PARTNERS
GMVIS SKYSOFT, S.A.
TIS.pt

Prepared by: **GMV**
Code: **EMSA.FWC.L2.R5.RES.DD.D5.2**
Date: **September 23rd, 2014**
Version: **1.8**

EUROPEAN MARITIME SAFETY AGENCY

STUDY TO ASSESS THE FUTURE EVOLUTION OF SSN TO SUPPORT CISE AND OTHER COMMUNITIES

EMSA ITT No. EMSA/OP/07/09/Lot2/RFP 5

FINAL REPORT

GMVIS SKYSOFT, S.A.
Av. D. João II, Lote 1.17.02, Torre Fernão Magalhães -7º, 1998-025 Lisboa
Tel. +351 213829366; Fax. +351 213866493 - www.gmv.com

INNOVATING SOLUTIONS

TRANSPORTES, INOVAÇÃO E SISTEMAS

MOVIMENTO INTELIGENTE

DOCUMENT STATUS SHEET

Version	Date	Pages	Changes
1.8	2014/09/23	140	Final minor editing and publication as “Final Report”.
1.7	2014/09/15	141	Additional language review.
1.6	2014/07/14	142	Layout editing and language review.
1.5	2014/07/02	139	Review of Executive Summary.
1.4	2014/05/16	140	Further comments from EMSA.
1.3	2014/05/05	134	Comments from DG MARE. Overall review of document.
1.2	2014/02/28	127	Further comments from EMSA.
1.1	2014/02/24	126	Initial comments from EMSA.
1.0	2014/01/28	129	First version for review.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1
EXECUTIVE SUMMARY

This study was undertaken as part of a Delegation Agreement between the European Commission (EC) and EMSA, as a result of Action 3.1 of the *Commission Implementing Decision of 12.3.2012 concerning the adoption of the Integrated Maritime Policy work programme for 2011 and 2012* ("IMP Work Programme").

The ad hoc steering committee of the project was established by DG MOVE and includes DG MARE and EMSA with the study being performed by an independent consulting team consisting of GMV and TIS.

GMV (www.gmv.com) is a privately owned international technological business group in the sectors of Aeronautics, Banking and Finance, Space, Defence, Health, Security, Transportation, Telecommunications, and Information Technology. In the maritime sector, GMV provides technological solutions (AIS/VTS, DGPS, ERS and bespoke systems) and consultancy services for national and international organizations on issues like IT and business strategy, security and innovation.

TIS (www.tis.pt) is consultancy company specialised in Mobility and Transport, and provides services in areas related to Transport Economics, Logistics, Energy and Environment, Sustainable Mobility, Collective Transports, Traffic Engineering, Urban and Regional Development and Regulation and Policies.

The overarching conclusion of the assessments performed is that the SSN ecosystem has the appropriate technical capabilities to exchange the data [more likely to be shared] with other user communities which are supporting the development of a Common Information and Sharing Environment (CISE) for the maritime domain, since it:

- Is established and operational 24 x 7 x 365 and accessible by all EU Member States as well as relevant EU bodies/organisations;
- Supports and feeds information exchange by/between all maritime user communities through operational services built up over time in accordance with their needs. These services are:
  - Adapted to the specific needs of each user community;
  - Standards-based;
  - With appropriate security and access management policies;
- Is largely aligned with CISE:
  - Fulfils 8 out 9 CISE Principles;
  - Fulfils 29 (out of 41) CISE Requirements, partly fulfils 7 and does not fulfil 5;
  - Around 72% of the CISE "data groups more likely to be shared" are already available in or through the SSN ecosystem;
- Possesses the technical capabilities and the flexibility to evolve in accordance with the needs of different user communities.

The European Commission 2009 Communication "Strategic goals and recommendations for the EU's maritime transport policy until 2018"[1] sets out the key areas for action by the EU to strengthen the competiveness of the sector. One of the key actions is the integrated information system; the creation of a platform to ensure the convergence and interoperability of maritime systems and applications, including space-based technologies, coupled with appropriate management, building on resources available (SSN, LRIT and CleanSeaNet, Satellite-AIS etc.) to enable enhanced surveillance of maritime transport (goods and passengers) and maritime traffic (vessels). The Communication suggest that the SSN [ecosystem], should be used by all relevant users and be developed further to function as the main platform for maritime information exchange in the EU.
The 2011 White Paper for the future of transport[2] reiterates the development of Union Maritime Information and Exchange system into the core system for all maritime information tools needed to support maritime safety, security and the protection of the marine environment from ship-source pollution, and beyond.

In addition, the 2013 Communication on Blue Belt[3], a single transport area for shipping, building on the earlier Communication on establishing a European maritime transport space without barriers[4], both point to Union Maritime Information and Exchange system as the 'tool' enabling the sharing of the information supporting the different authorities in their operational functions and tasks.

Furthermore, the Communication of October 2009, "*Towards the integration of maritime surveillance: A common information sharing environment for the EU maritime domain*"[5] sets guiding principles on how to achieve integration of maritime surveillance information through the development of a "Common Information Sharing Environment" (CISE). CISE is defined as *a voluntary collaborative process in the European Union seeking to fur-*

[1] COM(2009)8 final.

[2] "Roadmap to a Single European Transport Area – Towards a competitive and resource efficient transport system": COM(2011) 144 final.

[3] COM(2013) 510 final.

[4] COM(2009) 10 final

[5] Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions: "Towards the integration of maritime surveillance: A common information sharing environment for the EU maritime domain". COM(2009)538 final.

ther enhance and promote relevant information sharing between authorities involved in maritime surveillance. It is not replacing or duplicating but building on existing information exchange and sharing systems and platforms. Its ultimate aim is to increase the efficiency, quality, responsiveness and coordination of surveillance operations in the European maritime domain and to promote innovation, for the prosperity and security of the EU and its citizens.

The same Communication also states that "*the Community system SafeSeaNet (SSN) should be used by all relevant user communities and be developed further to function as the main platform for information exchange in the EU maritime domain with regard to port arrival and departure notifications, notifications on dangerous goods, maritime security notifications, incident and accident information, AIS, LRIT and pollution monitoring.*"

Following the above, it is important to note that the European Parliament and the Council adopted Directive 2010/65/EU on reporting formalities[6]. The purpose of the Directive is to "*simplify and harmonise the administrative procedures applied to maritime transport by making the electronic transmission of information standard by rationalising reporting formalities*". According to the same Directive, Member States have to set up single window systems (National Single Window – NSW) where reporting formalities of ships entering and departing from ports of the EU are fulfilled in electronic format, no later than 1 June 2015.

The SSN ecosystem has been further developed to ensure the exchange of the relevant information from the reporting formalities and in order to demonstrate this, a NSW prototype was implemented by EMSA and is being tested in operational conditions.

The purpose of the current study – as defined in the Terms of Reference (ToR) and in accordance with the Action 3.1 of the IMP Work Programme – is to assess and evaluate the potential of SSN (understood in a wider context as the overall EMSA information systems[7]) to support a CISE, and to demonstrate how this SSN ecosystem can serve as a platform which could be of benefit to various end-users (communities).

The report was created based on an exhaustive review of documentation, including EU legislation, communications from the EC and the EU Parliament, EU-level white-papers, CISE roadmap documents, and Technical Advisory Group (TAG[8]) progress of activities, legal records and pilot case results (like the "national single window" demonstrator project). The initial documentation review revealed that in order to support the end objective of the study – "to assess the future evolution of SSN to support CISE and the information exchange with other user communities" – an approach was needed to cater for the fact that CISE is currently a "work in progress". It is continuing to evolve, with a wide range of issues stretching from technical up to governance, are still being discussed within the appropriate fora.

The study focused on identifying:

- The technical capabilities of the SSN ecosystem that already support or can be used to support the information exchange with other user communities;
- The more significant technical developments required of the SSN ecosystem in order to further support CISE;
- The data and information deemed more likely to be exchanged in CISE and within this context which data is already available (or already exchanged) in the SSN ecosystem.

It is imperative to note that the objectives of the study did not include the identification of which "*CISE data is important for each user community*"[9]. Such a task is difficult given the different and varying national set ups for

[6] Directive 2010/65/EU of the European Parliament and of the Council of 20 October 2010 on reporting formalities for ships arriving in and/or departing from ports of the Member States and repealing Directive 002/6/EC.

[7] Hereafter referred as "SafeSeaNet ecosystem". The "SafeSeaNet ecosystem" is the set of maritime information systems and platforms hosted by EMSA which supports the Member States and the Agency's role in general: SafeSeaNet, EU LRIT Cooperative Data Centre, CleanSeaNet (CSN) Data Centre and THETIS as integrated within the IMDatE platform.

