* A cluster of servers (the maritime intranet) connecting the actors
* Security: Identity and Authentication of actors, Integrity and Confidentiality of information
* The Maritime Service Portfolio Registry – how to find relevant information services

An overview is given, aspects are described and some use cases provide illustrative examples of the envisaged goal.

Considerations are derived from ongoing work in the ACCSEAS project, an EU cofounded project in the in the North Sea Region.

# Background

The IMO e-Navigation Correspondence Group is currently processing the first steps of Formal Safety Assessment of prioritized 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
* S9 Improved communication of VTS service portfolio

A prerequisite for S2, S4 and S9 is a technical infrastructure that supports a seamless flow of information between the relevant actors, involved in providing or requesting reported information, presentable navigation information or information related to VTS services.

# Overview

The IMO overarching e-Navigation architecture dwells on:

1. **A Shipboard technical infrastructure**

Shipboard communication, navigation and display equipment is integrated to exchange information seamlessly, using harmonized data formats.

1. **A Shore based technical infrastructure**

Shore based information is made available through harmonized information services

1. **Communication**

A concept of generic communication links providing the logical connections that allow information flow between the Shipboard and the shore based systems - or at a higher logical level: The people operating these systems.

To provide efficient and secure delivery of an information service from one actor to another in this architecture, some an added level of detail is needed. This document will propose:

* **The e-Navigation cloud**
* How actors connect through a ‘maritime intranet’ inside the e-Navigation cloud – utilizing the same physical links that support access to any other service on the internet
* **A Maritime Identity Registry**
* How to identify and authenticate actors, addressing information security - integrity and confidentiality of information
* **A Maritime Service Portfolio Registry**
* How to locate services available
* **Communication Primitives**
* How to describe generic primitives of information exchange processes
* How to map this to existing instances of available communication links
* Identify relevant requirements for future maritime communication links

Table of content

[1 Introduction 1](#_Toc350845791)

[2 Background 1](#_Toc350845792)

[3 Overview 2](#_Toc350845793)

[4 The ‘e-Navigation cloud’ – and the Maritime Intranet 4](#_Toc350845794)

[5 Maritime identity Registry (Identity Broker) 6](#_Toc350845795)

[6 Maritime Service Portfolio Registry (Service Broker) 6](#_Toc350845796)

[7 Almanac 8](#_Toc350845797)

[8 Communication 8](#_Toc350845798)

[8.1 Voice communication versus data communication 8](#_Toc350845799)

[8.1.1 Voice communication 8](#_Toc350845800)

[8.1.2 Digital communication 9](#_Toc350845801)

[8.2 Messaging 9](#_Toc350845802)

[8.2.1 Acknowledge 9](#_Toc350845803)

[8.2.2 Broadcast/geocast 10](#_Toc350845804)

[8.2.3 Multicast 10](#_Toc350845805)

[8.2.4 Publish-subscribe 10](#_Toc350845806)

[8.2.5 Request-response 10](#_Toc350845807)

[8.3 Streaming 10](#_Toc350845808)

[8.4 Information Security 11](#_Toc350845809)

[8.5 Defining e-Navigation Messaging Primitives 11](#_Toc350845810)

[8.6 Mapping existing maritime communication links to the messaging primitives 12](#_Toc350845811)

[8.6.1 Internet access 12](#_Toc350845812)

[8.6.2 NAVTEX 12](#_Toc350845813)

[8.6.3 SafetyNet 13](#_Toc350845814)

[8.6.4 INMARSAT C 13](#_Toc350845815)

[8.6.5 LRIT 13](#_Toc350845816)

[8.6.6 AIS 13](#_Toc350845817)

[8.6.7 DSC 13](#_Toc350845818)

[8.6.8 VHF data 13](#_Toc350845819)

[8.7 e-Navigation cloud via internet connectivity – and other communication 13](#_Toc350845820)

[9 Geographical domain Awareness 14](#_Toc350845821)

[10 ShipboArd equipment 14](#_Toc350845822)

[11 Shore infrastructure 14](#_Toc350845823)

[12 Cost of communication 14](#_Toc350845824)

