

Appendix E

to the Tender Specifications

Overview of Applications

Sub-Appendix E.1 to Appendix E of the Tender Specifications

SafeSeaNet Overview

V1.0

Date: 18/04/2016

Document History (if needed)

| Version | Date | Changes | Prepared | Approved |
|---------|------------|-----------------|----------|----------|
| 1.0 | 18/04/2016 | Initial version | EMSA | |

Table of Contents

| | |
|--|----|
| 1. Introduction | 5 |
| 2. Objectives of SSN and its network organisation..... | 5 |
| 3. Mandatory system functionalities..... | 6 |
| 4. Additional system functionalities | 7 |
| 5. Information exchange mechanisms..... | 8 |
| 5.1 Message based mechanism | 9 |
| 5.1.1 Notification:..... | 9 |
| 5.1.2 Request and response: | 9 |
| 5.2 Distribution for Incident Reports | 10 |
| 5.3 Streaming mechanism:..... | 11 |
| 6. Cooperation with Other EU Systems | 11 |
| 7. SSN Applications | 13 |
| 7.1 SSN release in production at the time of launching the procurement (SSNv3.0) | 14 |
| 7.2 SSN baseline version for the procurement (SSNv3.2) | 15 |
| 7.2.1 SSNv3.1 (target GO LIVE – July 2015)..... | 15 |
| 7.2.2 SSNv3.2 [target GO LIVE – October 2015]):..... | 15 |
| 7.3 System performance requirements | 16 |
| 7.4 Other pertinent information concerning SSN data quality | 19 |

List of Tables

Table 1 SSN mechanisms for information exchange 9

List of Figures

Figure 1 SafeSeaNet system 6

Figure 2 Sequence diagram of notification, request and response mechanisms 10

Figure 3 Interfaces of the central SSN system with other EU systems 12

List of Abbreviations

| | |
|--|--|
| | |
| | |
| | |

1. Introduction

SafeSeaNet (SSN) is an EU vessel traffic information exchange system between designated participants. This annex to the tender specifications provides the objectives of SSN, a system overview and the main flows of information, system functionalities and actors. Technical specifications are developed in separate technical documents adopted by the SSN group.

2. Objectives of SSN and its network organisation

The objective of the SSN system is to support EU and MS activities with respect to maritime safety, port and maritime security, marine environment protection and the efficiency of maritime traffic and maritime transport.

The operation of SSN involves a number of entities or users at regional, national and local level. These can vary from those in the shipping industry (ships' masters, agents or operators) to national administrations (such as port authorities and coastal stations, Port State Control officers, SAR centres, VTS, ship reporting systems, pollution response bodies, etc.).

Through sharing and distributing maritime related information, the SSN system supports users at EU and MS level in achieving the objectives set out in the Article 1 of Directive 2002/59 (as amended). SSN facilitates the exchange of information in electronic format between MS and to provide the Commission with the relevant information.

It is composed of a network of national SSN systems in Member States and a central SSN system acting as a nodal point (see figure 1 below). The central SSN system has a number of interfaces available thereby allowing optional/alternative means of information exchange with Local Competent Authorities (LCA) and National Competent Authority (NCA) at MS level (see figure 1 below)

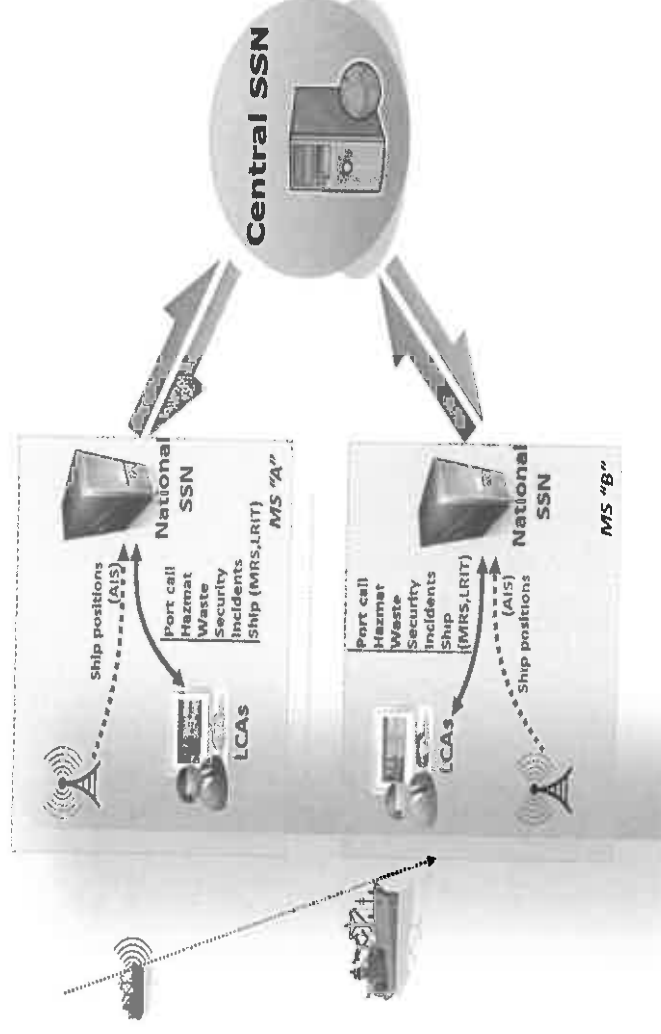


Figure 1 SafeSeaNet system

- LCAs may be data providers as well as data users at local level.
- National SSN systems and/ or National Single Window (NSW) systems established in accordance with Directive 2010_65_EU provide information to the central SSN system in the form of notifications. Authorised users within the SSN Community can retrieve information related to these notifications. The central SSN system locates and retrieves this information and provides it to the data user.
- While the central SSN system stores some information which enables rapid, effective response to users' requests, detailed information may be stored at national level. When the notifiable information is changed by the data provider, a notification is provided to the central SSN system, and information is updated accordingly.

3. Mandatory system functionalities

SSN, at its national and central levels, is built upon mandatory system functionalities which are essential to the normal operation of the system. The mandatory system functionalities are the sending, receipt, storage, retrieval and exchange of information required by the SSN legal framework. SSN shall support the exchange of the following information:

- Port call information:
 - ✓ Pre-arrival information sent to ports 72 and 24 hours in advance from estimated arrival to the Port of Call
 - ✓ Actual arrival and departure notification
 - ✓ Notifications on carriage of dangerous or polluting goods (sent or pre-arrival and departure stages)
 - ✓ Notifications on waste/ security (sent at pre-arrival stage of the call, at least 24h prior to the estimated arrival.;
- Incident information:
 - ✓ Information on accidents and incidents which have occurred at sea;
- Position information: AIS, MRS and LRIT flag state information;

The information collected and exchanged through SSN must comply with the quality and performance standards defined in the Interface Control and Functionalities document (IFCD) agreed with the MS and in the relevant technical and operational documentation.

4. Additional system functionalities

SSN provides for additional functionalities in support of its main operations. These functionalities are not considered mandatory, therefore their unavailability would not affect the overall service level of the SSN system.

The additional system functionalities are related but not limited to:

- statistics;
- graphical display of information;
- SAT-AIS position information;
- background information display (nautical charts, etc.);
- system monitoring tools;
- secondary or reference data sources (Location codes, SSN users contact details, ship particulars, special lists of ships).

Subject to approval by the SSN group, further functionalities may be incorporated in the SSN system.

5. Information exchange mechanisms

The central SSN system provides different alternative mechanisms to the national SSN systems in order to enable the mandatory exchange of information. These are:

- **Message-based mechanism:** A mechanism which allows individual messages to be exchanged between the national and central SSN applications. The messages (in XML format) fulfil the needs of both data users and data providers (e.g. proprietary protocol, web-services, etc.). This mechanism supports the notification, request and response functions for all types of SSN information.
- **Streaming mechanism:** A mechanism which enables the constant flow of AIS data (based on predefined criteria) from the national systems to the central SSN system (either directly or via an AIS regional server). This mechanism is currently only available for the provision of AIS information and is an alternative to the message-based mechanism.
- **Central SSN Web browser-based mechanism:** This mechanism is available for requesting information and providing Incident Reports, and may be used to provide other information as a back-up solution in the case of failure of the national or local SSN systems. It is also available for system administration. The central SSN Web browser-based mechanism offers two interfaces:
 - **Textual interface:** This provides direct access to the central SSN system using a textual layout;
 - **Graphical interface:** This uses geographical information system technology to provide access to ship positions enriched with the data in the central SSN system (information on pre-arrival, arrival, Hazmat cargo, incidents, etc.), thus creating a vessel traffic image showing movements in near-real time.

The table 1 below lists the mechanisms available for exchanging information via the central SSN system.

| SSN Mechanisms for information exchange | Message-Based | Streaming | Web Browser-Based | |
|---|----------------|-----------------|--------------------|--|
| | | | Textual interface | Graphical interface |
| Available for: | Data Providing | All information | Ship AIS positions | Incident, exemptions information and In case of failure as a backup mechanism for 72 hours pre-arrival, ATA and ATD |
| | Data Request | All information | All information | N.A. |

| | | | | | |
|--|-------------------|------------------|---|------------------|------|
| | Data Distribution | Incident reports | Ship AIS positions enriched with SSN data | Incident reports | N.A. |
|--|-------------------|------------------|---|------------------|------|

Table 1 SSN mechanisms for information exchange

5.1 Message based mechanism

5.1.1 Notification:

- The data provider gathers the necessary information to be reported.
- This information is sent to the national SSN system.
- The national SSN system compiles the message in the SSN compliant format and forwards it to the central SSN.
- On receipt the central SSN determines whether the notification is well formed:
 - If well formed, the notification is indexed in the server.
 - If not well formed, the notification is rejected by the central SSN system and the national SSN system should resend the corrected message.

5.1.2 Request and response:

- The data user requests information from the national SSN system.
- When the information cannot be provided nationally, the national SSN system forwards the request to the central SSN system.
- The central SSN system verifies the access rights of the user, and subject to acceptance, proceeds as follows:
- In the case of information stored at central SSN level, the information is sent back to the requester (via national SSN system).
- In the case of information is available in MS national servers through document download, the central SSN system retrieves directly the document and forwards it to the requester (via the national SSN system).

- In the case of information is available upon request only, the central SSN system forwards the request to the national SSN system where the information is located, which, may, in turn, forward it to the data provider that owns the information. The data provider that owns the information then responds with detailed information which is transmitted (via the national SSN system) back to the central SSN system for forwarding to the data user.

A sequence diagram describing the above mechanisms is provided in the figure below.

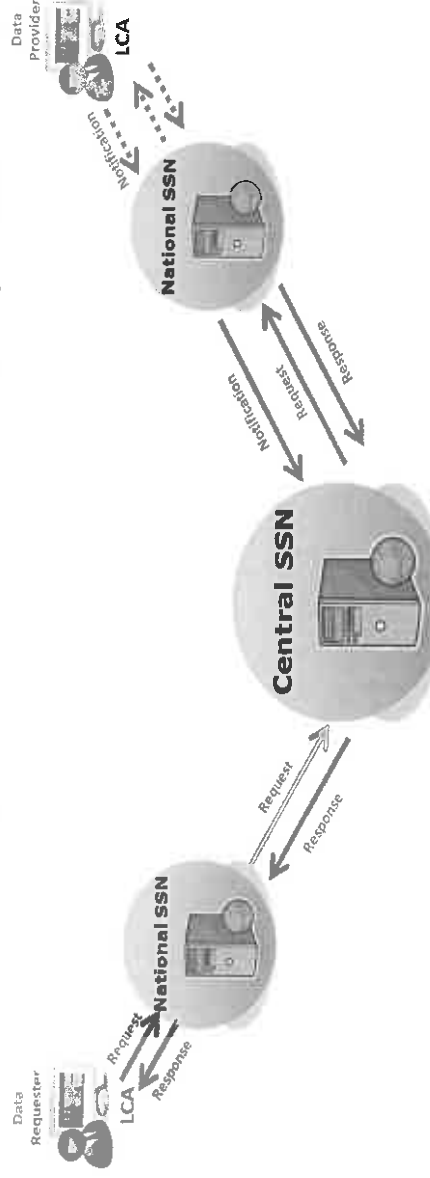


Figure 2 Sequence diagram of notification, request and response mechanisms

5.2 Distribution for Incident Reports

- The *data provider* can define the list of recipients for distributing Incident Reports via the national SSN system (in XML) or via the central SSN web interface.
- The central SSN system verifies the access rights of the user and distributes the Incident Reports in accordance with the distribution list.
- Incident Reports can be distributed via XML, emails or both depending on the user configuration as follows;
 - If the user is an XML recipient, the central SSN forwards the full information to the national SSN system;
 - If the user is an email recipient, the central SSN distributes emails including basic information about the incident. The full details can be retrieved by the user through the central SSN web interface.
- The central SSN logs the distribution status and activates a failure management procedure in case of a failure in the distribution.

5.3 Streaming mechanism:

- Provision of AIS data
 - SSN is equipped with a streaming mechanism which enables the near-real-time exchange of ship positions obtained via the AIS network. This exists at the regional and national levels in order to enable national SSN systems to provide AIS information to regional servers and/or the central SSN system.
- Distribution for Ship AIS position enriched with SSN data
 - The streaming mechanism supports the distributing of AIS information enriched with SSN data in accordance with the access rights of the user.

6. Cooperation with Other EU Systems

Information exchanged between the central SSN system and other EU systems must respect the access rights policy defined in Chapter 3 of the SSN IFCD (refer to Appendix C of this annex).

The cooperation between the central SSN system and the other EU systems described above can be summarised as follows.