[8] The Technical Advisory Group (TAG) is defined in "COM(2010) 584 final" as a group composed of representatives of each User Community, a representative from BLUEMASSMED and MARSUNO as well as the pertinent EU Agencies and initiatives.

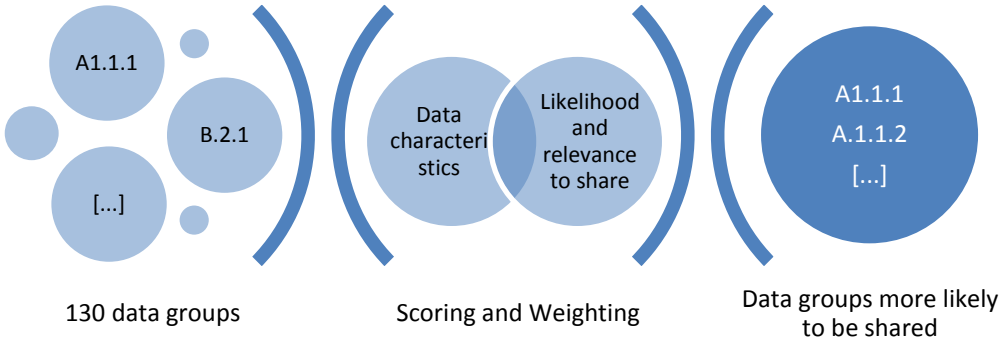
[9] Border Control, Customs, Defence, Fisheries Control, General Law Enforcement (also referred as "Law Enforcement" for short), Marine pollution preparedness and response, Marine Environment (also referred as "Marine Envi-

dealing with maritime monitoring and surveillance (no national set up is the same and information needs vary accordingly between MS, organisations/authorities and user communities). The aforementioned task would have required additional resources, time as well as individual MS, their authorities and administrators, and would have been incompatible with the project planning. The study utilised work already undertaken on this important aspect by other parties i.e. the abovementioned Technical Advisory Group (TAG).

As such, the approach followed by the project team was to identify – starting exclusively from the available CISE documentation that provides the "*inventory of all types of maritime surveillance relevant data across sectors and borders within the EU*" – the "*data more likely to be shared with each user community*", based on criteria that could be evaluated from the mentioned documentation. These criteria addressed issues like the security classification of the data, presence of a legal obligation to collect the data and if it is needed to fulfil operational tasks, if the data is available already in an information system and the spatial coverage and added cost of gathering the data.

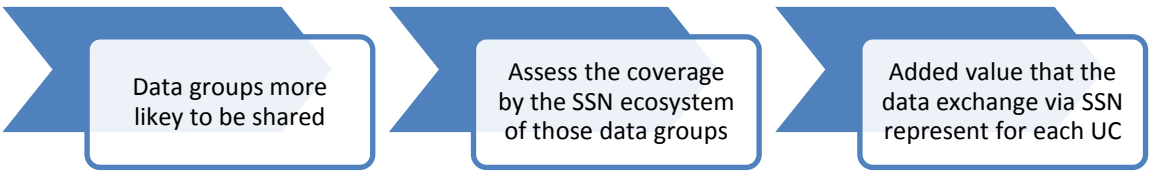
The starting point for the analysis is exclusively the "*Mapping of Data Sets and Gap Analysis*", TAG, Step 2 of the CISE Roadmap dated 08/02/2012, where the TAG identified 500+ data elements as illustrative of the maritime surveillance relevant information already existing across sectors and borders: as referred by TAG "*[…] proposals by TAG have been established on the basis of an illustrative list of 500 data elements. For future operational purposes it may however be useful to reflect on the usefulness to exchange 500+ data elements separately or to regroup a certain number of them into information service packages serving specific maritime surveillance purposes and attach corresponding pre-established access rights to each package".*

For the purpose of this study, the 500+ CISE datasets have been grouped into approximately 130 data groups. Those 130 data groups result from 113 CISE level 2 datasets and 17 CISE level 3 datasets. Despite such level of aggregation, the integrity of all the CISE structure was kept, as no modification to datasets was done.



Two types of variables were considered for the analysis: (1) "likelihood and relevance to share" and (2) "data characteristics", the latter being relevant for the purpose of identifying impacts on the existing system performance (and hence on the technical characteristics of the SSN ecosystem).

A multi-criteria analysis was conducted for the 130 data groups in order to identify which data groups are more likely to be shared between user communities. The initial results of this analysis were reviewed by user community experts (from each one of the seven CISE maritime user communities) and the initial results were reviewed with the inputs provided by those experts.



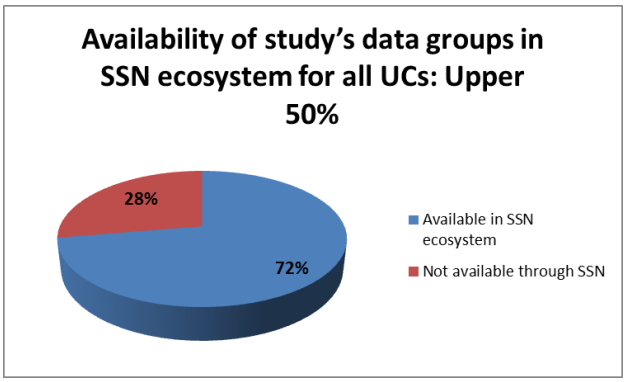
ronment" for short), and Maritime Safety - including Search and Rescue, Maritime Security and prevention of pollution caused by ships(also referred as "Maritime Safety and Security" for short)

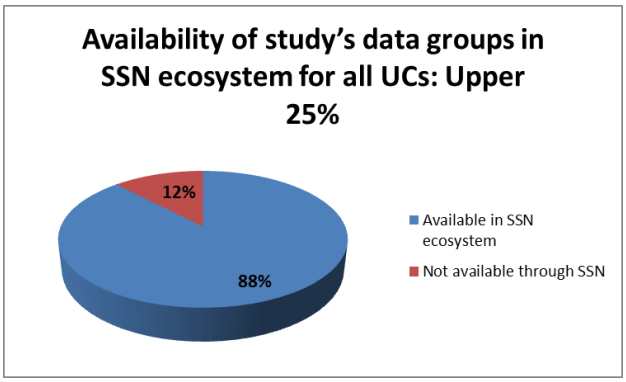
Data groups more likely to be shared (i.e. top results, corresponding to the upper 50% of the 130 data groups) for all UCs, independently on scenario considered, include:

- "Ship position" data;
- "Ship pollution" data;
- "Resources localization for maritime interventions";
- "Maritime infrastructures" data; and
- "Legal maps" data.

The added value that SSN ecosystem possesses for exchanging data with other end-users is evident from the analysis of the current SSN ecosystem "coverage" (understood as the capability to provide or exchange the data) of CISE "data groups more likely to be shared":

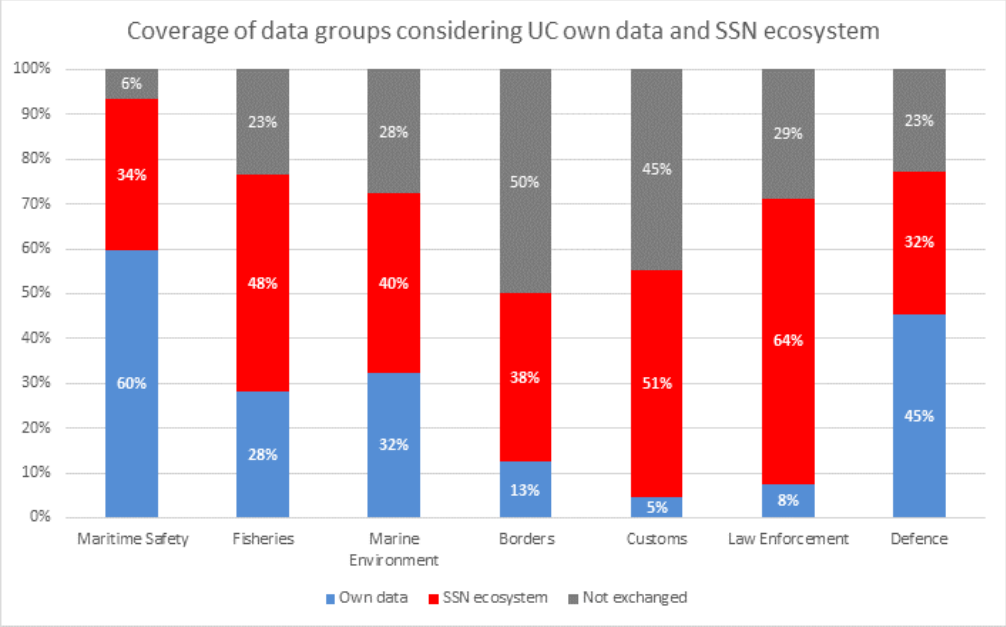
- In the "top 50%" (i.e. the highest ranked 50% of the 130 data groups used in the analysis – "top results"), 72% are available in or through the SSN ecosystem;
- In the "top 25%" (i.e. the highest ranked 25%), 88% are available and/or exchanged in the SSN ecosystem;
- Of the 58 data groups out of 130 where data is available in the SSN ecosystem:
  - 35 are native to the SSN ecosystem;
  - 23 have origin in other user communities;