[13 Relationship between e-Navigation and GMDSS 15](#_Toc350845825)

[13.1 Terms of reference for e-Navigation 15](#_Toc350845826)

[13.2 Terms of reference for GMDSS review 15](#_Toc350845827)

[13.3 The need for coordination between these processes 15](#_Toc350845828)

[14 Illustrative usecases 15](#_Toc350845829)

# The ‘e-Navigation cloud’ – and the Maritime Intranet

It is envisaged that all actors interact under an umbrella we call the ‘**e-Navigation Cloud**’ – containing a M**aritime Intranet** based on well known TCP/IP technologies, a **Maritime Identity Registry** and a **Maritime Portfolio Registry**.

The physical link connecting each actor to the Maritime Intranet may be *any* internet service provider – and may change over time by least cost routing or manual selection. A ship may use a VSAT connection using one service provider at some stages of her journey, another service (for instance cellular mobile network or a HF data service) on other stages, or use a wifi or wimax connection in a port environment.

C:\Documents and Settings\obo-sfs\Dokumenter\Dropbox\e-Navigation\Projects\ACCSEAS\WP4\server.png

VTS, Ports,

etc.

Figure 1 – the E-Navigation cloud

Each actor – a ship, a VTS centre, a specific Port authority, MSI provider or other actor – is connected to the Maritime Intranet through a logical connection to one of the central servers in the e-Navigation cloud. The central servers cluster in the cloud will function as a redundant and transparent gateway for reliable and secure transfer of maritime data from one actor to others connected to the e-Navigation cloud.

For an actor to be entitled to participate in the e-Navigation cloud, the actor will need an authorized **Maritime Identity**, i.e. a certificate registered in a **Maritime Identity Registry**. Applying for a Maritime Identity may be considered similar to registering for a Maritime Mobile Service Identity (MMSI) or call sign, required to participate on maritime radio systems.

All actors in the e-Navigation cloud can be considered **service providers** as well as **consumers** **of** e-Navigation services. A ship may for instance be a consumer of a VTS e-Navigation service providing real time data on tide, current or wind for a particular area, planned time of lock or bridge operation or other services, while being a service provider of information to the VTS center on ship particulars or voyage related information such as actual draught and air draught, number of persons on board, previous and next port of call, estimated time of arrival at lock / bridge, etc.

Actors can identify services available through the Maritime Service Portfolio Registry – or rather through the ‘Almanac’ – a regularly updated local copy of the Maritime Service Portfolio Registry functioning as a ‘white pages’/‘yellow pages’ phonebook of where and how to contact other actors and which e-Navigation services they provide.

The central cluster of servers in the e-Navigation cloud will be aware of actors geographical position or area of responsibility at protocol level. This means that an actor can ‘broadcast’ information to an area, i.e. transmit information to actors listening in that area, and actors can ‘listen’ to an area – even though each actor does not know the geographical position, physical link or address of other actors. We call this ‘geocasting’ or ‘geo messaging’.

Figure 2 – Geocasting – enabled by geographical awareness at protocol level within the e-Navigation cloud

Mobile actors may frequently loose the online connection to the central servers of the Maritime Intranet in the e-Navigation cloud or switch to another physical link. The shipborne e-Navigation router and the central servers of the Maritime Intranet will act as buffers in these instances, and by techniques of store-and-forward and prioritized queuing ensure that messages otherwise lost during a communication outage are delivered when a new connection is initiated – highest priority first - and could ensure that bulky transfers are only announced available for download and not necessarily pushed over a low bandwidth / high cost communication link unless specifically requested.

Actors in the e-Navigation cloud may access other internet based services *outside* the e-Navigation cloud directly, utilizing the same physical links that support e-Navigation, but these services will not benefit from the buffering or priority queuing provided by the gateway servers inside the Maritime Intranet. Security restrictions may be imposed on workstations inside a certain part of the ships network (the navigation subnet) by the shipborne e-Navigation router, restricting access to services via the e-Navigation cloud only, while workstations on another part of the ships network may access services outside the e-Navigation cloud.