- **SSN/THETIS:** The central SSN system provides to the THETIS system information received from national SSN systems on the port call (pre-arrival 24 hours, arrival, and departure), waste and security information for ships calling at EU ports and anchorages.
- **SSN/CSN:** The central SSN system provides ship positions and identifiers (transmitted by national AIS networks) to the CSN system in order to assist in the identification of vessels and possible polluters (within a limited timeframe and area).
- **SSN/EU LRIT CDC**
- **SSN/EU LRIT Ship Database:** The EU LRIT ship database provides the central SSN system with ship information in order to validate the ship information held in the SSN system
- **SSN/CECIS:** The central SSN system provides incident reports of type POLWARN and POLINF to CECIS

The technical implementation to allow for the full distribution of LRIT data to MSs through SSN is under development.

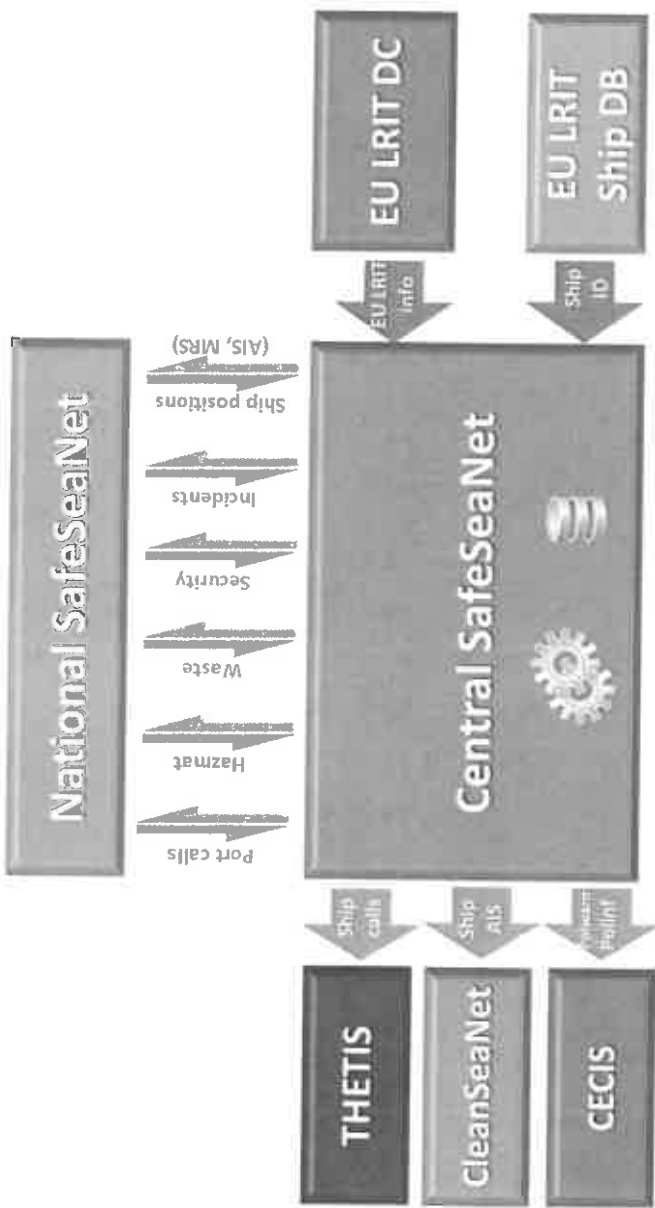


Figure 3 Interfaces of the central SSN system with other EU systems

7. SSN Applications

The architecture of the Central SSN system at the time of launching this procurement includes several applications (either already in operation/production or under development). The applications are designed/implemented with Service Oriented Architecture logic.

The SSN applications are:

- **The European Index Server (EIS)**

Through this application certain core services are implemented e.g.

- ✓ **The SSN textual interface, t**
- ✓ **The XML/ SOAP messages interface,**
- ✓ **The Central Ship database (CSD)** containing reference data for ship identifiers and ship particulars
- ✓ **The Central Organisation Database** containing reference information for maritime Authorities
- ✓ **The Central Location Database containing reference location (e.g. ports) information.**
- **The SSN Tracking Information and Real Time Exchange System (STIRES) module**

Through this application certain core services are implemented e.g. the SSN Graphical Interface (SSN GI) and SSN Streaming Interface – SSN SI)

Important note:

This applications shall be deprecated within 2016 and replaced by STAR (refer to the Annex G of the tender specifications for the anticipated evolution of EMSA maritime applications architecture

- **The SSN accident module**

SSN uses the single sign on platform of EMSA (**Oracle Identity Management** suite) for user access authentication. The EIS application comprises several **SSN management utilities** (made available as distinct deployables) enabling provisioning of user access rights and management of the reference and operational data in the SSN system. User are accessing SSN via the **Maritime Application Portal** a LifeRay-based application used by all the critical operational services currently managed by EMSA.

The GIS capabilities for SSN GI mentioned above are currently based on the ESRI ArcGIS platform. The visualisation of Electronic nautical charts (ENCs) is implemented as an horizontal web map service fetching ENCs from the Agency's chart database (licensed by Jeppesen). For the verification and validation process of ship particulars, a link to the Agency's MARINFO database has been implemented (utilising store procedures). The reference databases are exposed taplications external to SSN via XML/ SOAP-based web services. At the time of the procurement the CSD is exposed to MS in the framework of a pilot project while COD and CLD are exposed only to other EMSA applications.

7.1 SSN release in production at the time of launching the procurement (SSNv3.0)

At the time of launching the procurement the release of SSN available in production is the one identified as "SSNv3.0²". The release complies with the data exchange specifications listed in the XML Reference Guide v3.02 and meets the legal requirements of Directive 2002/59/EC establishing a Community vessel traffic monitoring and information system as amended by the Directives 2009/17/EC as well as the legal requirements of the Directive 2010/65/EU (on reporting formalities for ships arriving in and/or departing from ports of the Member States

The following new features of SSN v3 are supported:

1. Creation of additional user profiles: Enables SSN and national administrators to create the National Single Window Authority and assign to users permissions associated with the provision/request of waste and security information,
2. Option to notify SSN using the revised PortPlus² notification that includes Waste, Security and Hazmat information,
3. Option to notify SSN of exemptions using the new exemption notification,
4. Option to query SSN using the new ShipCall request / response mechanism³,
5. The new MRS protocol including:
 - a. A revised Ship MRS notification;
 - b. A revised Ship request/response mechanism;
6. A mechanism to support a transition period from SSN v2 to SSN v3 protocol (refer to SSN Group paper SSN 22.4.2):
 - a. PortPlus notifications and ShipCall request / response
 - b. Ship notifications and Ship request / response
7. Improvement of the SSN Textual Interface and Graphical Interface in relation to the changes mentioned above and the Incident Reports function.
8. Central Ship Database

Detailed design information concerning this release is available in the Appendices of this Annex A .

² The Portplus message was initially introduced in SSN v2 back in 2011 and is used as well for the notification of pre-arrival notices (72h/ 24h) and actual arrival/ departure notices.
³ This mechanism is utilised in SSN for the exchange of voyage/ shipcall information notified to SSN using Portplus. It was initially introduced to the system with SSNv2.

7.2 SSN baseline version for the procurement (SSNv3.2)

Bidders should note that at the time of signature of an FWC based on this tender the baseline SSN version in production shall be **SSNv3.2**. Below is outlined the context of the two releases anticipated to enter into production during the time this tender shall be still in the evaluation stage:

7.2.1 SSNv3.1 (target GO LIVE – July 2015)

- The release shall include:
 - a. SSN CECIS interface
 - b. Improvements on the IR protocol for the SSNv2 –SSNv3 transitional period¹

7.2.2 SSNv3.2 [target GO LIVE – October 2015]]:

- The release shall include:
 - a. Upgrades enabling the integration of Shore-based traffic monitoring infrastructure database (STMID) in the COD.
 - b. Implementation of a WFS that COD shall expose to SEG enabling the visualisation of the STMID data in SEG..
 - c. Implementation of a WFS that the Central Geographical Database (CGD) will expose for enabling registering a reference descriptor for geographical areas in the COD (for STMID purposes).
 - d. Improvements in the web interface of the CSD (for improved usability and alignment with the System Interface Guide agreed for the MS CSD pilot).
 - e. Amendment of the CSD business logic enabling registration of ship particulars delivered via PortPlus and AIS messages into the CSD.
 - f. Amendment of EIS application logs to register all types of http errors.
 - g. Improvement of labelling the fields in the SSN web interface forms concerning ship voyage details, MRS and incident details.
 - h. Implementation of data archiving for SSN EIS data (voyage/ ShipCall, Incident, MRS) including changes in the SSN EIS business logic for accepting shipcall updated where data was registered in the system more than a year in the past.
(For the following items the Release version (SSNv3.2 OR ssnV3.3) is to be confirmed)
 - i. Improvement of the SSN user management console to streamline the user provisioning workflow¹.
 - j. Removing access rights-related data visualisation inconsistencies in SSN GI.
 - k. Fine-tuning and improvement of EIS and reference registries infrastructure for better performance and scalability.
 - l. The segregation from the STIRES application of all the functionality re-used in SSNv3 and currently implemented using its “front-end. The features to be migrated concern:
 - i. Accident module input tool.
 - ii. Accident module database.
 - m. Other minor-scale improvements in SSN EIS, SSN textual interface, COD/CSD/CLD web consoles stemming from requests from users.

- n. Hotfixes for the resolution of non –critical bugs affecting SSNv3.1 which are to be still unresolved until the 28th of August 2015.
- o. Changes in the COD/CLD/CSD web services taking into consideration the results of the CSD pilot with MS as well as the requirements of the CMC project
- p. The correction of messages 5, 24 – generated inconsistencies in timing referencing position tracks in SSN GI.3

Bidders may refer to Appendices G and H which contain information on the RFS launched by EMSA on SSNv3.1 and the main change in SSNv3.2 concerning the integration of STMID information into COD.

7.3 System performance requirements

The following performance requirements apply to the processing of messages and system information. Note that Member State authorities may assign more specific performance standards in accordance with their national requirements.

Timeframes for data availability

The national SSN systems connected to the central SSN system should be supported by data communication links and networks that allow them to transfer information within 1 minute between the two systems.

SSN data requesters should receive the desired information from SSN within an average of 30 seconds (central SSN system will not process responses received after 4 minutes) of making a request. In the case of phone, fax or email, data requesters should receive the requested information within 60 minutes. This is not applicable to archived information. . The timeframes above should be respected for 95% of the information exchanged during a 24h period and for 99% of the cases during a one year period.

The NCAs should respond to requests for archived data as per point below within 5 working days.

Timeframes for data storage⁴

The data shall be available "live" through the SSN system:

- a) Minimum of five (5) years for information related to incidents and accidents; and
- b) Minimum of two (2) months from the departure of the ship for information related to port calls and hazmat and from the reporting date for ship messages.

In any case, the data indicated above should be archived (off-line) for at least five (5) years, down-sampled when necessary. The archived data should be made available following a request by another NCA or EMSA. The requestor must provide adequate reasoning as to why the information is required. This type of data may be used for purposes such as statistical analysis or studies on traffic flows.

System availability requirements

System availability refers to the availability of the hardware and software necessary for the performance of the mandatory functionalities of the SSN system.

The SSN system shall be maintained in operation twenty-four hours a day, seven days a week to satisfy the mandatory functionalities of the system.

Availability of the SSN system shall be maintained at 99% minimum over a period of one year, with a maximum permissible period of interruption being 12 hours per incident.

The same availability requirements apply independently/individually to each national SSN system (including the communication links to the central SSN and local systems) and to the central SSN system (and communication links to the national SSN systems).

Backup procedures

Backup procedures should be implemented for each SSN system component in the event of a failure or a scheduled interruption as provided in the "Common Operational Procedures".

The NCA shall ensure that SSN messages are stored and transmitted to the central SSN system when communications and/or systems have recovered. The national and central SSN systems should be able to resend messages for up to 2 weeks.

The body responsible for the affected SSN system component must inform the other SSN system participants, in accordance with the operational procedures, whenever a failure or scheduled interruption occurs.

Additional system performance requirements

⁴ This requirement at the time of drafting this document is still to be implemented. Some of the relevant actions are planned for SSNv3.2

All participants should aim to prevent invalid messages (those not compliant with standards set in the SSN interface reference guide) from being sent. Nevertheless, invalid messages should be less than 0.1% of the total number of messages sent.

When the central SSN system receives an invalid message, an error message shall be produced and forwarded to the national SSN system. When central SSN system transmits an invalid message, the national SSN system should inform the MSS of the reasons for the invalid message as soon as possible.

Data quality

MSs should ensure that the automatic data quality rules agreed by the SSN group are applied prior to notifications being sent to central SSN.

Missing information (that should have been provided in accordance with the SSN legal requirements) should be less than 0.1% per type of notification (PortPlus, incident reports etc.).

MSs should put in place, in cooperation with EMSA, the appropriate control mechanisms to investigate data quality issues that affect more than 0.1% of the reports per country and type (as per chapter **Error! Reference source not found.**) per month.

Network coordination

Each NCA and EMSA should maintain a 24/7 contact point available to manage SSN related requests relating to daily operations or reporting issues from any other NCA or EMSA.

EMSA Maritime Support Services (MSS) provides 24/7 monitoring of notification requirements and network coordination as well as a helpdesk for the SSN system.

7.4 Other pertinent information concerning SSN data quality

The SSN system complies with the following requirements with respect to all information provided by the NCA or LCA..

Reliability - SSN system shall ensure that the information is available, accessible and usable under the defined conditions.

Confidentiality - SSN shall ensure that information is shared only among authorised persons or organisations (e.g. the information can be accessed only by the data provider or by accepted users). The level of confidentiality is defined for each type of information. Where information is requested via a national SSN system, the national SSN system is responsible for ensuring that information is only provided to authorised persons.

Integrity - SSN system shall ensure that the information is authentic and complete.
The information transmitted via the central SSN system is not modified unless by:

- its data provider;
- the NCA covering the data provider;
- the central SSN system, according to rule or procedure defined in the SSN documentation.