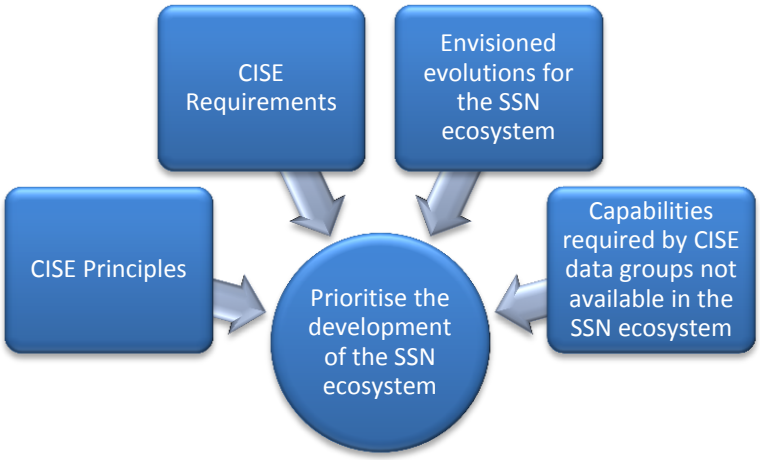
The added value that SSN ecosystem possesses for exchanging data is even clearer when it was evaluated against the data currently owned by each User Community (UC). The data groups covered by the SSN ecosystem represent a substantial value for all the UCs, catering for the coverage of at least more 32% (defence) up to 64% (law enforcement) of data groups most likely to be shared, compared to the ones covered by own data.

At the same time the below figure clearly shows that the two user communities having access to and managing most of the data are Maritime Safety and Defence. Hence there is a gap identified in how the (relevant) information, in particular the one held by the defence, could be exchanged/shared with the other (civilian) communities.



Following the above analysis on the "*data groups more likely to be exchanged*", a "technical analysis" of the capabilities of the SSN ecosystem was performed to identify the pertinent technical evolutions required by CISE. This analysis was performed in two steps:

- Starting from the description of the SSN ecosystem services, functionalities, technical capabilities and supporting infrastructure, the changes required in order to address the shortcomings between the SSN ecosystem and CISE Principles and Requirements were identified and prioritized;
- A ranking of the envisioned developments of SSN ecosystem that are more pertinent to support CISE and deliver benefits to other communities was performed.



The conclusions of the analysis performed about the fulfilment of the CISE Principles and Requirements by the SSN ecosystem are that:

- EMSA's SSN ecosystem has the technical capabilities to fulfil 8 (out of 9) CISE's Principles. The only exception is related to the handling of "highly secure" data, a feature which is not required within EMSA's SSN ecosystem mandate (all systems being "unclassified systems" according to the Commission Decision 2001/844/EC of 29 November 2001);

- Regarding CISE Requirements, the SSN ecosystem fulfils 29 (out of 41), partly fulfils 7[10] and doesn't fulfil 5[11]. The requirements which are not fulfilled are related to a) secure video/audio/instant messaging/white-boarding communication b) handling of sensitive and highly secure information and c) standardised discovery of available information and services.

The "Handling of Highly-Secure Information" can be addressed in the SSN ecosystem through:

- Implementation of a secure information exchange protocol (e.g. "Two-way SSL", "HTTPS over TLS") for all the system-to-system interfaces that handle sensitive and highly-secure information; and
- Provision of Electronic Digital Rights Management (E-DRM) mechanisms, if the need is to control properly not only the system-to-system interfaces but also enforcing access and usage rights on the sensitive information throughout its lifecycle.

It is currently difficult to meet the CISE requirement on the need to "rely on a common data model for information exchanges which is as language-neutral as possible" as the "CISE data model" itself is not yet known. It is expected that the voluntary CISE common data model will "only" define the data fields to be shared between the various systems used by the entities participating in CISE. It will not define what and how each entity should structure the data internally. Therefore, it should be highlighted that all SSN ecosystem applications provide known data models that can be used for information exchange.

Finally, the developments envisaged in the SSN ecosystem that are important for the support of a CISE concept and the information exchange with other end-users are the ones related with:

- **New services** provided by the SSN ecosystem to end-users (including the Maritime Safety one): a Global SAT-AIS data coverage service[12], the implementation of Copernicus Maritime Surveillance Services, an upgraded service for the support of the Fisheries user community, and an upgraded service to support to FRONTEX activities;

---

[10] Partial fulfilment:

- SI9 - CISE must rely on a common data model for information exchanges which is as language-neutral as possible;
- DI3 - CISE must allow looking up what information CISE participants can provide and how they can provide that information;
- DI4 - CISE must allow information providers making available how their services can be used, including parameters such as the refresh rate;
- IA1 - CISE information exchanges must include a confidence value and must indicate who provided it. The confidence value must be a commonly agreed coded value;
- IA2 - CISE information requests must include a priority level reflecting the urgency of the request. The priority level must be a commonly agreed coded value;
- IS5 - CISE information exchanges must respect a commonly agreed information classification scheme supporting security levels from up to EU secret;
- IS7 - CISE must use a messaging protocol that ensures a minimum level of integrity of information exchanges between consumer and provider. The messaging protocol must also ensure higher levels of integrity depending on the classification level of the information.

[11] No fulfilment:

- DI1 - Member States and User Communities must provide one or more points of access that facilitate standardised discovery of the services they provide to CISE participants;
- CO3 - CISE must support secure audio communication;
- CO4 - CISE must support secure video communication;
- CO5 - CISE must support secure instant messaging;
- CO6 - CISE must support secure white-boarding.

[12] Since the launch of the study, the service has been established within the SafeSeaNet ecosystem and is operational.

- **New functionalities** in the SSN ecosystem services, namely the ingestion and processing of new data (e.g. High Resolution Radar and Optical satellite-based sensors for VDS and to detect "marine-based illegal/suspicious/unlawful activity"), new information (e.g. AtoN, AIS-SART, recorded and live video streams, aerial assets tracking information), the exchange of (some) FAL forms through SSN, new LOCODE and AUTHORITIES registries, and an Enhanced Ship Database;
- **Technical evolutions** that improve the availability and sharing of information: namely, the development of "Mobile Applications for accessing the services provided by SSN ecosystem" for smartphones/tablets and a geoportal for information discovery.