# Maritime identity Registry (Identity Broker)

All communicating actors participating in the e-Navigation cloud will need an authorized **Maritime Identity**, registered in a **Maritime Identity Registry**. Applying for a Maritime Identity may be considered similar to registering for a Maritime Mobile Service Identity (MMSI) or call sign, required to participate on maritime radio systems.

The Maritime Identity Registry will through one or more **Identity Brokers** maintain

* **Identities**
* **Attributes for identities**
* **Certificates for identities**

These Identities and their certificates will enable implementation of information security through **public key infrastructures** using security solution well known in many other domains, e.g. the financial sector, this addresses security concerns such as:

* **Authenticity**
* **Integrity**
* **Confidentiality**

Using well proven technology from other domains, it will be possible to ensure the integrity of a transmitted document, it originated from a particular ship, it was signed by a particular Master and was transmitted as encrypted, confidential information.

# Maritime Service Portfolio Registry (Service Broker)

The Maritime Service Portfolio Registry will contain

* A service specification catalogue
* A service instance catalogue

The specification of a service is located in the product specification part of the IHO S-100 GI Registry.

The Service Instance Catalogue is a register of provided services. The service instance catalogue links

* The Service
* The Service provider Identity
* The Area / leg / junction / point where this service is offered
* Metadata for the provided service (e.g. communication, quality etc.)

Service providers maintain their own information on provided services in the instance catalogue.

Service consumers can make queries for available services in the instance catalogue.

**Service catalogue, draft modelling**



*"Maritime Identifyer / Maritime Identity" concept* (as *correlated with "Voyage Number" concept* presented by **US**); the following reference document to be taken into account:

* + Discussion at AIS-ASM-Drafting Group at Technical Working Group at IMO NAV56 (2010)
  + COMSAR17 document(s)
  + Relevant IMO TWG document(s)
  + Relevant ITU-R WP5B document(s)
  + Relevant IEC document(s)

Modelling of (electronic) *“Services Almanach”* at IHO Registry (Product specification + feature catalogue) as a contribution to Common Maritime Data Structure (CMDS)

Consider using a “Uniform resource identifier” way of addressing services.

# Almanac

An offline version of a public part of the Maritime Identity Registry and Maritime Service Portfolio Registry may be downloaded by actors as an ‘Almanac’ – a ‘whitepages / yellowpages phonebook’ describing public, static attributes of actors, including public keys for use in establishing secure communication, and which different information services are available from which actors, in a particular area.

Using this Almanac, the identity of other actors, such as name, location and callsign of a VTS centre, or name, IMO number, MMSI number and callsign of a ship, is available together with a list of which services they provide.

The Almanac may function as an advanced phonebook for contact information via a multitude of communication channels, for instance providing a specific ships name, callsign, MMSI number for DSC calling or AIS messaging, e-mail address, phone number(s), INMARSAT terminal number or other contact information to a VTS centre, Port or MRCC – or vice versa.

Furthermore, the Almanac will enable a VTS centre to see which ships in it’s area of interest support a certain automatic reporting service. A ship will be able to see which service providers can deliver Meteorological/Hydrographic data relevant to it’s intended route. A ship will be able to see which information service are provided by a particular port. Even if the only service provided by a port is just a link to the ports own webpage, outside the e-Navigation cloud, the registration in the Almanac will provide a single point of locating professional maritime information services.

# Communication

Proposed e-Navigation services will put requirements on communication.

It is unlikely that a new, dedicated communication infrastructure with worldwide coverage will be developed to support e-navigation services in the short term. Rather e-navigation communication will utilize existing communications networks and possibly new evolving communication systems like VHF data.

Communication will be described in an actor and carrier-neutral manner. That is, communication will not be initially restricted by existing communication systems. That is not to say however, that proposed services will not need to be evaluated against existing communication systems. On the contrary - this evaluation will provide insight into desirable requirements for future evolving communication systems.

Communication can be divided into different types of communication. E.g., one-way or two-way, broadcast, addressed, and acknowledged or un-acknowledged. Different kinds of services may put different requirements on communication links. Below different types are described that can be used to describe the needs of particular services.