Traceability - SSN system allows the verification of the history, location, or application of the information by means of documented recorded identification. The following actions are traced by the central SSN system and are available to the data provider at all times:

- Receipt of the information;
- Modification of the information;
- Request of the information through request/response mechanism;
- Communication of the information by any other mean.

The information recorded is:

- user identification
- time stamp
- description of action

The requirements above are translated into measures applied to the whole SSN system.

Anchor for footnote⁵

⁵ Footnote Text

European Maritime Safety Agency

Praça Europa 4
1249-206 Lisbon, Portugal
Tel +351 21 1209 200
Fax +351 21 1209 210
emsa.europa.eu



**Sub-Appendix E.2 to
Appendix E
of the Tender Specifications**

EU LRIT Cooperative Data Centre

Table of Contents

| | | |
|-------|--------------------------------------|----|
| 1. | EU LRIT Cooperative Data Centre..... | 3 |
| 1.1. | Introduction | 3 |
| 1.2. | EU DC Overview | 3 |
| 1.3. | Software and technologies used..... | 5 |
| 1.4. | Software Technologies..... | 5 |
| 1.5. | Software Architecture | 6 |
| 1.6. | User Web Interface | 7 |
| 1.7. | Monitoring Tools | 8 |
| 1.8. | System Configuration | 9 |
| 1.9. | Interfaces | 10 |
| 1.10. | Network..... | 10 |
| 1.11. | Performance and Availability | 11 |
| 1.12. | Message Size..... | 11 |

1. EU LRIT Cooperative Data Centre

1.1. INTRODUCTION

This document gives an overview of the EU LRIT Cooperative Data Centre. The EU LRIT Data Centre (EU DC) has been operational since June 2009 and EMSA hosts and operates the EU DC since 5 November 2011.

1.2. EU DC OVERVIEW

The Long-Range Identification and Tracking (LRIT) system is a global ship tracking service developed under the co-ordination of the International Maritime Organization (IMO) and available to IMO Contracting Governments.

The LRIT Data Centres (DC) collect, store and provide LRIT information (ship position reports) to users worldwide through an Internet based network.

The main function of the EU DC is to provide positions of EU flagged ships worldwide and non-EU flagged ships passing or coming to Europe via the exchange of messages with other Data Centres.

There are currently 27 Member States, Norway, Iceland, Croatia and 5 Overseas Territories Participating in the Data Centre. Around 9000 ships are monitored/tracked by the Data Centre and around 3 million messages are processed per month with around 190,000 position reports per month being exchanged with other Data Centres. There are around 600 users of the EU LRIT Data Centre.

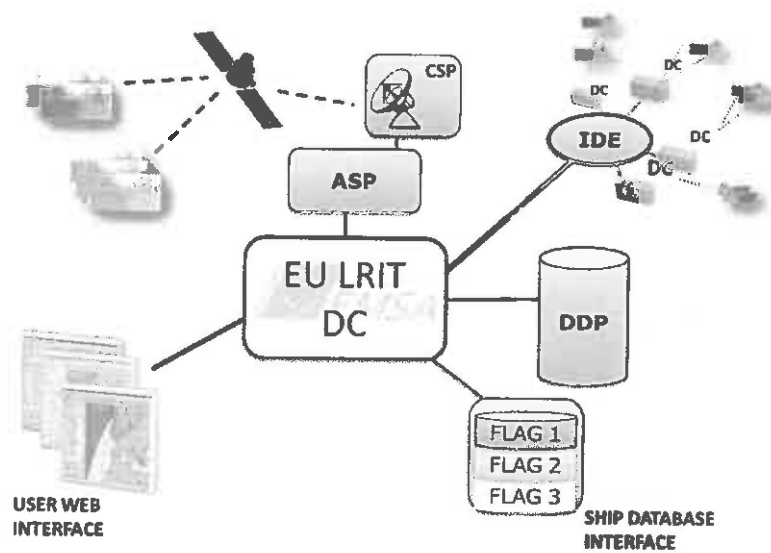


Figure 1 – The EU LRIT DC within the LRIT System

The high level architecture of the EU DC is shown in Figure 1. This shows the general flow of messages which are sent from the ship, via a satellite, through a communication service provider (using various communication networks Inmarsat C, D, Iridium), an application service provider and then to the EU Data Centre. The DC has an interface with the Ship Database which includes all the ship related information for each ship registered in the database for an EU flag and the EU DC receives a copy of the Ship Database once a day. The Data Centre has a User Web Interface for users to be able to access the LRIT information and some Participating countries of the EU DC also use an XML interface or web service to receive streamed data.

The exchange of messages between DCs is done through the International Data Exchange (IDE) which can be seen as the communication hub of the LRIT network (Figure 1). The IDE routes the messages to the proper destination by using address information contained in the Data Distribution Plan (DDP), an XML document maintained by the Contracting Governments and made available by the DDP Server, hosted at IMO.

Not shown in Figure 1, the EU DC also has an interface with the Invoicing and Billing System which allows the EU DC to bill users when they request LRIT information as well as change the rate of reporting of a ship and allows invoicing of other Data Centres. A journal is sent by the EU DC to the Invoicing and Billing system to allow these transactions to take place.

1.3. SOFTWARE AND TECHNOLOGIES USED

The LRIT DC is based on several software modules allowing an easy deployment and management of the LRIT DC system. It embeds software COTS, such as the Tomcat and the Jetty engines.

The LRIT DC is basically a data driven system, which handles messages received from others systems (ASP, IDE, DDP server, etc.). The internal communication between the LRIT DC sub-systems is also data driven.

The LRIT DC system architecture provides a high service availability system, which minimizes downtime and prevents message loss. The LRIT DC has been designed to respond to demanding requirements in terms of latency and performance.

There are three main categories of software components:

- Core Components
- User Web Interface
- Monitoring Tools

1.4. SOFTWARE TECHNOLOGIES

The following software technologies are used in the EU LRIT DC system:

- **Database:** the LRIT DC system is using Oracle 11g database. All the sub-systems written in JAVA are using the Oracle JDBC drivers and the Hibernate persistence framework.
- **Web Application Server:** The LRIT DC web application is running in the Tomcat JSP and Servlet engine.
- **SOAP web service and SOAP engine:** the web services of the LRIT DC system are running in the Jetty engine, embedded in the Java application of the corresponding sub-system. The CXF services framework is used to implement the SOAP web service
- **Log4J:** is used by the LRIT DC system to handle log files. It allows an easy configurable way to define the content of log files according to log levels and software components.
- **Web Ajax Framework:** the LRIT DC web interface is built using the Ext JS cross-browser JavaScript framework for rich web apps.
- **Apache Commons:** several Apache commons libraries are used within the LRIT DC (bean-utils, collections, dbcp, logging, pool, io)
- **Custom made:** several Custom made libraries are used by the LRIT DC

1.5. SOFTWARE ARCHITECTURE

A graphical representation of the LRIT DC System Architecture is shown in Figure 2. The central component (MOM) is a library that provides a logical communication bus between the sub-component:

- ACQ: message reception
- POST: message dispatch
- WAS and WS: web user interface
- CORE: message processing
- DDP RULES CHECKER: data access rights entitlement based on the Data Distribution Plan

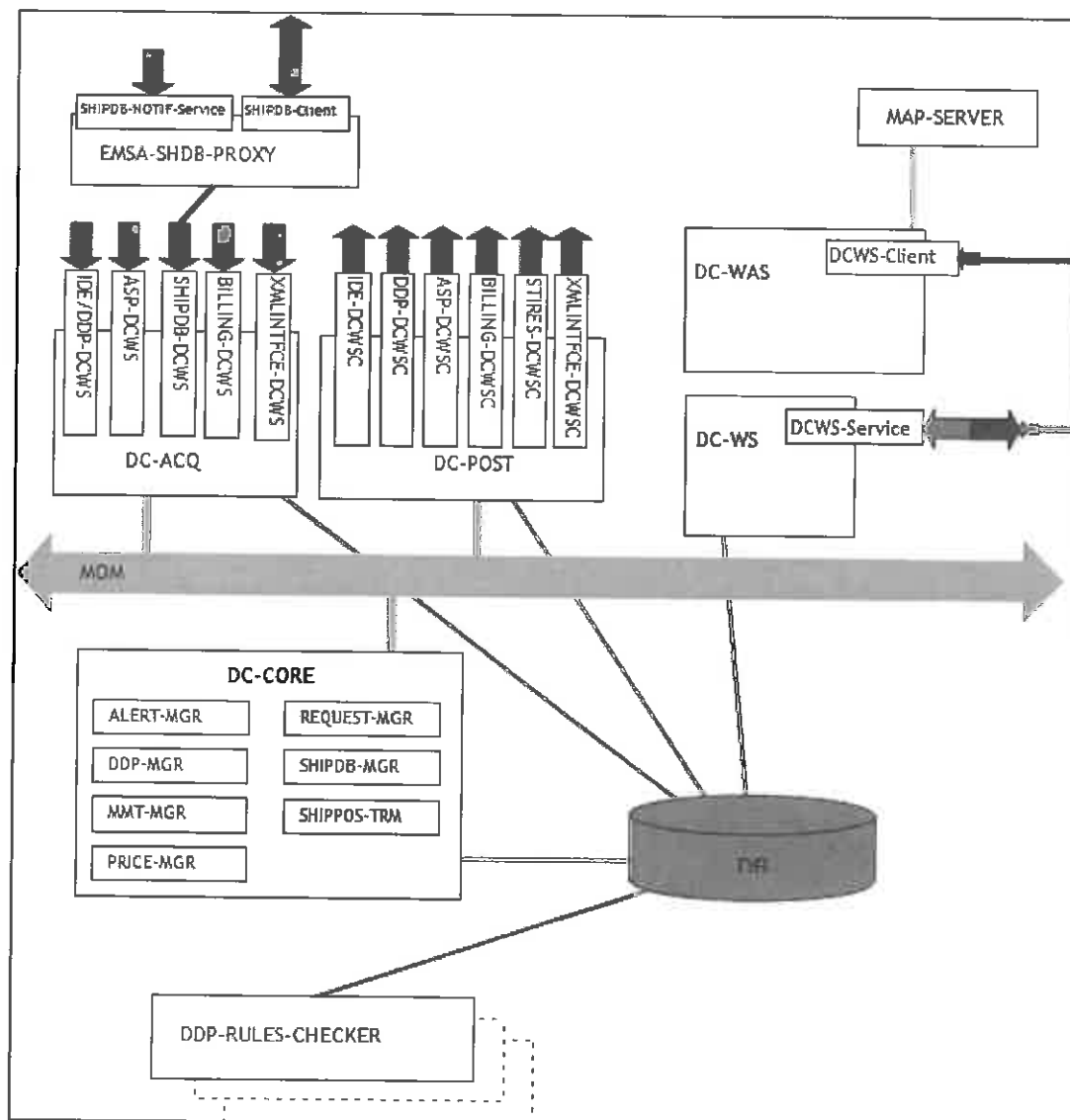


Figure 2 – LRIT DC system software architecture

The LRIT DC components are responsible for the following tasks (see sample Use Case diagram in Figure 3:

- message reception from external systems, e.g. the ASP
- message processing
- message storage
- message delivery to external systems, e.g. the IDE

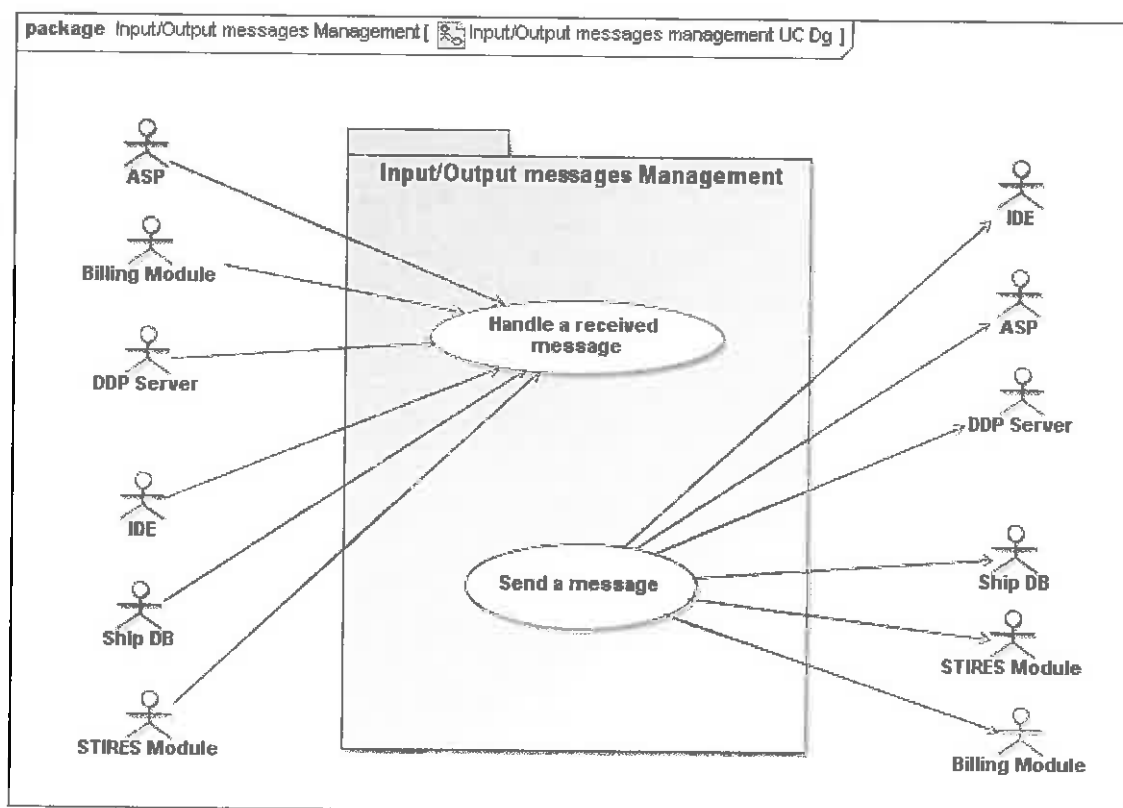


Figure 3 - Message Management (Use Case diagram)

The LRIT DC Core is composed of 15 sub-systems. The business model comprises more than 70 classes.