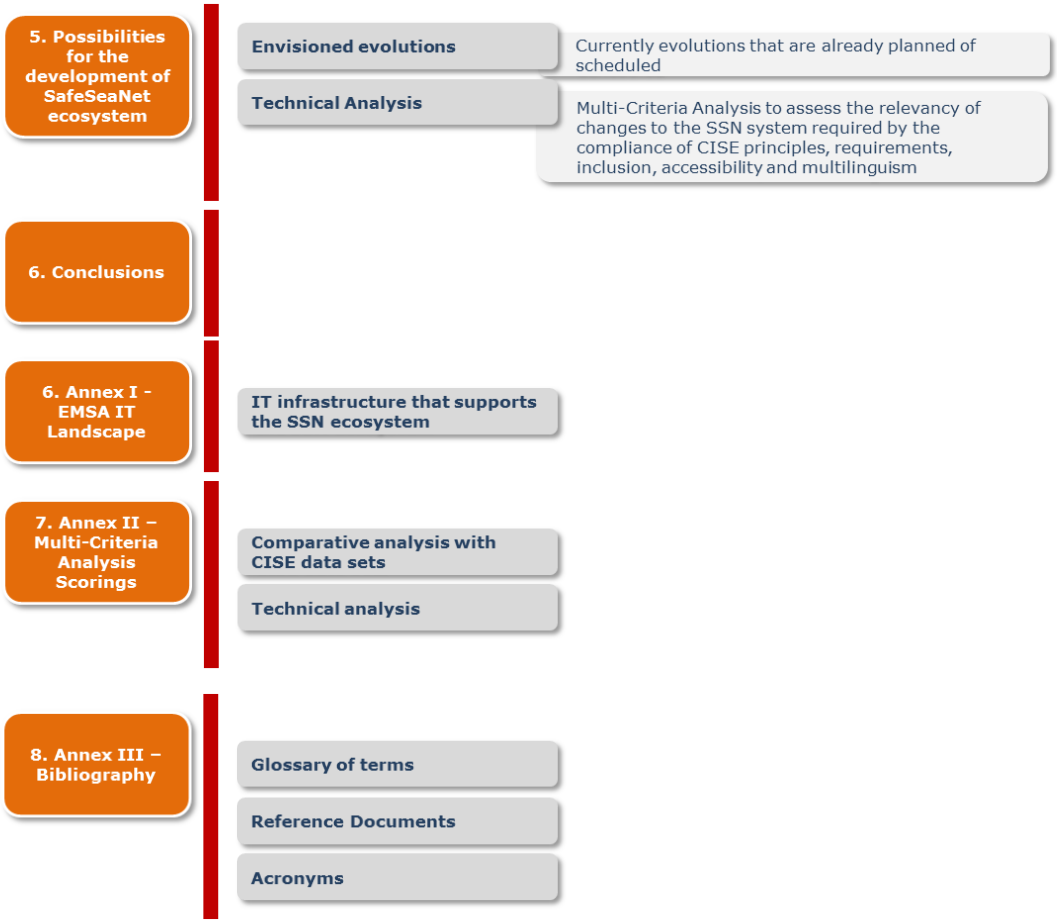
Such developments are in line with the overarching message of the Athens Declaration "Mid-Term review of the EU's Maritime Transport Policy until 2018 and Outlook to 2020" by the Council of the European Union.

CHAPTER 2
INTRODUCTION

This study aims to assess and evaluate the existing and potential capabilities of EMSA's systems and applications to support the overall objectives of the European integrated maritime surveillance initiative, and to evaluate the further development of the SafeSeaNet (SSN) [ecosystem] as a platform which could be of benefit to other user communities in the context of a future Common Information Sharing Environment (CISE).

The study is part of the Commission Implementing Decision of 12.3.2012 concerning the adoption of the Integrated Maritime Policy (IMP) work programme for 2011 and 2012, namely Action 3.1.

This report is structured along eight chapters, the key contents of which are highlighted below.


5. Possibilities for the development of SafeSeaNet ecosystem
Envisioned evolutions
Currently evolutions that are already planned of scheduled
Technical Analysis
Multi-Criteria Analysis to assess the relevancy of changes to the SSN system required by the compliance of CISE principles, requirements, inclusion, accessibility and multilinguism
6. Conclusions
6. Annex I - EMSA IT Landscape
IT infrastructure that supports the SSN ecosystem
7. Annex II – Multi-Criteria Analysis Scorings
Comparative analysis with CISE data sets
Technical analysis
8. Annex III – Bibliography
Glossary of terms
Reference Documents
Acronyms

2.1. BACKGROUND

The European Union and its Member States are at the forefront in improving maritime safety and promoting high-quality standards. The adoption of three maritime packages since 2000 and the establishment of a dedicated agency – EMSA, European Maritime Safety Agency - with the objective of assisting the Commission and Member States in this regard, are illustrative of the efforts and significance that Europe gives to maritime issues.

A considerable number of documents establishing the European Union (EU) policy regarding maritime issues have been published in the last few years: in 2009, the European Commission adopted a Communication and an action plan "*Maritime Transport Strategy until 2018*"[13], which, among other issues, looks to establish a *European maritime transport space without barriers*, aiming to harmonise and simplify administrative procedures for intra-EU maritime transport. In March 2011, the new *White Paper for Transport*[14] was adopted providing the policy response to address some of the challenges confronting the transport sector (i.e. dependency on oil, climate and environmental challenges, congestion and scarcity of funding). For the maritime sector, the White Paper reflects the guidelines formulated within the "*Maritime Transport Strategy until 2018*".

Following the "*Maritime Transport Strategy until 2018*" action plan, the European Parliament and the Council adopted *Directive 2010/65/EU* on reporting formalities of 20 October 2010. Its main objective is to simplify and harmonise the administrative procedures for maritime transport by making the electronic transmission of information standard practice and by rationalising the reporting formalities.

In order to assist the implementation of the reporting formalities Directive, the Commission has also established an expert group on maritime administrative simplification and electronic information services (the eMS group). This group is empowered to develop specifications and services for electronic data exchange and 'single windows' for EU maritime transport. Within this context, EMSA is tasked with supporting the Commission and the Member States in developing these functional and technical specifications.

The European Commission Communication of 2009, "*Towards the integration of maritime surveillance: A common information sharing environment for the EU maritime domain*"[15] sets out to improve maritime surveillance information sharing through an 'environment'. It includes a set of guiding principles for the integration of Maritime Surveillance towards establishing a *Common Information Sharing Environment* (CISE) *for the maritime domain*. The adoption of the draft roadmap on CISE[16] in the subsequent year, reinforces the aim of integrated maritime surveillance as a concept to generate a situational awareness of all activities at sea impacting on maritime safety and security, border control, maritime pollution and marine environment, fisheries control, general law enforcement and defence. This will serve the economic interests of the EU as well as facilitate sound decision making.

The institutional missions of the above authorities, as defined in the Annex of the *"Draft Roadmap towards establishing the Common Information Sharing Environment for the surveillance of the EU maritime domain"*[17] are:

- Border Control:
  - Monitoring of compliance with regulations on immigration and border crossing; support of enforcement operations;
  - Early warning/identification of cases of illegal migration or trafficking in human beings; support of response operations;
- Customs:

[13] COM(2009) 8 final of 21.1.2009.

[14] COM(2011) 144 final of 28.3.2011.

[15] COM(2009) 538 final.

[16] COM(2010) 584 final.

[17] COM(2010) 584 final.

- Monitoring of compliance with customs regulations on the import, export and movement of goods; support of enforcement operations;
- Early warning/identification of criminal trafficking of goods (narcotics, weapons, etc.); support of response operations;

- Defence:
  - Monitoring in support of general Defence tasks, such as:
    - Exercising national sovereignty at sea;
    - Combating terrorism and other hostile activities outside the EU;
    - Other Common Security and Defence Policy tasks, as defined in Articles 42 and 43 TEU.
- Fisheries control:
  - Monitoring of compliance with regulations on fisheries; support of enforcement operations
  - Early warning/identification of illegal fisheries or fish landings; support of response operations.
- General Law enforcement:
  - Monitoring of compliance with applicable legislation in sea areas, where there is policing competence and support for enforcement and/or response operations.
- Marine pollution preparedness and response, Marine Environment[18];
  - Monitoring of compliance with regulations on the protection of the marine environment; support of enforcement operations;
  - Early warning/identification of incidents/accidents that may have an environmental impact; support of pollution response operations.
- Maritime Safety (including Search and Rescue, Maritime Security and prevention of pollution caused by ships)[19].
  - Maritime safety (including search and rescue);
  - Monitoring safety and prevention of pollution caused by ships (crew/passengers, cargo); Support of enforcement operations;
  - Monitoring of the safety of navigation (vessel traffic safety); support of enforcement operations;
  - Monitoring of the security of ships; support of enforcement operations;
  - Supporting safe and efficient flow of vessel traffic; vessel traffic management;
  - Early warning/identification of ships/persons in distress; support of response operations (search and rescue, salvage, place of refuge);
  - Early warning/identification of maritime security threats within the scope of SOLAS Chapter XI-2; support of response operations;
  - Early warning/identification of threats/acts of piracy or armed robbery; support of response operations.

These were used to illustrate the so called 'user communities' in the context of the CISE discussions. It is however important to recall that this does not reflect the reality as no national organisational set up for dealing with maritime monitoring and surveillance is the same and information needs vary accordingly between MS, organisation/authority and user community.

The Technical Advisory Group (TAG[20]) in consultation with user communities represented at the TAG compiled a representative but non-exhaustive inventory of all types of maritime surveillance relevant data across sectors

[18] The user community is also referred as "Marine Environment" for short.