## Voice communication versus data communication

### Voice communication

Voice communication is prone to language barriers – a frequent source for misunderstandings, however a large portion of maritime communication is today reliant on voice communication over two-way radio telephone (VHF, MF or HF) – or via satellite (or in coastal navigation via cellular mobile network) connections to the Public Switched Telephone network (PSTN).

Radio telephone equipment support broadcasts as well as actor-to-actor communication.

The interoperability of radiotelephone communication equipment is primarily achieved through standardization based on IMO performance standards related to GMDSS carriage requirements, executed through related IEC / ITU technical standards.

Interoperability of voice over PSTN is entirely achieved through industry standards – but requires availability of a telephone dictionary to achieve contact with any specific actor, and is restricted to point-to-point communication.

### Digital communication

e-Navigation is defined as “…the harmonised collection, integration, exchange, presentation and analysis of maritime information onboard and ashore by electronic means to enhance berth to berth navigation and related services, for safety and security at sea and protection of the marine environment”.

e-Navigation is thus a move towards digital data exchange, supporting automatic information transfer through harmonized digital data formats containing automatically displayable or processable information, rather than manual information transfer via voice telephony hampered by language barriers or manual information transfer between non compatible systems or data formats.

## Messaging

A large portion of information exchange in e-Navigation can be described as passing a **Maritime Information Message (MIM - a package of digital information)** from one actor to another, or to several other actors. A shore authority promulgating Maritime Safety Information as a broadcast is one example – a vessel providing an early notice of arrival to a port is another.

### Acknowledge

In many two-way communication protocols, the transmission of an ‘acknowledge’ is an integral part of point–to-point low level transmission protocols, ensuring that the message is successfully delivered between the transmitting and receiving transmission equipment. Using a TCP connection an IP network provides acknowledge mechanisms at transmission link level which ensure that an error indication can be generated if the message was not successfully delivered over the transmission link. Transmission of an addressed Application Specific Message via AIS is another example providing acknowledge at transmission link level.

An acknowledge mechanism can also be implemented at application level, requesting the receiving application (or the user) to acknowledge reception. Requesting a delivery confirmation – or a ‘read’ confirmation from recipients of an e-mail – are examples of such an application level acknowledge.

### Broadcast/geocast

A message can be broadcast by a particular or several physical communication systems, covering a desired geographical area, assuming that the intended recipients are listening. Today this is typically a one-way, non-acknowledged action. MSI broadcast via NAVTEX or SafetyNet are typical examples.

If the geographical location (or area of interest) of actors are known, a bradcast could be implemented as a *geocast*, by selecting a group of relevant actors by area of relevance for the information broadcast, transmitting the messages to each actor individually (multicast, see below) using one or more available communication links.

Broadcast / geocast could – in principle – request an ‘acknowledge’ by recipients, if a two-way communication link is available.

### Multicast

Multicast means delivering a message to a selected group of relevant actors.

This may be achieved as a broadcast, including the list of targeted actors identities in the message broadcast itself, assuming that all relevant actors are listening to the communication link used for the broadcast.

Multicast will however more likely be achieved by transmitting the relevant message to each actor individually, using one or various available communication links. Using Application Specific Messages transmitted via AIS in an addressed mode would be a typical example, providing an automatic acknowledge at the physical link level.

A multicast message may request an ‘acknowledge’ by recipients.

### Publish-subscribe

Messages may be published by making them available at a particular service point where interested actors can subscribe to a multicast service. New messages will thus be pushed to those actors, who subscribed to the service at the time of publication.

### Request-response

A particular actor requiring a specific bit of information from a specific actor or group of actors, may initiate a request to a webservice at that particular (group of) actor(s), and await response. This requires two-way communication capabilities.

To be further elaborated - Capability interrogation…?

## Streaming

To be further elaborated

* There may be a need for streaming E.g. IVEF or AIS stream

## Information Security

Addressing reliability and integrity of information distributed through the e-Navigation cloud is the core of one of the selected focus solutions for the e-Navigation process.