1.6. USER WEB INTERFACE

The EU DC has a User Web Interface (UWI) is built using the Ext JS cross-browser JavaScript framework for rich web apps and is running in the Tomcat JSP and Servlet engine. Around 29 menus host an interface with many features such as:

user management, worldwide map view, detailed filtering features, customizable web interface, manual LRIT requests menu, ship integration reporting and monitoring menu, administration menu, etc.

The following figure shows the worldwide map view of the EU DC UWI:

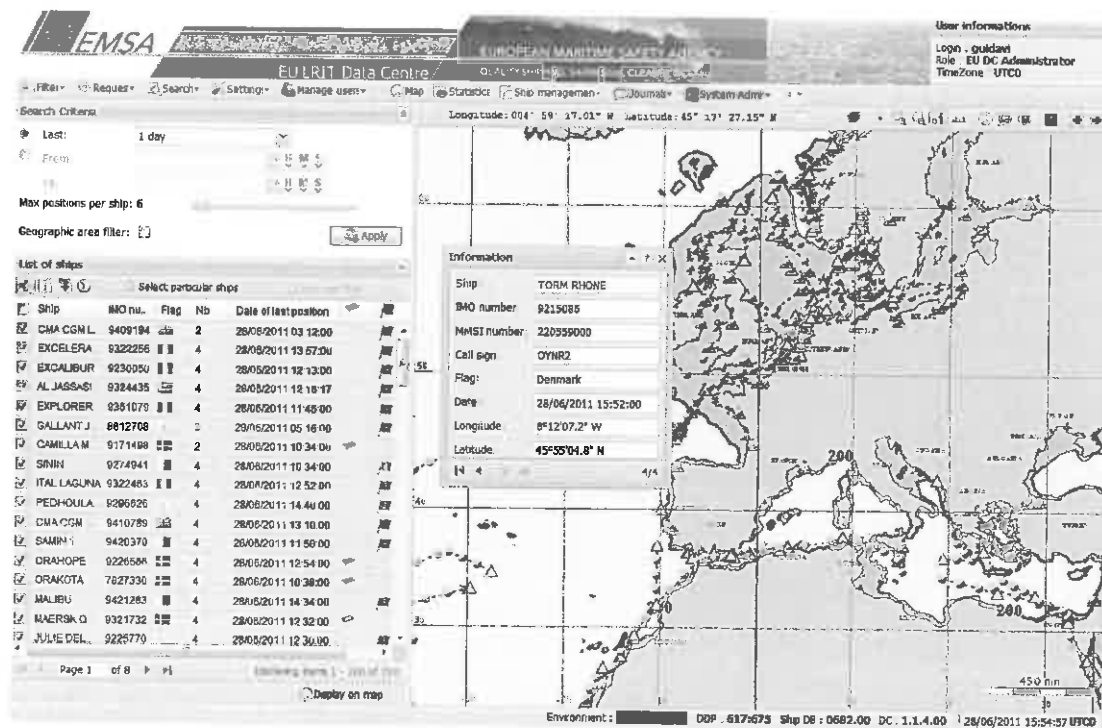


Figure 4 – EU LRIT DC Map View

1.7. MONITORING TOOLS

The EU LRIT DC is continuously monitored through a custom made monitoring tool specifically tailored to the architecture and requirements of the system.

It is composed of:

- **Supervisors:** which look into the application, identify alerts and warn the DC operators; these are mostly bash scripts.
- **Reports:** which include system incident and performance information; these are in html
- **Web Interface:** which is the interface for the DC operators
- **Wiki:** which contains all operational procedures for the DC operators

1.8. SYSTEM CONFIGURATION

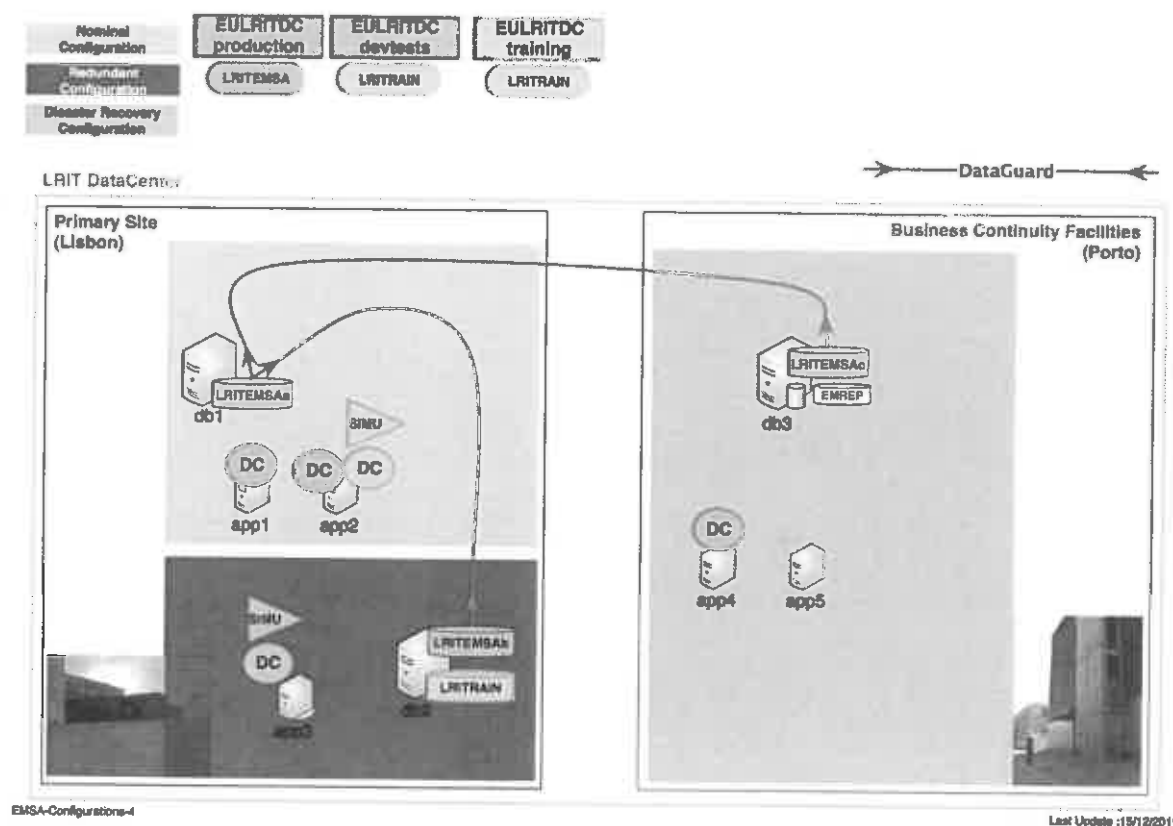


Figure 5 – Main environments and servers

In terms of System Architecture, the EU LRIT DC system is composed of:

- **2 sites:** primary and secondary;
- **3 configurations:** nominal, redundant and disaster recovery; and
- **3 environments:** production, training and devtest.

1.9. INTERFACES

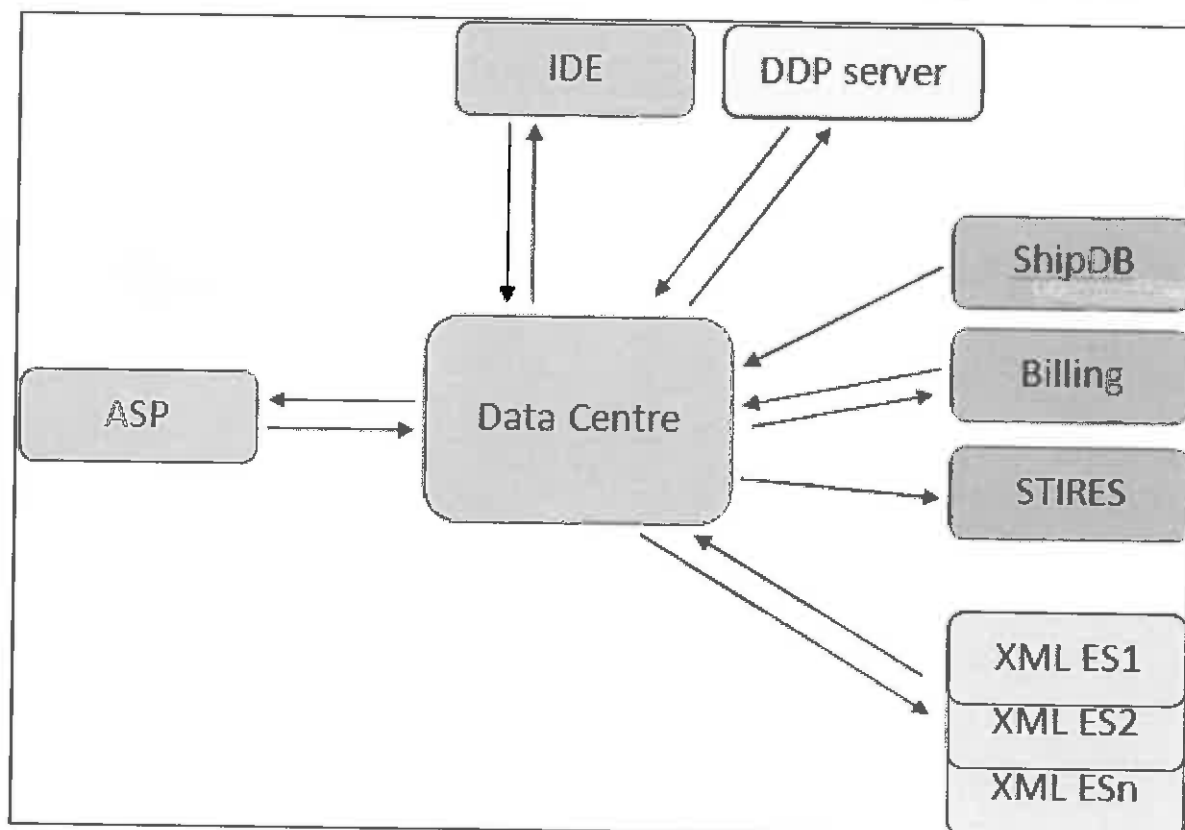


Figure 6 – External Interfaces

The external interfaces between the DC system and other systems consist of web services. For all of these web services, the same principle is adopted: it consists in the exchange of a message which content is defined under the form of an XML schema.

There are around 9 active external interfaces with around 10 WSDLs, 22 message schemas and operations, and 20 messages types.

Internally, there are around 70 internal interfaces with around 3 WSDLs, 9 message schemas and 4 messages types.

1.10. NETWORK

For each site, the EU LRIT DC network is set-up thanks to:

- 2 firewalls (External and Internal)
- 3 LAN switches
- 2 VLANs (Management and Applications)
- VPNs

External connections are limited to interfaces illustrated in Figure 6 and are assured by DNS/https. Internally, the two sites are connected through a VPN which creates a remote network between them through a public channel (internet).

1.11. PERFORMANCE AND AVAILABILITY

The EU DC should process any regular position report in the system from the time it transmitted by the ship within 15 minutes.

The EU DC should process and handle any request sent by an LRIT Data User within 30 minutes of the time the LRIT Data User requested the information.

The EU DC should operate 24/7 with an availability of:

- 99 % over any 1 month;
- 95 % over any 24 hour period.

The EU DC should have:

- seamless switch-over to local redundant servers;
- seamless switch-over to remote disaster recovery site server

1.12. MESSAGE SIZE

The average size of an LRIT position report or a request message is of some kilobytes. The size of the DDP message is approximately 2 MB.

**Sub-Appendix E.3 to
Appendix E
of the Tender Specifications**

CleanSeaNet

Table of Contents

1. CleanSeaNet 3

1.1. Available datasets4

1.2. Main capabilities:4

1.3. Current functional blocks:5

1.4. Interfaces with other systems:5

1. CleanSeaNet

The Service Oriented Architecture approach based on interoperable recommendations (compliance against the standards) is a crucial aspect to be addressed in CSN, not only because they represents the principles on which the service was originally designed and implemented, but mainly because they outline how the service itself can and should continually improve. It is based on these principles that new CSN related components, or modules, will be developed (i.e. platform monitoring and oil spill drift models); integrated (i.e. Vessel Detected provisioning to IMDatE); and new data sources added (i.e. optical satellite).

The CleanSeaNet Data Centre (CSN-DC) offers its functionalities as a combination of two set of software components: a) the Maritime Earth Observation System and, b) the CSN Clients.

Satellite images are planned and tasked by EMSA, and acquired via a network of Service Providers (presently CLS, EDISOFT, E-GEOS, KSAT and EUSI). The data, hereafter referred to as Earth Observation packages, is delivered to EMSA and inventoried in the MEO (see Figure 2). The derived information is then disseminated to the users through the following standard web services: Web Map Service (WMS), Web Feature Service (WFS), Web Coverage Service (WCS), and Catalogue Service (CSW). To perform the aforementioned tasks MEO shall comprise the following components: Ingestion tools (PDS and ISM), the geospatial services (WMS, WFS, CSW, WPS, and WCS), the MD5 service, the JOU service and Ordering.