[19] The user community is also referred as "Maritime Safety and Security" for short.

and borders within the EU and combined it in a table with respective sector supply and cross-sectorial demand for such data. The TAG proposed to structure these Data in 3 main "Data Categories":

- **A: Maritime Traffic Data:**
  - Ship Positional Data: this refers to the instant knowledge of the position of the ship. The position update comes either from reports sent by the ship (hence the need to detail the various types of ships as they are not subject to the same reporting obligations), or from non-cooperative detection systems of ships (visual sightings, radars, sonar, electro-optic systems, electromagnetic support measures…). It includes data on the ship activity when it might vary at any time (fishing vessels);
  - Ship Voyage Data: this refers to information valid for a whole journey from one port to the next (route, goods, equipment and people on board) and only updated when a change or a new voyage occurs. It is recognized that Customs Data relate to the whole journey of goods and are not limited to the considered ship voyage; however it remains a convenient way to access it in the context of maritime surveillance.
  - Ship Data: this refers to permanent information on the ship: physical characteristics, ownership, operations, features allowing visual identification, historical data generally found in large databases.
  - Other non-permanent infrastructures at sea: this refers to information on rigs, cages etc. which are not ships but are neither permanently chartered artefacts.
- **B: Maritime Geospatial Data:**
  - Data geo-referenced to the sea floor (in the general meaning of marine charts) irrespective of the passing of ships: hydrographical data, meteo-oceanic data, biological resources, sea bed data etc. again with different degrees of permanency
- **C: Maritime Events Data:**
  - Data required to manage any event at sea calling for institutional attention: safety, law enforcement, pollutions, natural disasters etc.

The SafeSeaNet ecosystem - which in the context of this study comprises all EMSA hosted maritime information systems[21] including SafeSeaNet central system, EU LRIT Cooperative Data Centre, CleanSeaNet, THETIS and the IMDatE platform - is the European Union (EU) "ecosystem of systems" for the exchange and sharing of information between designated authorities and in electronic format, of ship positional data (AIS, Satellite AIS, LRIT, coastal radar, VMS, ship-borne AIS, VDS), ship particulars, logistic and voyage related information, the detection of potential oil spills and involved polluters and to facilitate the planning of ship inspections. The objective of the SafeSeaNet ecosystem is thus to support EU and Member States activities for the purpose of maritime safety, port and maritime security, marine environment protection and the efficiency of maritime traffic and maritime transport.

In addition to its main roles, the SafeSeaNet ecosystem is already a service provider to all seven of the CISE defined user communities.

[20] The Technical Advisory Group (TAG) is defined in "COM(2010) 584 final" as a group composed of representatives of each User Community, a representative from BLUEMASSMED and MARSUNO as well as the pertinent EU Agencies and initiatives.

[21] Developed in full cooperation with all EU Member States to ensure the implementation of Union legislation.

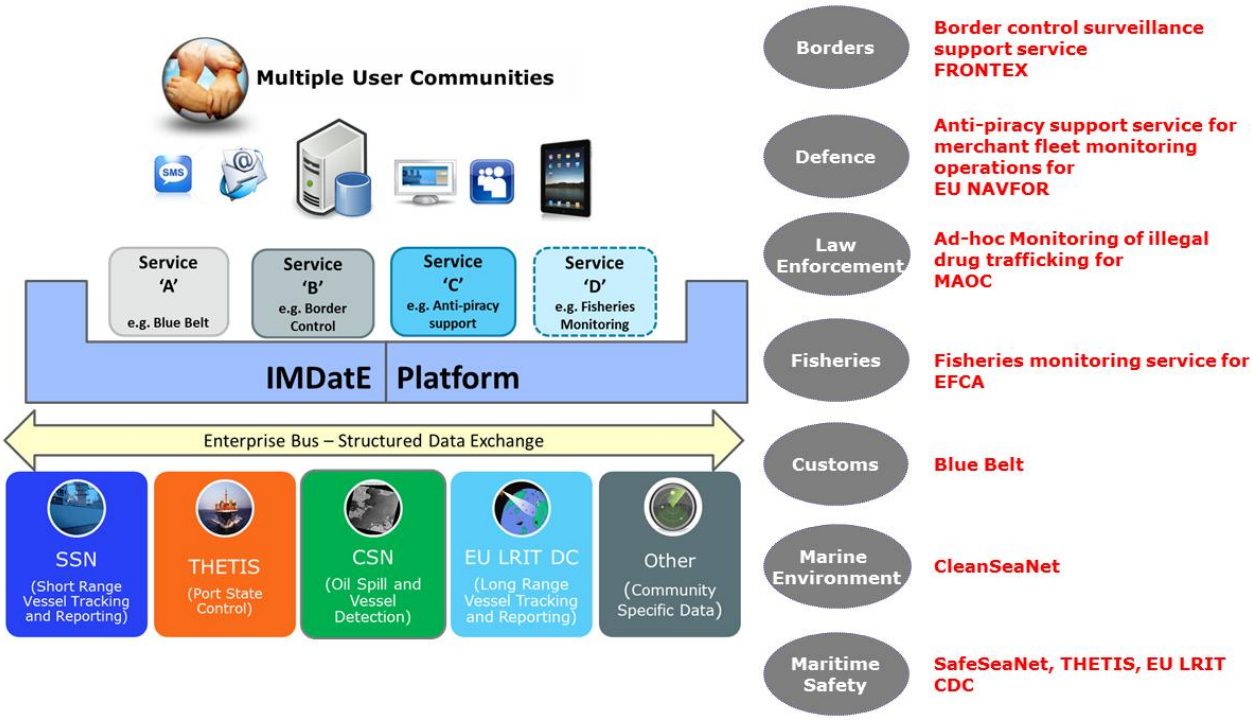


Figure 2-1: SSN ecosystem and services to other user communities

2.2. STUDY OVERVIEW

The purpose of the study was to assess and evaluate the potential of SafeSeaNet ecosystem as regards to:

- Support the development of a CISE;
- Further benefit the other user communities;
- Support related EU Strategies and policies (e.g. the set up at national level of single window systems);
- Further exchange information with other user communities.

The study has four main tasks answering to four specific objectives as depicted in the figure below.

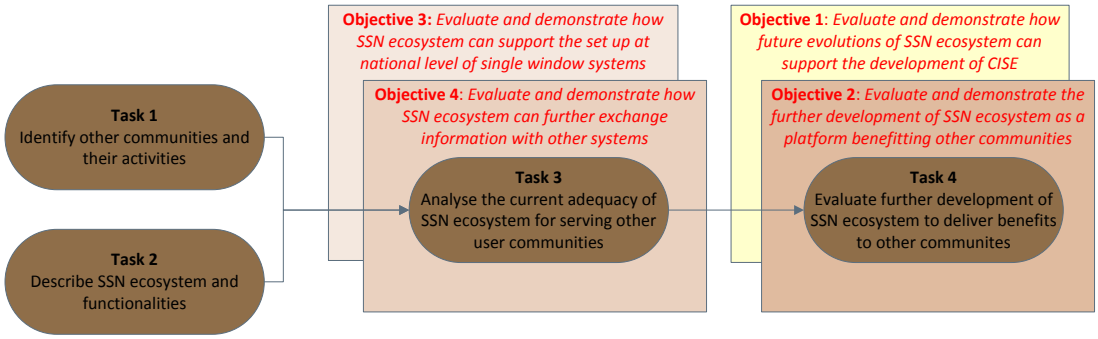


Figure 2-2: Study Tasks and Objectives

The starting point for the study was exclusively the CISE documentation and the TAG data mapping created in Step 2 of the CISE roadmap[22] that establishes:

- 9 principles;
- 41 requirements;
- 500+ data elements.

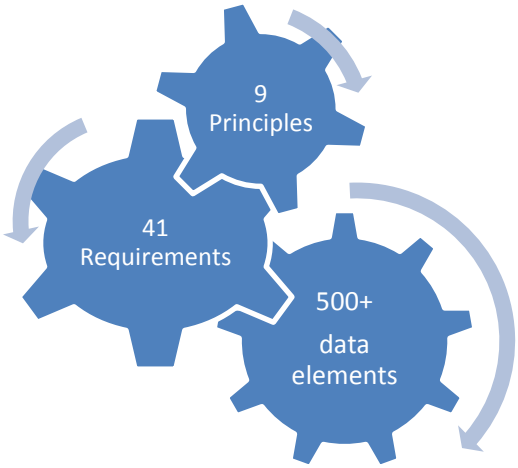


Figure 2-3: CISE Principles, Requirements and Data Elements

The study was performed along two major activities:

- A "comparative analysis with the *CISE data sets*" to establish the changes required in the SSN ecosystem in order to support the information exchange in CISE and with other user communities;
- A "technical analysis" of the capabilities of the SSN ecosystem:
  - Starting from the description of the SSN ecosystem services, functionalities, technical capabilities and supporting infrastructure, the changes required in order to address the shortcomings between the SSN ecosystem and CISE Principles and Requirements were identified and prioritised;
  - A ranking of the envisioned developments of SSN ecosystem that are pertinent to support CISE and deliver benefits to other communities was performed.