Information Security covers information

* Authenticity
* Integrity
* Confidentiality

Handling of information security in e-Navigation does not require new technology. The whole world is relying on the use of secure information transfer for financial transactions, and a lot of this over the public internet via secure connections using well proven technologies.

To be further elaborated - see: <http://www.brighthub.com/computing/smb-security/articles/31234.aspx>

Introduce X509 certificates and public key infrastructures.

Solutions used in many domains, e.g. the financial sector with comparable security needs.

How the security issues can be solved

* Signing/hashing for authenticity and integrity
* Encryption for confidentiality (TLS)

Impact on bandwidth usage…

## Defining e-Navigation Messaging Primitives

Within the e-Navigation Cloud we consider that maritime messaging can be abstracted into one or more of the following primitives:

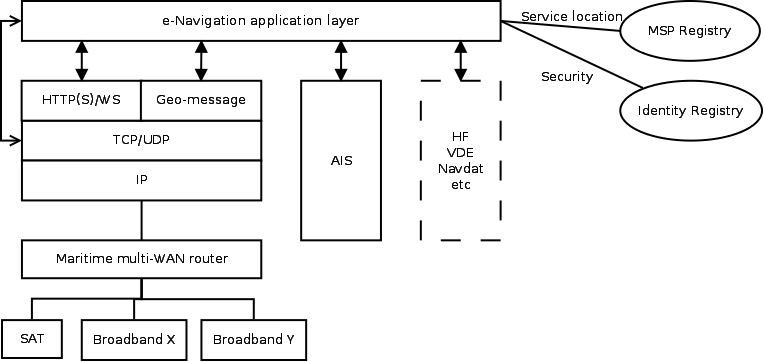
**send(receiver, message) → ack**

**broadcast(message, area)**

**listen(area) → message**

For the infrastructure test-bed we propose the definition of a **Geo-messaging protocol:**

* Messaging protocol on top of TCP/IP that allows to geocast to actors with a specified area
* Can mimic existing communication solutions and possible future solutions
* Permits the test-bed evaluation of how existing and possible future communication solutions can be used
* The solution has no geospatial restrictions
* Existing well known messaging protocols can be extended with geospatial awareness to obtain solution



## Mapping existing digital maritime communication links to the messaging primitives

Specific communication systems will incur limitations:

* Bandwidth (message size)
* Range (area)
* Abilities (push, two-way, addressing, etc)

### Internet access

Internet access will provide for any of the messaging primitives via each actor maintaining a connection to the Maritime Intranet. This will include the options for ensuring information security (authentication, encryption, etc.) This will be the primary carrier of ship-shore communication in the infrastructure test-bed.

Shorebased users may achieve broadband internet access via many different technologies, usually providing fixed access with high availability and high bandwidth and possibly a fixed IP-address.

Mobile actors such as ships may achieve internet access via several satellite services, GSM, 3G, 4G or other cellular dataservices, Wifi/Wimax or other mobile technologies, depending on their current area of operation and availability of services. The connection may change frequently and the bandwidth available, quality and cost may vary greatly depending on service availability. The IP-address of the connecting router may also typically change dynamically. Some areas of operation of mobiles may be outside coverage of any of the subscribed internet services.

### NAVTEX

NAVTEX is a broadcast system only, and part of the GMDSS. The system only supports infrequent broadcast of short human readable text messages, and is not considered useful for the promulgation of machine readable data.

A similar, but higher bandwidth system called NAVDAT using the same frequency band and potentially reusing the same transmission sites, has been proposed. This system could support the promulgation of machine readable data (Application Specific Messages, similar to AIS) , but would require new receivers on vessels.

Neither of these systems support acknowledge of reception. The broadcast area is determined by the coverage of each transmitter.

### INMARSAT C

Satellite-Telex. Allows two way text messaging between satellite terminals. INMARSAT-C is an approved part of the GMDSS.

### SafetyNet

SafetyNet is an INMARSAT-C based broadcast system, providing similar broadcast capabilities as NAVTEX, but complete coverage of the A3 area (global except for the polar regions) as part of the GMDSS.