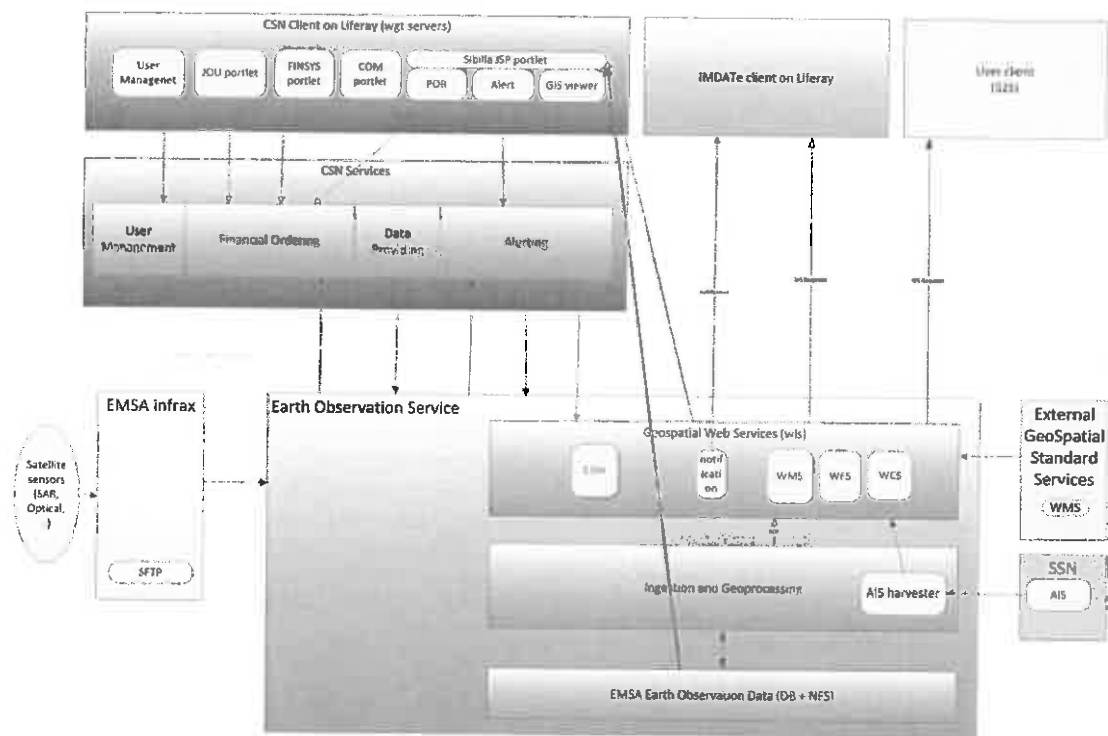


Figure 1- Conceptual CSN Architecture

1.1. AVAILABLE DATASETS

CSN service processes the following satellites:

- RADARSAT 1 and RADARSAT 1
- COSMO-SkyMed
- TerraSAR-X
- in the future SENTINEL missions

Furthermore the following MyOcean meteo-oceanographic data are acquired:

- sea surface temperature
- surface current speed & direction
- chlorophyll a concentration
- ice edge
- surface winds

1.2. MAIN CAPABILITIES:

- identifying and tracing oil pollution on the sea surface
- monitoring accidental pollution during emergencies
- contributing to the identification of polluters

1.3. CURRENT FUNCTIONAL BLOCKS:

- **Discovery.** CSN resources (e.g. datasets, dataset series, geospatial services or sensors) are inventoried in catalogues in order to make them searchable and discoverable.
- **Data Acquisition Request and Feasibility Analysis.** These components deal with how EO systems and sensors can be programmed such that the desired datasets can be downloaded and processed after their retrieval.
- **Product Ordering.** The product ordering allows EMSA to enter into a commercial relationship with the EO data provider, in order to task and acquire the desired datasets.
- **Ingestion.** Raw datasets which are retrieved by EO sensors have to be acquired, processed and geo-referenced by CSN.
- **Online Data Access and Presentation.** It is a set of services that allow to access at the data processed by CSN.

1.4. INTERFACES WITH OTHER SYSTEMS:

CSN provides the following data through standard service to IMDatE and moreover CSN enables S2S with the EU MS:

- Oil Spill features, Vessel Detected (OGC- Web Feature Service 1.1.0);
- Simplified SAR images (OGC - Web Map Service 1.1.3);
- Grid SAR images (OGC - Web Coverage Service 1.0);
- Discovery capabilities based on Metadata (OGC - Catalogue Service 1.1.1 (ebRIM profile));
-

Sub-Appendix E.4 to Appendix E of the Tender Specifications

Overview of the SSN Ecosystem GUI (SEG)

V. 1.1 – 2016-04-13

1 Introduction

The SSN Ecosystem may be defined as the technical framework encompassing the following EMSA maritime applications: SafeSeaNet, Integrated Maritime Data Environment, Earth Observation Data Centre and LRIT Cooperative Data Centre. As such the SSN Ecosystem is the provider of a number of different maritime information services to Member States, EU bodies and relevant third party partners.

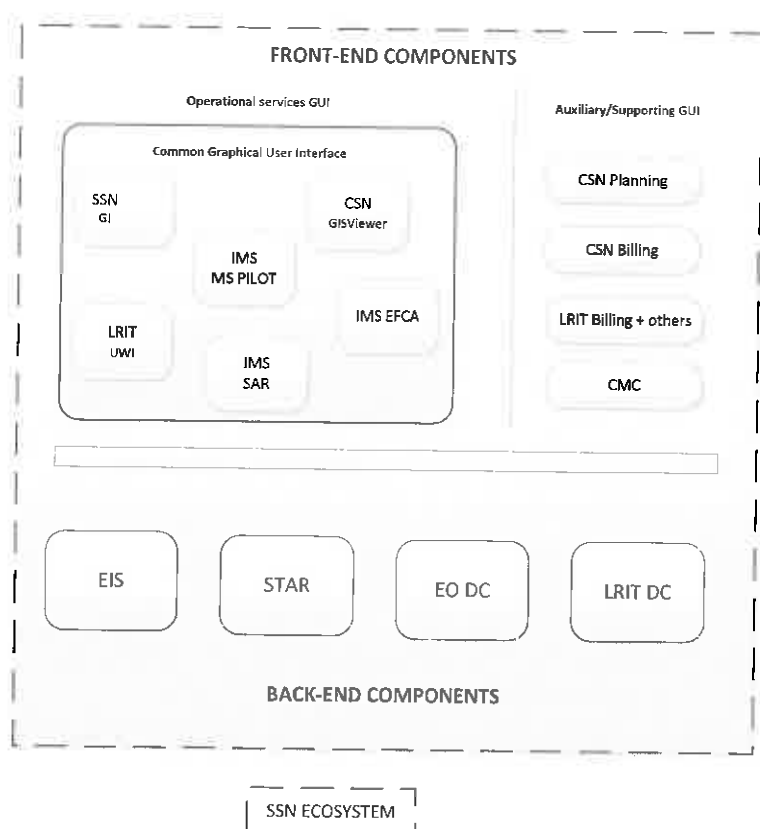
While currently these services are provided through, inter-alia, individual graphical user interfaces (GUI), the objective is to develop a single front-end platform (i.e. a single GUI) supporting all configurations required to cover existing legal and operational requirements for all services provided through the SSN Ecosystem.

This SSN Ecosystem GUI (SEG) will be implemented throughout the course of 2016 and will be the front-end of the different maritime information services and as such will be the common platform to display and perform operations on, inter-alia, SSN information (e.g. ship, voyage, incident and hazmat data, as well as STMID information), vessel positions (e.g. T-AIS, LRIT, SAT-AIS, VMS, Radar, etc.), Earth Observation related products (e.g. satellite imagery, oil spill detections, vessel detections, etc.), alerts, incidents, and ancillary data (e.g. met-ocean). The SEG will therefore cater for all services provided by the SSN Ecosystem and as such serve different user communities and cover the needs of different user domains.

1.1 Scope of the SEG

Referring to the figure below, the SSN Ecosystem itself contains all of the elements within the dashed rectangle. The back-end components, represented by black boxes, are the technical applications on which all maritime information services are based on. The front-end components are divided into 2 categories: the operational and auxiliary-supporting. The SSN Ecosystem [common] Graphical User Interface, represented by the red box, falls within the operational category, is not service specific and thus covers all relevant maritime information services. The different maritime information services, examples of which are illustrated as orange boxes, will therefore be served through this front-end component. The auxiliary-supporting front-end components are either service and application specific (e.g. CSN Planning, LRIT billing, etc.) or horizontal services which do not fall within the SSN Ecosystem GUI (e.g. Common Management Console). As such they will continue to be served through their own front-ends.

One of the guiding principles for the development of the SSN Ecosystem Graphical User Interface (SEG) will be the ability to configure the GUI in-house and be able to set up different operation/services both independently and quickly. Whenever possible the intervention of external contractors for service configurations should be avoided as this will enable EMSA to reduce cost and increase the rate to which we can respond to incoming needs and user requirements.



1.2 Main Wireframes

This section provides a short summary of the main design approach for the presentation layer.

1.1 Overview

This section provides an overview of the layout.

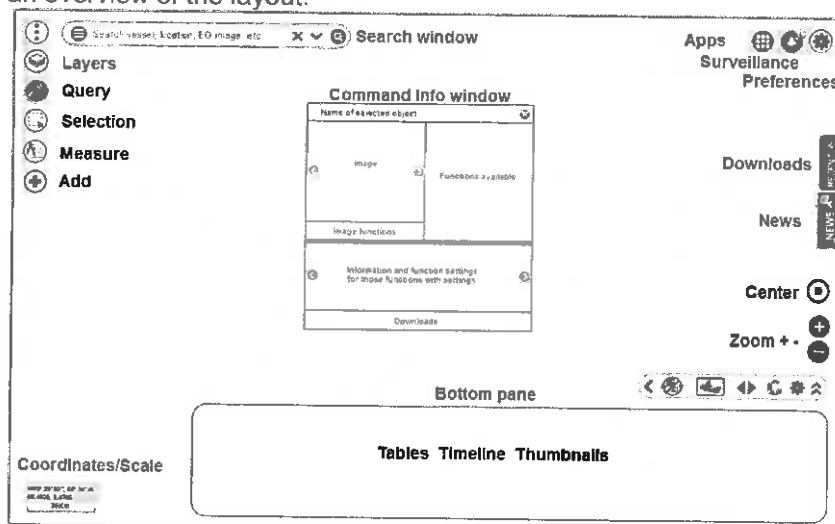


Figure WF1: Overview of the SSN Ecosystem GUI.

1.2 The main screen

Figures WF2 and WF3 show the main screen of the SSN Ecosystem where no object is selected.

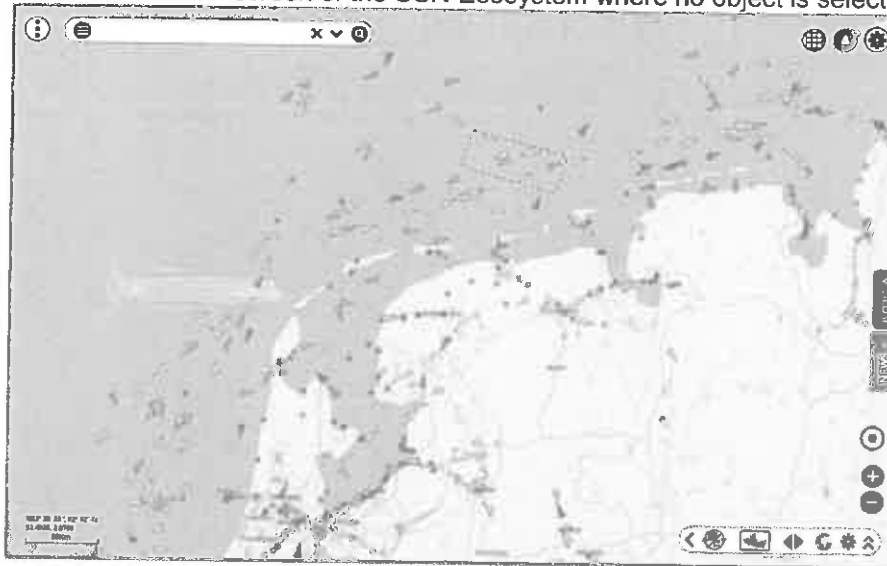


Figure WF2: Overview of the SSN Ecosystem GUI, no object selected.

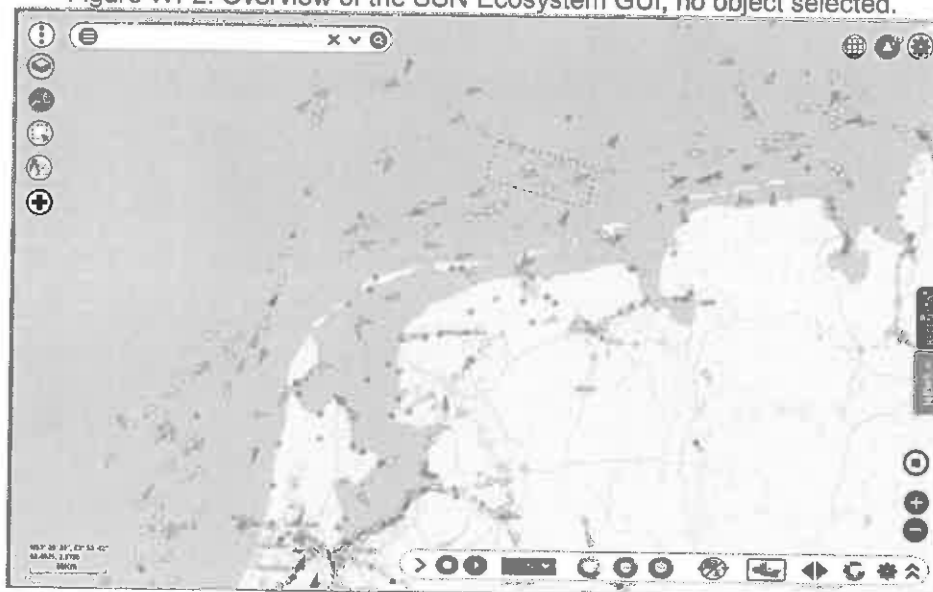


Figure WF3: Overview - no object selected, function button and bottom pane expanded.

1.3 The Command and Info window

The command and info window, as can be seen in Figures WF4 to WF7, is a general window with certain architecture to show image, information, downloads and functions of any object selected in the map.