The "comparative analysis with the CISE data sets" and the "technical analysis" described above were both based on the use of "multi-criteria analysis" (MCA). This type of method was chosen as it allows a comparative assessment between heterogeneous criteria/objectives resulting in an overall ordering of options; from the most preferred to the least preferred option.

For analysing the preferred options that result from the MCA, it is adopted the median as statistical unit. The median is the middle value of a set of numbers when the numbers are arranged in either ascending or descending order. The median separates the data into two equal halves; 50% of the numbers are below the median, 50% of the numbers are above the median. This unit, given the presence of outliers (i.e. extremely high and/or lower values) is a better indicator for the most typical value of a set of scores. Given this, and since the goal of the analysis was to identify the "data groups more likely to be shared" we selected the "Top 50%" of the *ranked data universe* ("Top Results"), in other words, the results above the median. This sub-set of the results provides a large amount of elements (50% of the total elements in the data set, making it statistically relevant) and also "selects" the elements with the characteristics we would like to further analyse.

[22] *"CISE Architecture Visions Document", version 2.01 dated 25/02/2013*, and *"Mapping of Data Sets and Gap Analysis", TAG, Step 2 of the CISE Roadmap, dated 08/02/2012*.

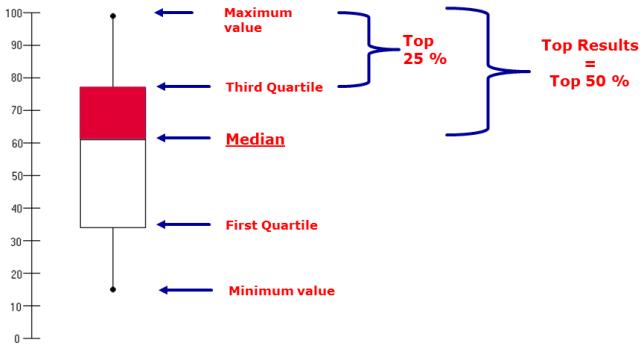


Figure 2-4: Median, "Top Results", "Top 50%" and "Top 25%"

2.2.1. METHODOLOGY FOR "COMPARATIVE ANALYSIS WITH CISE DATA SETS"

For the "Comparative Analysis with CISE data sets", the methodology followed was defined along with EMSA and scoring and validation of the chosen "variables" performed with the support of user community experts (from the seven CISE user communities)[23]. The references/starting points for this "comparative analysis" was:

- *"CISE Architecture Visions Document"*, version 2.01 dated 25/02/2013;
- *"Mapping of Data Sets and Gap Analysis"*, TAG, Step 2 of the CISE Roadmap, dated 08/02/2012;

The assessment conducted in the framework of current study shows that current situation is too fragmented and a need to categorise, prioritise and thereafter classify the different data elements in order of relevance vis-à-vis: a) the scope and objective of the study, and b) the principles and requirements of CISE was identified.

In the above documents, the TAG compiled a representative but non-exhaustive inventory of all types of maritime surveillance relevant data across sectors and borders within the EU. Elements are grouped in 3 "Data categories" and each category is subdivided in data groups:

- A: Maritime Traffic Data: Ship Positional Data + Ship Voyage Data + Ship Data + Other non-permanent infrastructures at sea.
- B: Maritime Geospatial Data: Data geo-referenced to the sea floor irrespective of the passing of ships: hydrographical data, meteo-oceanic data, biological resources, sea bed data etc.
- C: Maritime Events Data: Data required to manage any event at sea calling for institutional attention: safety, law enforcement, pollutions, natural disasters etc.

Data groups are subdivided in data sets containing altogether 500 + data elements considered illustrative of what might be accessed through CISE.

For the purpose of this analysis, the 500+ CISE datasets have been grouped into approximately 130 data groups, as in figure below, over which the scoring and weighting methodology is conducted. Those 130 data groups result from 113 CISE level 2 datasets and 17 CISE level 3 datasets[24].

The reasons behind the decision for this grouping were:

- From a concrete perspective, it is clear that within 500 datasets, some data will be more likely to be shared and of more interest than others and accordingly, there is a need to list the "data" in order of these two criterion (likelihood to be shared and interest for the user communities);

[23] Experts participating in this exercise are actively engaged in the activities of the seven UC. They accepted to take part in this exercise on a personnel basis and not formally as UC.

[24] CISE presents 118 datasets of level 2; of those 5 have a desegregation per type of vessel (commercial, fishing, military, government, other type). In those 5 cases, the level of analysis used is the 3rd level which lead to a total of 17 data groups considered (118 -5 +17 = 130).

- In practice, the emphasis placed on the need for an external evaluation in the "comparative analysis" by external user community experts obliged to a pragmatic approach: requesting to external participants a collaborative validation of 500+ datasets along 7 critical variables could increase the level of error and consequently the level of accuracy of the collected results.

Despite such level of aggregation, the integrity of all the CISE structure was kept, as no modification to datasets was done as it could be observed from the figure below.

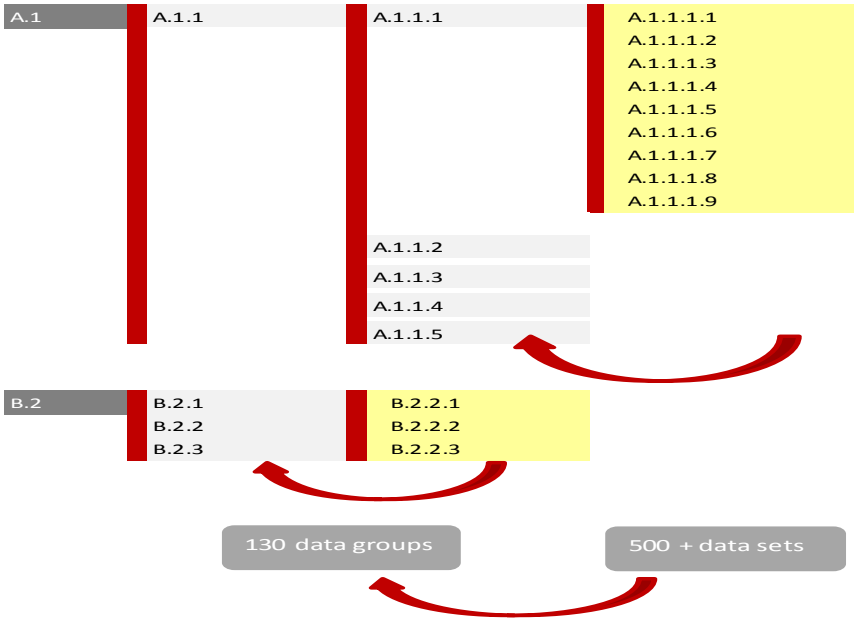


Figure 2-5: Grouping of CISE 500+ data elements into 130 data groups

For the purpose of multi-criteria analysis 2 types of variables were considered: "data characteristics" and "likelihood and relevance to share", although just the second type of variables were object of the weighting analysis: "data characteristics" may generate technical constraints at system level but *in* itself do not reflect a judgment criteria in what regards to the prospect and significance to share the data from the point of view of the user communities. The two types of variables are briefly described:

- *"Likelihood and relevance to share":* these variables reflect the data group's relevancy for the user community and the likelihood of the data group to be shared with other user communities:
  - *"Current level of security classification"*: This variable indicates different security levels at which data can be exchanged (i.e. from non-classified level to secure level), considering the applicable legal restrictions. The lower the data classification (less restrictions), the more likely it could be exchanged between user communities and the higher its associated score.
  - *"Legal obligation to collect"*: Notwithstanding different levels of implementation, legal obligations to collect data increase the likelihood of data exchange: The more relevant the legal obligation, the more likely data will be exchanged and the higher it's associated score. Highest score is given for data collected under EU law (Regulations and Directives). An International Convention transposed to EU law is classified as EU law. Implementation of International Conventions is linked to its ratification by individual MS. Its level of implementation across MS is different as from an EU law. Any obligation, even with a minor implementation facilitates likelihood to share.
  - *"Data availability in existing information systems"*: Availability of data elements in a User Community, particularly data already exchanged in existing system information networks from the different UC, indicates a high potential for exchange with others. Accordingly, a higher associated score.
  - *"Data distribution spatial coverage"*: The wider the existing (or potential) data distribution coverage (i.e. Global), the higher its relevance may be for other User Communities.