### LRIT

To be further elaborated

### AIS

To be further elaborated

May provide two-way link via ASM, but not IP connectivity

### DSC

To be further elaborated

Part of GMDSS – distress alerting and selective calling – useful for initiation radio telephone call

### VHF data Exchange

To be further elaborated

### Other…

To be further elaborated

## Quality assurance of communication

Acknowledge mechanisms are important, if quality assurance of information delivery is required. In principle, acknowledge mechanisms allow quality assurance of

* The reception of a transmitted message itself
* The involved communication links and service providers
* The communication equipment onboard ships

If Maritime Messaging was delivered via the geocasting approach, through various suitable communication links supporting acknowledge mechanisms, the certainty of delivery for a message targeted a particular area would be well known, the quality of utilized communication links and service providers could be measured, and the quality of communication equipment onboard ships could be determined.

This is currently not feasible using several GMDSS approved broadcast systems such as NAVTEX or SafetyNet.

## Separating communication within the e-Navigation cloud from other communication

For actors having an internet connection, access to services via the Maritime Intranet is quite straight forward. Actors in the e-Navigation cloud may also access internet services outside the e-Navigation cloud directly, utilizing the same physical links.

### Security

To protect the navigation equipment on ships bridges from internet threats, security restrictions may be imposed by the shipborne e-Navigation router (firewall), to ensure that workstations inside a certain part of the ships network (the navigation subnet), is restricted to accessing services inside the e-Navigation cloud only, while workstations on another part of the ships network may have full access to services outside the e-Navigation cloud for crew / passenger entertainment or other purposes.

### Cost

To be further elaborated

Separation of GMDSS, e-NAV and routine commercial or entertainment communication.

Can cost of e-Navigation communication versus other traffic be separated?

Basic Comms available as part of GMDSS ?

IP / non-IP communication

# Relationship between e-Navigation and GMDSS

## Terms of reference for e-Navigation

## Terms of reference for GMDSS review

## The need for coordination between these processes

# Geographical domain Awareness

The Geocasting approach requires geographical awareness about the listening area of actors.

For mobile actors, geographical domain awareness to support geocasting could be implemented like this:

1. Actors should maintain a connection to the Maritime Intranet, providing the Maritime Intranet with the current IP address, to enable seamless availability of information services to and from the mobile actor. This connection should be reconfirmed regularly or reconnected, if the communication link and thus the IP address changes, and include a regular update of the mobile units listening area. One easy way would be by providing own current position and a listening radius.
2. In order not to impose a need for very frequent additional updates, and thus to limit the bandwidth consumption of the communication links, AIS data, SAT-AIS (or existing LRIT data) could be utilized to update geographical awareness at protocol level of the Maritime Intranet.

This would enable a Global Identification and Tracking (GIT) service to be an integrated service within the Maritime Intranet. This GIT service could fulfill the performance specification of the LRIT and access to the GIT service could be governed by the same Data Distribution Plan as developed for the LRIT.

# Shipboard equipment

To be further elaborated

Brief examples of what is envisaged in ACCSEAS project:

We will have an e-Navigation prototype display system on the bridge.

It will as a minimum connect to

* Communication equipment (providing IP connectivity – via e-Navigation router)
* AIS transponder
* Multi source positioning device

Generic communication interface that will use appropriate carrier based on availability, reliability, bandwidth, cost etc.

Describe requirements for e-Nav router – firewalling of nav /admin workstations, connection to other sensors / comms, allowing the sharing of IP connectivity with other leisure or commercial use of same shared physical link.

# Shore infrastructure

To be further elaborated

Availability, reliability, ITIL

Show shore-based systems of different stakeholders.

Redundancy

# Illustrative usecases

Describe what we envisage to support with the technical infrastructure test-bed - the end goal – through use cases:

Automated reporting – early notice of arrival to port / police / other authorities including crewlist, etc., Port responding with predicted berthing availability, etc.

MSI promulgation

Ship requesting weather optimized route from selected service provider

MRCC investigating SAR capabilities of vessels in vicinity of ongoing SAR operation

VTS service interaction without language barriers of voice communication