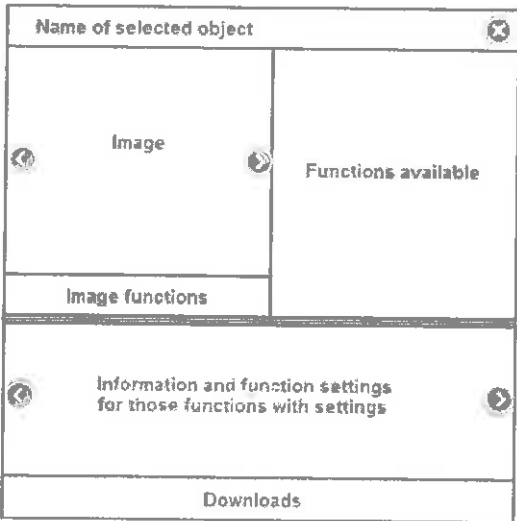


Figure WF4: The Command and Info window architecture.



Figure WF5: The Command and Info window, where a vessel is selected.

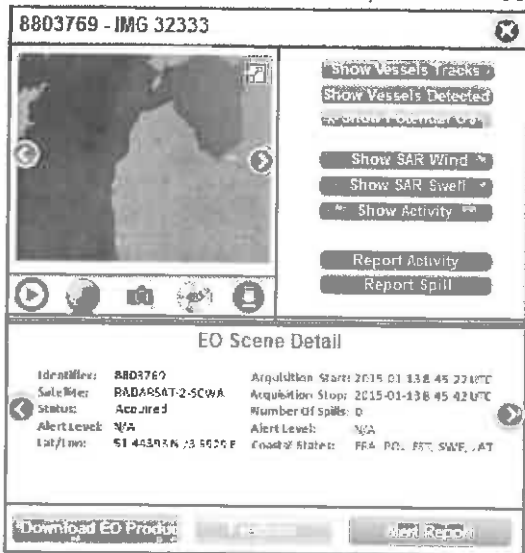


Figure WF6: The Command and Info window, where an Earth Observation image is selected.



Figure WF7: The Command and Info window in the map, where a vessel is selected.

1.4 Timeline, tables and thumbnails

The bottom pane can be switched between Thumbnails, Tables and Timeline (TTT) and whatever selected is updated in the command and info window and selected in the map.

The bottom pane pops up automatically with certain functions such as "Integrated ship profile" or in cases to show results in tables. The user can manually show/hide the bottom pane via the double arrows in the bottom pane bar. See Figure WF19.

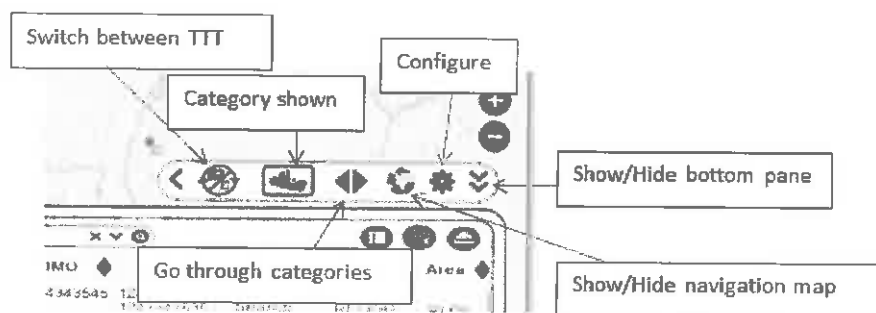


Figure WF19: The bottom pane bar.

The list of "My fleet", target of interest (TOI), earth observation images and more, can be displayed as thumbnails or tables.

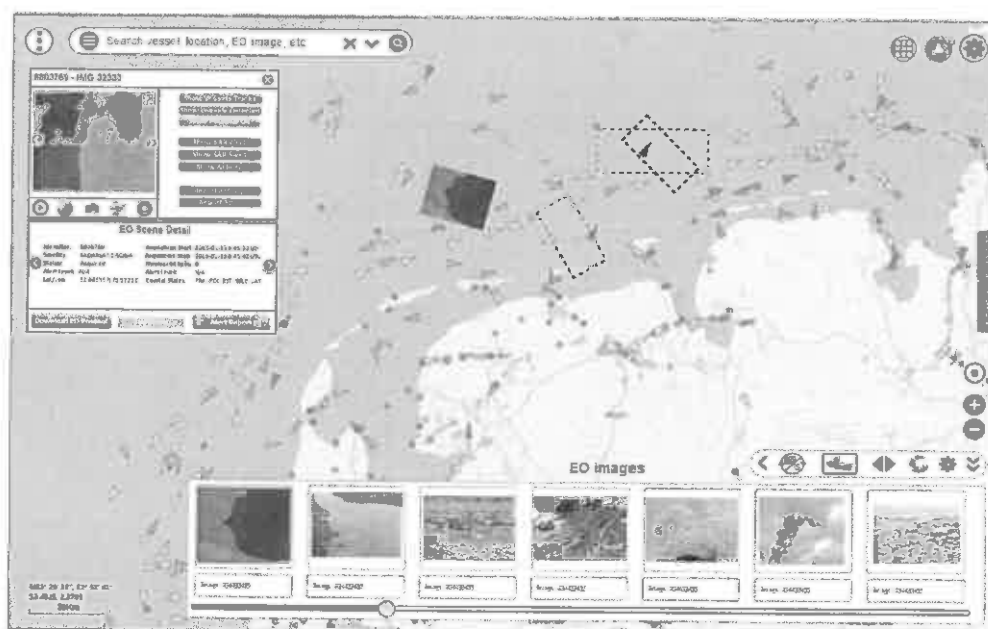


Figure WF20: The bottom pane in thumbnails mode, the image selected can be seen on the map and selection and info window.

1.3 Technical aspects

The SEG integrates with a wide range of business services from SSN, EO DC, IMDatE/STAR, LRIT CDC and THETIS. Therefore it is necessary for the backend services to be well controlled and documented. The figure below provides the high level architecture.

An integration layer will be placed between the SEG and the backend components in order to support “independence and isolation” from the underlying Business Services provided by the Backend Components, thus supporting Business Data Mash-ups from different Backend Components and Modularity.

The CMC includes the upgrade of the EMSA Identity Management solution as well as the CARD which is a repository of access rights policies.

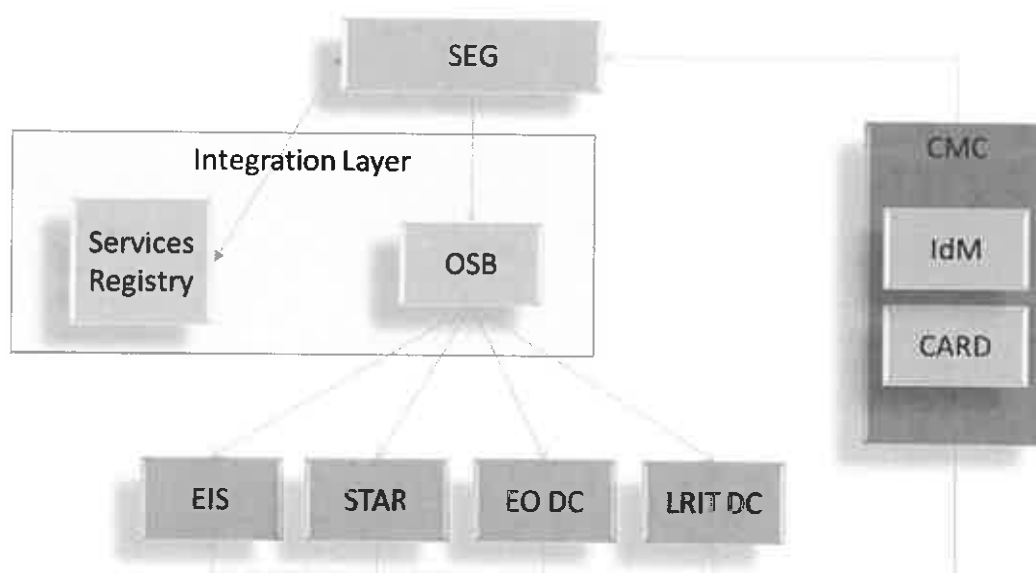


Figure 1: Architecture

1.4 Technologies

The front end web application is being developed using OpenLayers, Angular JS on the client side and Spring MVC version 4.2 for the server components. WebGL is used for rendering objects for a 3D view functionality. The application features a REST interface to be used by the web application for information updates on the web user interface.

The application connects to the remaining EMSA services via HTTP, mostly the communication will be through EMSA's Oracle Service Bus that proxy all internal EMSA services hiding future interface changes from SEG. In some cases the SEG is able to connect directly to the services via REST or SOAP interfaces.

| Technology | Version | Used for |
|-----------------------|---------|--|
| AngularJS | 1.4.8 | Client side logic implementation |
| WebGate | - | SSO token validation, HTTP header enrichment with the current user |
| Weblogic Server | 12.1.3 | Application server supporting the server components of the application |
| Spring Core Framework | 4.2.4 | Base IoC framework used for server components development |
| Spring MVC Framework | 4.2.4 | Creating the REST interface for remote communication between components. |
| Spring Security | 4.0.3 | User Authorization |
| QueryDSL | 4.0.7 | Creating SQL queries to be performed to the database. |
| Oracle Exadata | - | Data Persistence |

--- End of the Document ---

ABOUT THE EUROPEAN MARITIME SAFETY AGENCY

The European Maritime Safety Agency is one of the European Union's decentralised agencies. Based in Lisbon, the Agency provides technical assistance and support to the European Commission and Member States in the development and implementation of EU legislation on maritime safety, pollution by ships and maritime security. It has also been given operational tasks in the field of oil pollution response, vessel monitoring and in long-range identification and tracking of vessels.

European Maritime Safety Agency

Praça Europa 4
1249-206 Lisbon, Portugal
Tel +351 21 1209 200
Fax +351 21 1209 210
emsa.europa.eu



Sub-Appendix E.5 to Appendix E of the Tender Specifications

Overview of Mobile Applications for IMS

V. 1.0 – 2016-04-13

1.1 Introduction to IMS apps

The first IMS app project deployed an operational mobile solution to EMSA users of integrated services. This included:

- Development of iOS and Android application to address a set of use cases, including:
 - Vessel position & detail information
 - Area centric query
 - Incident reporting
 - Oil spill monitoring and feedback
- Development of the IMS web services on top of EMSA's Oracle Service Bus that connect to all other web-services needed by the mobile application
- Integration with the EMSA's single sign on via Oracle API Gateway

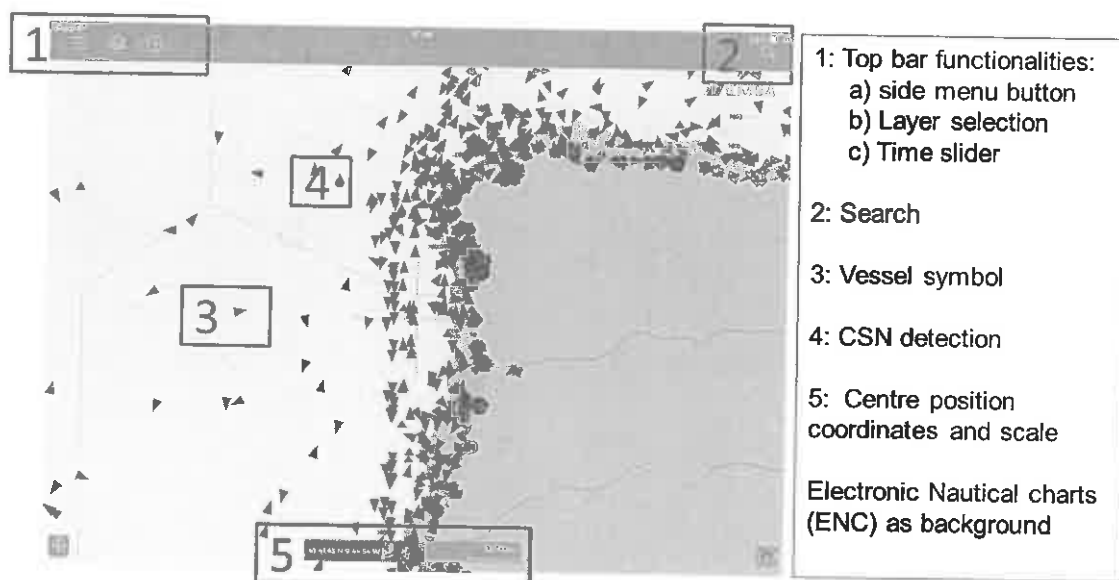
Three separate versions of the application were developed, tested with the end-users and deployed operationally:

- iOS (smartphone)
- iOS (Tablet)
- Android (Tablet)

1.2 Main screenshots

This section provides a short summary of the main design approach for the presentation layer.

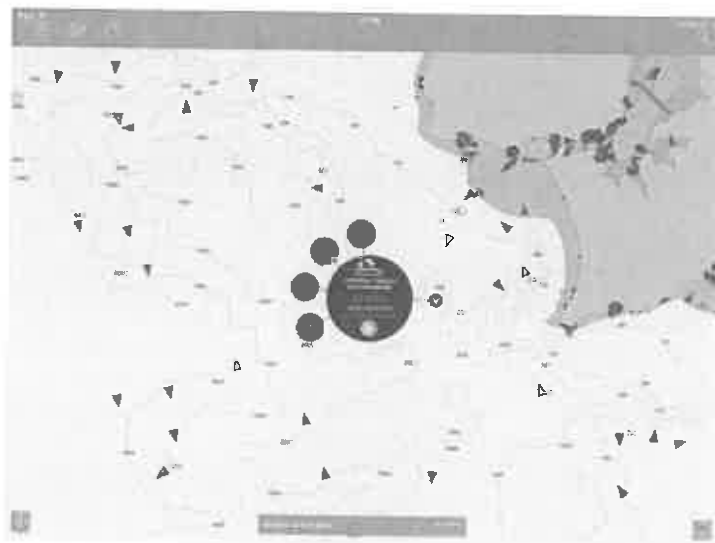
The following image shows the main application screen.