- *"Operational use of data group"*: Data requirements for routine monitoring are different of those being necessary for preparedness or on an ad-hoc basis: Routine data needs have the highest value for exchange and associated score.
- *"Data needed to fulfil operational tasks"*: This variable presents an "overall" qualitative assessment on the need and availability of data groups in order to fulfil the operational task(s) of individual User Communities. This could include ancillary data in addition to data generated because of legal obligations.
- *"Cost of gathering data"*: The lower the financial burden for gathering the data, the higher the likelihood to share and the associated score.

- *"Data Characteristics":* these variables reflect basic data characteristics such as "volume", "frequency", and "usage". These variables describe the data and are significant when considering the technical capacity of the SSN ecosystem:
  - *"Frequency of data generation"*: The frequency of data generation reflects the granularity of the data. The intervals considered in the classification are based on the frequencies of data generation by current systems e.g. AIS, VMS, LRIT, VTMIS.
  - *"Data spatial coverage"*: The wider the coverage (i.e. Global) reflects geographical extent for potential operational usefulness. However, a given port may not be interested in the "global maritime picture" but only in the entities that are directly impacting their operation on a given time.
  - *"Data volume generated"*: Similarly to the "frequency", the "volume of data" is a measure of potential of use of that data: the volume of the data is an indication of the potential to generate information. The intervals considered in the classification are based on the volumes of data generation by current systems e.g. AIS, VMS, LRIT, VTMIS.
  - *"Frequency of data need /data use"*: Frequency of data need/use reflects frequency of use/need by each user community: different User Communities may use the same data with different frequency for their activities

It is worth highlighting that the first three categories of the "likelihood and relevance to share" variables are defined upon the classifications provided in the TAG "Mapping of Data Sets and Gap Analysis"[7]:

- *"Current level of security classification"* derives from classifications included in TAG excel under "Current level of EU classification or equivalent" and "Legal restrictions";
- *"Legal obligation to collect"* derives from TAG's "Legal conditions for exchange - EU/ International Legislation for collection and/or exchange";
- *Data availability in existing information systems"*, from "Data availability in existing networks" identified per user community in the TAG documents (i.e. SSN, VMS and E-log books, FIDES, VIS/SIS, etc.).

"Data characteristics" variables, as previously referred are not weighed. This results from the fact that those characteristics do not influence the rankings of the "likelihood to share"; however can influence the system performance (i.e. a high "data volume generated" with a high "frequency of data need" has a different impact on system than a lower volume on "demand" basis)

Notwithstanding the interest to adopt as assessment criteria the *"business value"* of datasets, such analysis is not feasible with current data and without engaging in extended consultations with the different User Communities, falling outside the scope of current study. Taking that aspect into account, a proxy provided by the variable "data needed to fulfil operational tasks" is used. For that, experts were invited to assess if a data group corresponds effectively to a data needed for own mission (independently of being currently available) per comparison with a "wish" list.

Finally it should be referred that comparative analysis reflects the behaviour in "regular" operation, that is, a situation of "normal" exchange of data between the different User Communities, identifying through the above method the data groups more likely to be shared. This perspective differs from the one followed in other exercises, which starts from "Use Case Scenarios" reflecting behaviour under "exceptional" situations (i.e. in case of an accident).

Two weighting scenarios were established to rank the "data groups" more likely to be shared using the "likelihood and relevance to share" variables:

- A *"baseline scenario"* for sensitivity analysis, where all variables have equal weight;
- A *"weighted scenario"* where variables carry different weights, in line with their impact and significance. For example the "Legal obligation to collect", "Data availability in existing information systems", and "Cost of gathering data" variables have higher weights in this model than the other variables.

The weights considered in each of the scenarios are presented in the following table.

Table 2-1: Scenarios and weights

	Weighted	Baseline
Current level of security classification	15,0%	14,29%
Legal obligation to collect	15,0%	14,29%
Data availability in existing information systems	15,0%	14,29%
Data distribution spatial coverage	5,0%	14,29%
Operational use of data group	20,0%	14,29%
Data needed to fulfil operational tasks	20,0%	14,29%
Cost of gathering data	10,0%	14,29%

The "baseline scenario" is used for sensitivity analysis, in other words, to determine how different weights and values of the variables used impact the results of the scoring. The analysis performed showed that the "highest scoring data groups" above the median ("top results") are not sensitive to the weightings: these results are the same independently of the weighting scenarios, what differs is the relative ranking of the data group within the "top results".

Figure 2-6 summarises the methodology followed.

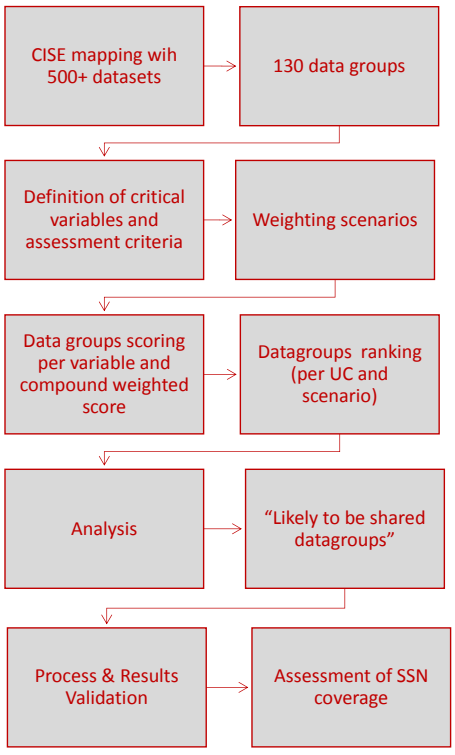


Figure 2-6: "Comparative analysis with CISE data sets" overview

The scoring used for the MCA variables is provided in Section "8.1 - Comparative Analysis with CISE data sets" of this document.

In the analysis performed, the "Top Results" (results above the median[25] or "Top 50 %") were identified as the ones whose relevance and likelihood to share is high. After the identification of these results, the next steps of analysis were:

- An assessment whether data groups more likely to be shared are already covered / provided by SSN ecosystem or through its Maritime Services;
- Same evaluation but excluding from the analysis the data groups that are already owned by each of the UC
- An assessment of the degree of coverage (high /medium /low) for data groups covered/provided by SSN

Throughout this assessment it was possible to measure the actual SSN ecosystem level of coverage for the "top results data groups" but also the added value that data exchange via SSN could represent for each UC (i.e. additional data groups covered when compared to own data).

2.2.2. METHODOLOGY FOR "TECHNICAL ANALYSIS"

In order to prioritise the different developments of the SSN ecosystem to support CISE and further strengthen the exchange of information with other user communities, a multi-criteria analysis was performed on the following aspects:

- Changes required by CISE Principles and Requirements not currently fulfilled or fulfilled partially by the SSN ecosystem;
- Envisioned evolutions for the SSN ecosystem, at:
  - Services level;
  - Functionalities and Technical levels.

Two multi-criteria analyses (MCA) were performed. The first one was used to assess the different possibilities for the development of the SSN ecosystem to support CISE regarding the "*CISE Principles and Requirements*". This MCA used the following variables:

- **Changes to Data Sets**:
  - A change that does not influence the existing data sets is more appropriate than the opposite scenario;
  - A qualitative assessment was performed using *High, Medium, Low, Very Low,* and *None* as *judgement*;
- **Impact Access/Security**:
  - A change that does not influence the existing access rights and security mechanisms of the involved system is more appropriate than the opposite scenario;
  - A qualitative assessment was performed using *High, Medium, Low, Very Low,* and *None* as *judgement*;
- **Impact Capacity**:
  - A change that does not influence the existing required capacity of the involved system is more pertinent than the opposite scenario;
  - A qualitative assessment was performed using *High, Medium, Low, Very Low,* and *None* as *judgement*;
- **Impact Administration/Operation**:

[25] The median is the middle value of a set of numbers when the numbers are arranged in either ascending or descending order. The median separates the data into two equal halves; 50% of the numbers are below the median, 50% of the numbers are above the median.