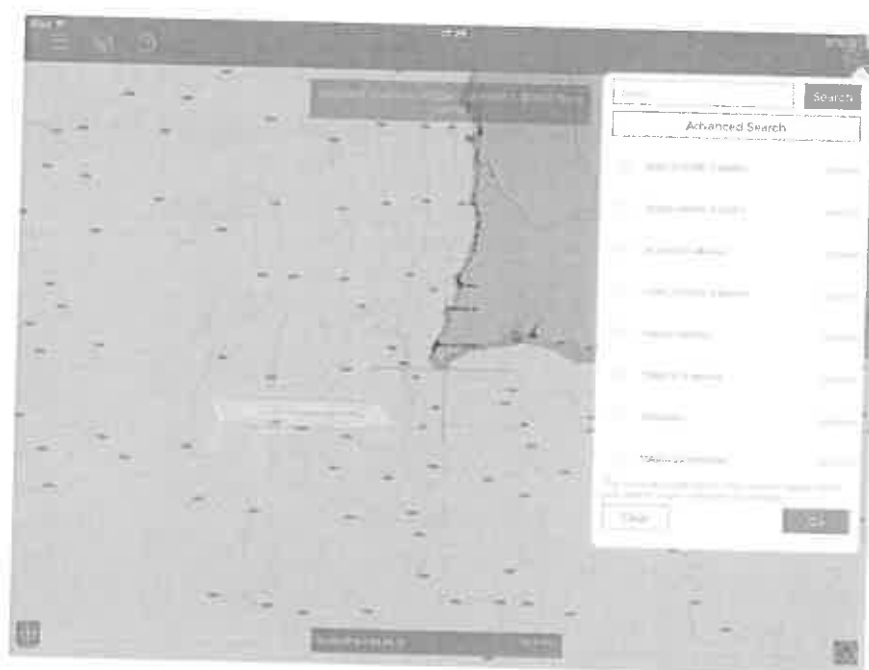
The following image shows the main menu detail.



The following image shows the vessel selection menu.



The following image shows the basic search results.

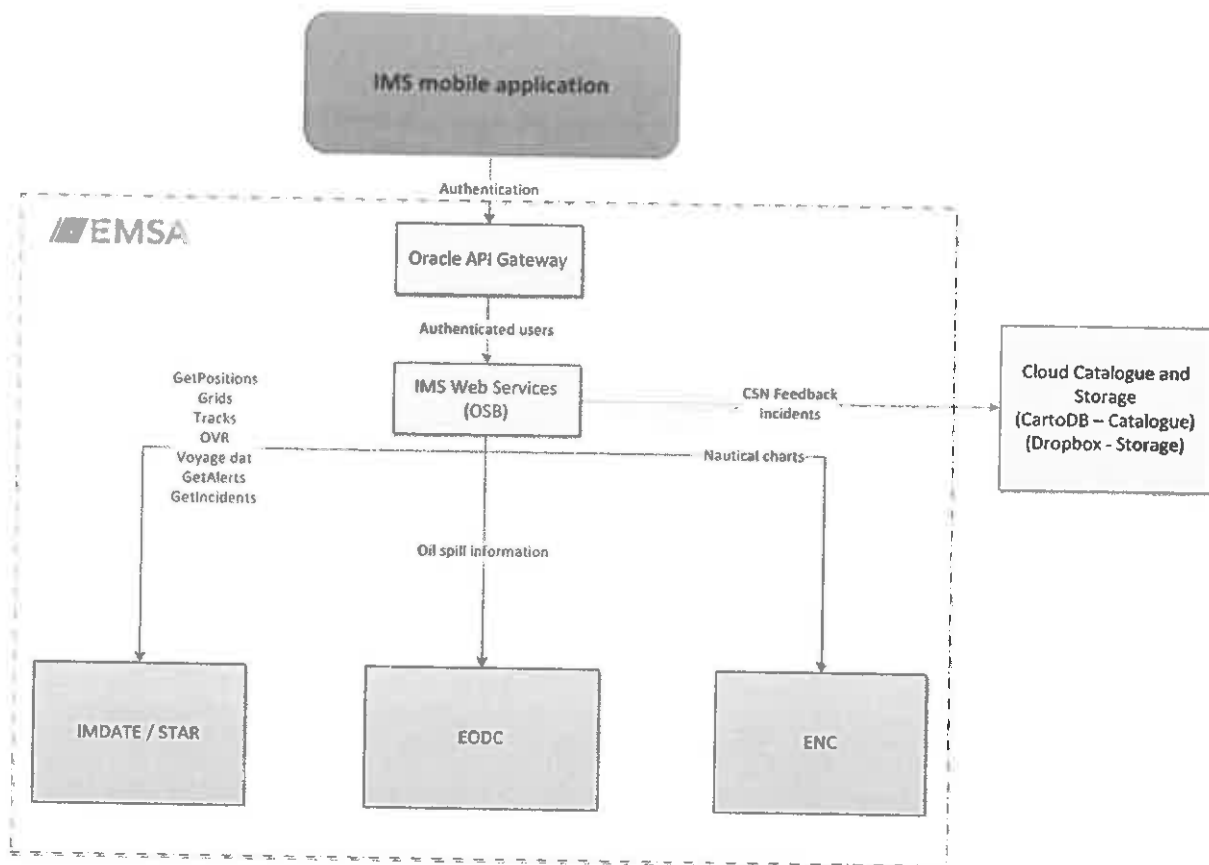


The following image shows the Incident report menu.



1.3 Architecture

The overall architecture of the current implementation can be found in the following image.



EMSA has implemented the Oracle API Gateway solution for the mobile application to interact with the existing IdM. This will:

- 1) Provide user authentication
- 2) Allow access to EMSA resources
- 3) Provide login / logout functionalities
- 4) Identify the user's role

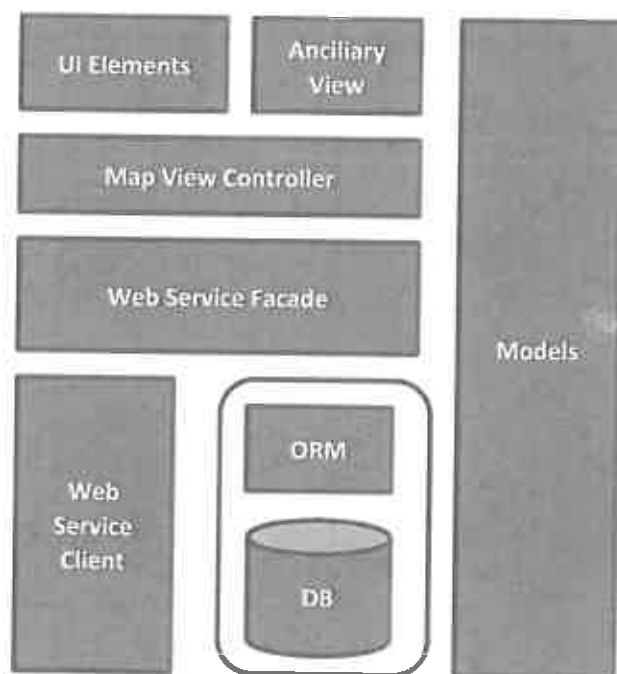
The EMSA IMS mobile application consumes information provided by the IMS web services. These web services are deployed on top of EMSA's Oracle Service Bus and are connected to the backends of IMDate/STAR, EO DC and the ENC/CMAP maps.

CartoDB is currently used as catalogue service to inventory all the multimedia contents metadata. This is a standard catalogue service that provides standard interfaces as Open Geospatial Consortium Catalogue Services (OGC-CSW) and compliant with INSPIRE discovery service. Additionally CartoDB is used for:

- Storing meta-information about uploaded content
- Storing menu preferences and lists to be used in the application
- Storing credentials for the cloud storage

The EMSA IMS mobile application uses Dropbox to store uploaded rich content (video, images and documents).

The mobile applications follow a Model-view-controller (MVC) architecture, centered on a view controller which orchestrates the map and related views. The map view controller depends on several loosely coupled modules that implement the application persistence and web service access layers.



--- End of the Document ---

ABOUT THE EUROPEAN MARITIME SAFETY AGENCY

The European Maritime Safety Agency is one of the European Union's decentralised agencies. Based in Lisbon, the Agency provides technical assistance and support to the European Commission and Member States in the development and implementation of EU legislation on maritime safety, pollution by ships and maritime security. It has also been given operational tasks in the field of oil pollution response, vessel monitoring and in long-range identification and tracking of vessels.

European Maritime Safety Agency

Praça Europa 4
1249-206 Lisbon, Portugal
Tel +351 211209 200
Fax +351 211209 210
emsa.europa.eu

Sub- Appendix E.6 to Appendix E of the Tender Specifications

IMDatE

Table of Contents

| | | |
|------|---|---|
| 1. | IMDatE | 3 |
| 1.1. | Core functionalities | 3 |
| 1.2. | System Architecture | 4 |
| 1.3. | Software and technologies used | 5 |
| 1.4. | System Performance and Availability | 6 |
| 1.5. | User Interface | 6 |

1. IMDatE

1.1. CORE FUNCTIONALITIES

Given below is a summary of the main data sets collected and processed by IMDatE as well as the interfaces and the main functional blocks.

Available datasets:

- Position reports (coastal AIS, S-AIS, LRIT, VMS, other)
- Non-cooperative targets (VDS, coastal radar)
- Voyage and cargo information
- Events (geo-referenced incidents)
- Ship particulars
- EO images and spill products
- PSC inspection information
- User Community assets and mission-specific information
- Video streaming and files
- Nautical and cartographic maps
- Meteorological and tidal information

Main functionalities of IMDatE:

- Addition of new streams of data (AIS, S-AIS, coastal radar, shipborne positions and radar, VMS, etc) for a particular user community
- Creation new alerts and reports (email, PDF, SMS) simply by configuration
- Configuration of new graphical web interfaces (symbols, associated colours, user provided data) for a given user community (VTS, fishery, border control, anti-piracy etc)
- Allows user community specific data to be provided (ie. ICCAT file and incidents from EFCA, ship registry from EUNAVFOR) and displayed – little configuration is required.
- Set-up a dissemination of vessel positions in a number of formats/protocols depending on the user needs.
- Create a template of automated behaviour monitoring (based on behaviour algorithms) that can be set-up by specific users. IMDatE provides the framework to add new algorithms and combine them, and the surveillance engine to detect the behaviour.
- Aggregate maritime data from multiple applications.

Current functional blocks:

- Multi-source ingestion component (see sources mentioned above)
- Data Fusion Module

- Satellite AIS data processing module
- Ability to tailor Operation/Services.
- Graphical User Interface
- Common Geo-Registries
- Automated behaviour monitoring engine and algorithms
- Alerting and report generation engine

Interfaces with other systems:

As mentioned previously, IMDatE connects directly to other systems providing maritime data (principally ship positions: coastal radar, VMS etc, voyage info, incidents). Namely it interfaces today with:

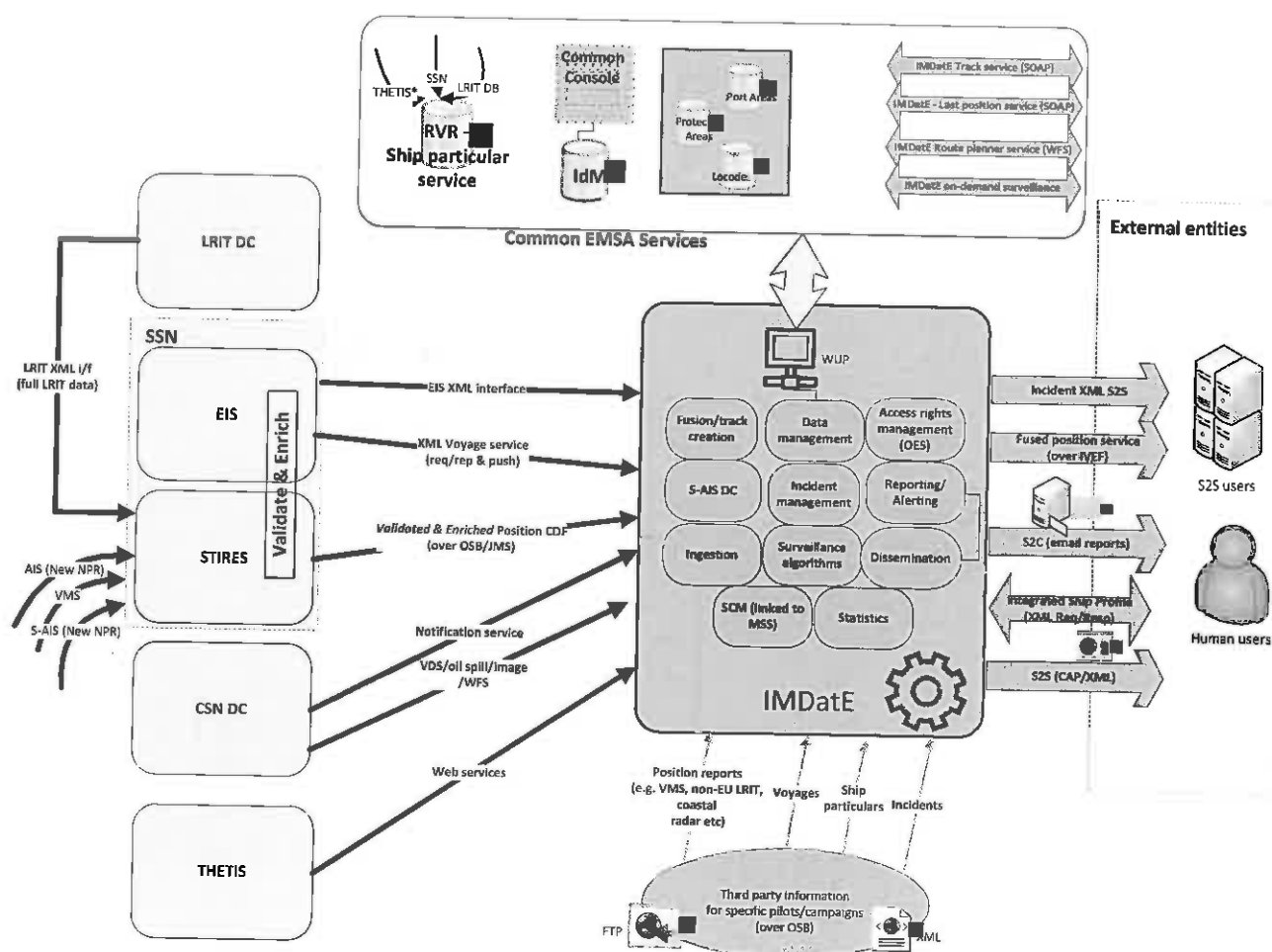
- SafeSeaNet
- THETIS
- CleanSeaNet
- EU Long-Range Identification and Tracking Cooperative Data Centre (EU LRIT CDC)
- VMS systems located in the Member States and other EU bodies.
- IMO LRIT distribution facility
- National position reporting systems (patrol vessels, pollution response vessels etc)
- Commercial and national Satellite AIS providers

1.2. SYSTEM ARCHITECTURE

The IMDatE system is designed following an event driven architecture. On one side external applications provide information (e.g. ship positions or voyages) in native format. These messages are systematically transformed into an XML canonical data format (CDF) and transmitted further into the processing pipeline via the Java Messaging System (WebLogic implementation).

The processing pipeline for each type of data is composed of a set of processing and transformation stages interconnected via JMS with CDF payload in pipes and filters architecture. The processing results are selectively stored in a central database and distributed to internal and external endpoints.

All critical components (Web Logic application servers, Messaging Servers, applications) are redundant and in high availability configuration. An enterprise service bus (Oracle Service Bus) is used to provide location transparency and processing pipeline configurability.



1.3. SOFTWARE AND TECHNOLOGIES USED

IMDatE uses the following software products and versions (where no version is specified the version is under review):

- WebGL for web client visualisation
- WebLogic Server Version: 10.3.4.0
- ORACLE RAC Database version: 11gR2
- Liferay Portal Enterprise Edition: 5.2 EE SP5 (upgrade to the newer version 6.1EE is foreseen during this year)
- Oracle Service Bus Version: 11.1.1.3
- RedHat Linux 6.2
- Oracle Complex Event Processor (TBD)
- Oracle Entitlements Server 11g (11.1.1.5)
- Oracle Coherence (version TBD)
- MySQL
- Jasper reports
- Zorba XQuery processor
- GeoServer
- Nagios

IMDatE is integrated with EMSA Identity Management framework (shared with other applications):

- Oracle Access Manager 10gR3 (10.1.4.3.0)
- Oracle Identity Management 10gR3
- Oracle Internet Directory 11g R1 (11.1.1.3 – 11.1.1.5)
- Oracle Virtual Directory 11g R1 (11.1.1.3 - 11.1.1.5)

1.4. SYSTEM PERFORMANCE AND AVAILABILITY

The system is designed to have the following system performance and availability:

- 95% availability over a year.
- Ingest up to 80 positions messages per second
- Operate with 250 concurrent users.

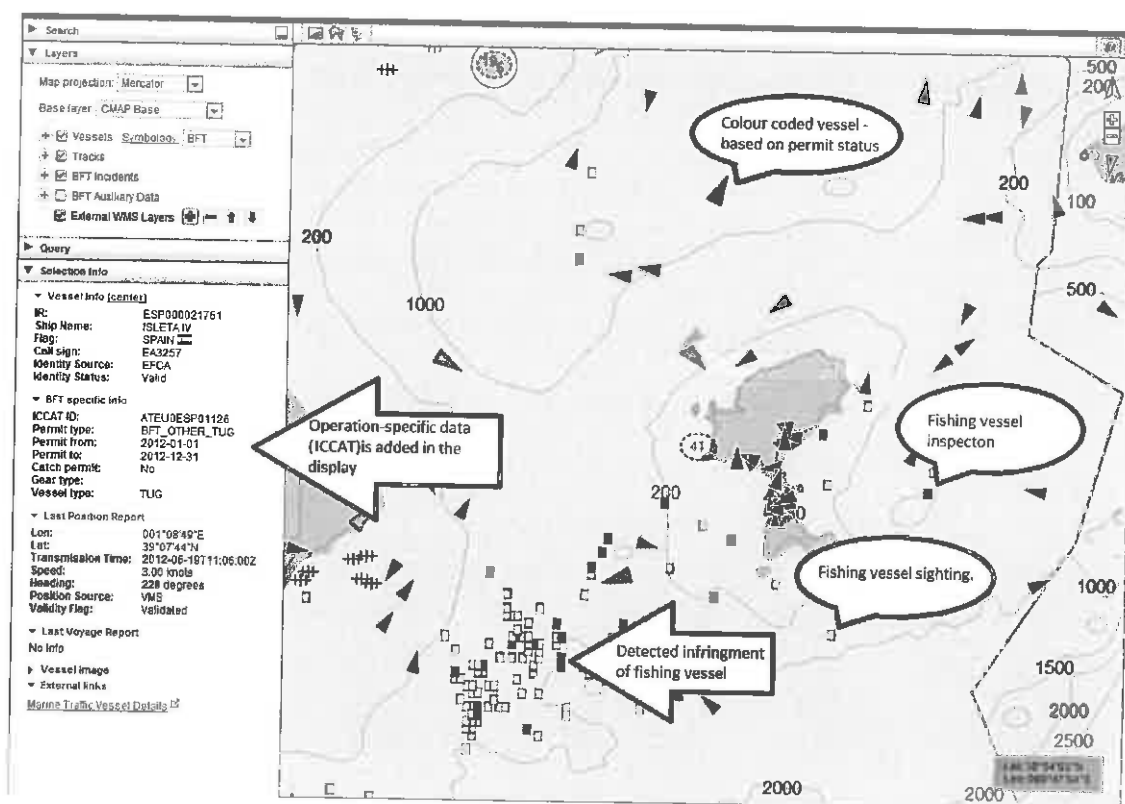
1.5. USER INTERFACE

The IMDatE provides a web based user interface implemented via a set of portlets in the EMSA enterprise portal (Liferay).

The main portlet is a map-centric view with additional information panels such as:

- Selection information
- Map Search
- Available queries
- Map Layers
- Time view

This portlet can be configured for serving different user communities by the concept of 'Operations'. An Operation defines a set of features and configuration options defining the symbols, labels, available menu options and user interface elements. The image below shows a typical map view with panels and symbols that are customised according to the specific Operation. This configuration allows customised services to be delivered to new users in the order of weeks rather than months.



A fine grained authorisation engine, based on the Oracle Entitlement Server, implements the policies authorising the access to the different user interface resources for each given user

**Sub- Appendix E.7 to
Appendix E
of the Tender Specifications**

**THETIS Technical Overview
Tender EMSA/OP/11/2016**

Table of Contents

| | |
|--------------------------------------|----------|
| 1. Technical Overview | 2 |
| 1.1 Technology Summary..... | 2 |
| 1.2 Environment..... | 2 |
| 1.3 Current Metrics | 3 |
| 2. Licenses..... | 4 |
| 2.1 Main System | 4 |
| 2.2 Oracle Identity Management | 4 |
| 2.3 Mobile Client | 4 |
| 2.4 Liferay | 5 |
| 2.5 Jaspersoft | 5 |
| 2.6 Build Environment..... | 5 |

1. Technical Overview

This part gives background on the information system THETIS and presents an overview of the technical landscape of THETIS.

The European Maritime Safety Agency (EMSA) was established under Regulation 1406/2002/EC for the purpose of ensuring a high, uniform and effective level of maritime safety. Among its tasks, the Agency has been entrusted with the project management and operation of the information system THETIS in order to help the Member States of the Paris MoU (PMoU) in the implementation of the new regime of port State control inspections. The system supports the implementation of Directive 2009/16/EC on Port State Control as amended including its Implementing Regulations, Directive 99/35/EC on a system of mandatory surveys for the safe operation of regular ro-ro ferry and high-speed passenger craft services, and relevant elements of Regulation 319/2009 on Common Rules and standards for Recognized Organizations and Directive 2009/17/EC establishing a Community vessel traffic monitoring and information system as well as the provisions laid down in the text of the memorandum of the Paris MoU. THETIS serves as an information source to facilitate the Port State Control inspection in the broadest sense, and is designed to handle various data simultaneously and keeps necessary separation of information, for instance the support of the implementation of Directive 2012/33/EU amending Directive 1999/32/EC as regards the sulphur content of marine fuels and for support of the implementation of Directive 2000/59/EC as regards the Port Reception Facilities in module THETIS EU. The system has the capacity to interface with other national, community and international maritime safety-related databases or information systems. For instance, information on ships in the system is enriched with information from other sources such as the databases of the Recognised Organisations, the IMO GISIS database or the SafeSeaNet system.

1.1 Technology Summary

The THETIS system and its module THETIS EU are Java web applications, running on WebLogic application server that stores and updates data in an Oracle database.

The system is using Liferay portal for the human interface. The JQuery technology, which until now supports the THETIS user interface tier, is currently being replaced by the ExtJS framework, thus replacing all of the existing portlets with new versions of those portlets based on ExtJS version 5.x.

The integration is done with WebLogic Integrator.

The user management is done through OAM (Oracle Access Manager for Single Sign On) and OIM (Oracle Identity Manager for Identity management).

The BI reporting is done using Jaspersoft tools.

The Mobile Client for usage in an offline environment is done using Adobe Air.

1.2 Environment

The development and testing is performed at Development Contractor's site and on Development Contractor's environments, while verification for acceptance and final production are performed at EMSA premises and on EMSA environments by EMSA personnel in conjunction with representatives from the Member States and intra muros consultants.

THETIS environments at EMSA:

- Test,
- Training,
- Pre-Production (clustered),
- Production (clustered).

THETIS Pre-Production and Production environments are made of portal cluster (runs Liferay), load balancer cluster, business cluster, RAC database and WLI cluster for system to system interfaces (interface with the SSN application, and other webservice) and sftp server cluster.

1.3 Current Metrics

THETIS - Current Source Code Metrics

| | |
|-------------------------|--------|
| Number of Lines of Code | 229585 |
| Number of Files | 3735 |
| Number of Classes | 3079 |
| Number of Methods | 19487 |
| Number of Accessors | 9502 |

THETIS - Current Database Metrics

| | | |
|------------------------|------------------|--------|
| Schema PSC_Operational | Number of Tables | 310 |
| | Size | 62 GB |
| Schema PSC_Historical | Number of Tables | 223 |
| | Size | 62 GB |
| Schema PSC_Batch | Number of Tables | 54 |
| | Size | 161 MB |

THETIS EU - Current Source Code Metrics

| | |
|-------------------------|-------|
| Number of Lines of Code | 30768 |
| Number of Files | 428 |
| Number of Classes | 399 |
| Number of Methods | 2185 |
| Number of Accessors | 1679 |

THETIS EU - Current Database Metrics

| | | |
|----------------------------|------------------|--------|
| Schema SULPHUR_Operational | Number of Tables | 30 |
| | Size | 550 MB |
| Schema SULPHUR_Historical | Number of Tables | 19 |
| | Size | 537 MB |

2. Licenses

2.1 Main System

| Licence Name | Version |
|--|---|
| WebLogic Server Version: Java Application Server for the Portal, Business and Integration tier | 12.1.2.0.0 (upgrade to the newer version is foreseen during 2016) |
| Java version | 1.7.0_65 64-Bit (upgrade to new patch set are applied regularly) |
| Oracle Database version (running on Exadata) | 11.2.0.4.5 (upgrade to 12c planned for 2016) |
| Liferay Portal Enterprise Edition: Portal framework shared across several applications | 6.2 EE (latest patches applied and regularly upgraded) |
| Oracle Service Bus Version: integration layer | 11.1.1.3 |
| openLDAP: Maritime applications user repository | 2.4 |
| ProFTP: sftp server | |
| RedHat Linux: operation system | 6.4 (upgrade to version 7 foreseen) |
| Sencha ExtJS version | 5.0 |

2.2 Oracle Identity Management

Changes to the User Management with new functionalities and possible access restrictions (data restrictions or functionality restrictions) inside the application will have to be addressed by the Contractor at application level.

| Licence | Version |
|----------------------------|------------------------------|
| Oracle Access Manager | 10gR3 (10.1.4.3.0) |
| Oracle Identity Management | 10gR3 |
| Oracle Internet Directory | 11g R1 (11.1.1.3 – 11.1.1.5) |
| Oracle Virtual Directory | 11g R1 (11.1.1.3 - 11.1.1.5) |

Project to upgrade IdM suite to 11gR2 (or later) will run during 2016.

2.3 Mobile Client

| Licence | Version |
|-----------|---------|
| Adobe Air | 4.0 |

2.4 Liferay

| Licence | Version |
|-----------------------------------|---------|
| Liferay Portal Enterprise Edition | 6.2 EE |

2.5 Jaspersoft

| Licence | Version |
|---|---------|
| Jaspersoft BI JasperAnalysis Professional | 5.6.0 |
| Jaspersoft ETL (TIS) (Enterprise Edition) version | 5.2.2 |

2.6 Build Environment

| Licence | Version |
|---|---------|
| Red Hat Enterprise Linux Server (Tikanga) | 5.4 |
| Apache Maven | 3.0.5 |
| Apache Ant version | 1.8.4 |
| Apache Archiva | 2.1.1 |
| Hudson | 3.2.1 |
| Sonar | 4.5.2 |
| Subversion | 1.8 |
| TeamForge | 8.1 |

European Maritime Safety Agency

Praça Europa 4
1249-206 Lisbon, Portugal
Tel +351 21 1209 200
Fax +351 21 1209 210
emsa.europa.eu