- A change that does not influence the existing administration and operation procedures of the involved system is more pertinent than the opposite scenario;
- A qualitative assessment was performed using *High, Medium, Low, Very Low,* and *None* as *judgement*;

- **Impact Governance**:
  - A change that does not influence the existing governance structure is more appropriate than the opposite scenario;
  - A qualitative assessment was performed using *Yes* and *No* as *judgement*;
- **Impact Legal Framework**:
  - A change that does not influence the existing EU legal framework for of the involved system is more appropriate than the opposite scenario;
  - A qualitative assessment was performed using *Yes* and *No* as *judgement*;
- **Required system changes**:
  - A change that is less onerous in terms of adaptations to the involved systems is more appropriate than the opposite scenario;
  - A qualitative assessment was performed using *High, Medium, Low, Very Low,* and *None* as *judgement*;

The second MCA was used for the assessment of "*Envisioned Evolutions*" of the SSN ecosystem. This MCA used the aforementioned variables, plus two additional ones:

- **Significance for CISE and other User Communities**:
  - The criterion was used to judge the interest and impact to CISE and the information sharing capabilities with other user communities.
  - A qualitative assessment was performed using *High, Medium, Low, Very Low,* and *None* as *judgement*;
- **User Communities involved**:
  - A change that benefits all CISE user communities is more significant than a change that only affects some.
  - Options are:
    - *All User Communities*
    - *Border Control*
    - *Customs*
    - *Defence*
    - *Marine Environment (only)*
    - *Fisheries Control*
    - *Law Enforcement*
    - *Maritime Safety and Security (only)*
    - *Maritime Safety* and *Security and Marine Environment*[26]

[26] In certain scenarios, for instance oil spills, both user communities can be involved.

2.2.2.1. Weighting for the Variables

As described before, in a multi-criteria analysis (MCA), after identifying the judgement criteria (the "variables" presented previously) it is necessary to *"determine each criterion's relative weight"*. The "criterion's relative weight" are presented in the following sections.

Since the analysis performed was based on qualitative assessments (and not quantitative assessments), the use of a "baseline weighting scenario" for "sensitivity analysis" did not make sense.

2.2.2.1.1. CISE Principles and Requirements

The goal of this MCA was to rank the different changes to the SSN ecosystem in increasing order of impact to the ecosystem (less impact will have the higher rank). In order to achieve this, the higher weight was given to first and foremost to *Required system changes* and then to *Changes to Data Sets, Impact Data Access/Security Policies,* and *Impact Capacity.*

As such, in the *"CISE Principles and Requirements"* MCA, the variables *Changes to Data Sets, Impact Data Access/Security Policies, Impact Capacity, Impact Administration/Operation, Impact Governance, Impact Legal Framework* and *Required system changes* described above were weighted according to the criteria described in the following table:

Table 2-2: Weighting for "CISE Principles and Requirements" required changes

Variable	Weighting
Changes to Data Sets	15 %
Impact Access/Security	15 %
Impact Capacity	15 %
Impact Administration/Operation	15 %
Impact Governance	10 %
Impact Legal Framework	10 %
Required system changes	20 %
Total	100 %

The weightings above fall into three categories (10%, 15% and 20%) and they were selected based on the fact that there are 7 criteria to be judged (which means that if we used equal weights we should use around 14.3%) and the fact that we didn't want to "under\over weight" a specific criteria over the others. As such criteria deemed "normal" were weighted with 15%, criteria with "less significance" where weighted with 10% and the "more significant" criteria was weighted with 20%, hence only having two times the importance of the criteria with the lesser weights.

2.2.2.1.2. SSN ecosystem envisioned evolutions

The goal of this MCA was to rank the SSN ecosystem "envisioned evolutions" in decreasing order of significance for CISE and the sharing of information with user communities: so the higher weight was given to *Significance for CISE and other User Communities* and Required *system changes* and then to *User Communities involved, Changes to Data Sets, Impact Access/Security, Impact Capacity* and *Impact Administration/Operation.*

As such, In the *"SSN ecosystem Envisioned Evolutions"* MCA, the variables *User Communities involved, Changes to Data Sets, Impact Data Access/Security Policies, Impact Capacity, Impact Administration/Operation, Impact Governance, Impact Legal Framework*, *Required system changes* and *Significance for CISE and other User Communities* described above were weighted according to the criteria described in the following table:

Table 2-3: Weighting for "SSN ecosystem envisioned evolutions"

Variable	Weighting
User Communities involved	10 %
Changes to Data Sets	10 %
Impact Access/Security	10 %
Impact Capacity	10 %
Impact Administration/Operation	10 %
Impact Governance	5 %
Impact Legal Framework	5 %
Required system changes	20 %
Significance for CISE and other User Communities	20 %
Total	100 %

The "weighting selection" used here was similar to one described above for the "CISE Principles and Requirements": the weightings above fall into three categories (5%, 10% and 20%) and they were chosen based on the fact that there are 9 criteria to be judged (which means that if we used equal weights we should use around 11.1%): as such criteria deemed "normal" were weighted with 10%, criteria with "less significance" where weighted with 5% and the "more significant" criteria was weighted with 20%. It should be noted that in the weighting used we clearly wanted to "dilute" the impacts on the legal framework and governance with respect to the "required system changes" and "significance for CISE and other user communities" as the former are related with issues that fall outside the realm of the technical developments of the SSN ecosystem.

2.2.2.2. Scoring for the Variables

The scoring used for the MCA variables is provided in "8.2 -Technical Analysis" of this document.

2.2.2.3. Selection of "Top Results"

As with the comparative analysis performed for the "CISE data sets", the "Top Results" (results above the median[27] or "Top 50 %") were selected as the ones pertinent for the implementation in the SSN ecosystem.

[27] The median is the middle value of a set of numbers when the numbers are arranged in either ascending or descending order. The median separates the data into two equal halves; 50% of the numbers are below the median, 50% of the numbers are above the median.

CHAPTER 3
THE SAFESEANET ECOSYSTEM

This chapter provides an overview of the SafeSeaNet ecosystem and its current technical capabilities relevant for the support of CISE and the sharing of information with maritime user communities.

3.1. INTRODUCTION

The "SafeSeaNet ecosystem" is the set of maritime information systems hosted by EMSA which support the agency's role and the Maritime Safety and Security user community in general:

- **SafeSeaNet** – SafeSeaNet (SSN) is the EU system for the exchange, in electronic format, of vessel and voyage related information between designated authorities within the European Union. The objective of SSN is to support EU and Member States´ activities for the purpose of maritime safety, port and maritime security, marine environment protection and the safety and efficiency of maritime traffic. SSN was initiated in October 2004 and became fully operational in 2009. Currently the SSN central node is managed and operated by EMSA. It is an internet based system with distributed databases. The data exchanged include Automatic Identification System (AIS) data, ship MRS notifications, incident reports, port notifications and hazmat notifications.
- **EU LRIT Cooperative Data Centre** – The Long-Range Identification and Tracking (LRIT) of all EU flagged vessels is performed worldwide by the EU LRIT Cooperative Data Centre (CDC). The EU LRIT CDC is hosted and managed by EMSA. The EU LRIT CDC is a central application taking care of capturing, storing and distribution of LRIT data with other international LRIT data centres globally. Equipment on board of vessels automatically submits ship identification and position data via satellite to the EU LRIT CDC, from where it can be accessed by the Member States.
- **CleanSeaNet** - CleanSeaNet (CSN) is the European, satellite-based, oil spill and vessel detection service. It offers assistance to participating States in the identification and tracking of oil pollution on the sea surface, monitoring accidental pollution during emergencies and contributing to the identification of polluters. The images captured by Synthetic Aperture Radars (SAR) on-board satellites are transmitted to the nearest ground station where they are processed and interpreted by designated service providers and then sent to CleanSeaNet. If an oil spill is detected, alert information will be sent by CleanSeaNet to the pollution control authorities of Member States. On top of oil spill alerts, CleanSeaNet also provides slick position and shape, as well as wind and wave data. Member States can access the application via the web-based portal or via a system-to-system interface using web services. Vessels appearing in satellite images can be identified by correlating the satellite data with AIS data from SafeSeaNet. CleanSeaNet is a central system with an EU level database.
- **THETIS** - THETIS is a central, web-based system hosted by EMSA which supports the Port State Control inspection regime[28] by facilitating the planning, logging and publishing of vessel inspections. Data regarding the results of inspections are stored in a central database located in EMSA's Data Centre in Portugal and accessed via a web portal. The system serves both the EU Community and the wider region of the Paris Memorandum of Understanding on PSC (Paris MOU) which includes Canada, Iceland, Norway and the Russian Federation.

In order to provide a cohesive view of the above systems (and transform them in a true "ecosystem of systems"), the **IMDatE platform** was developed as an interoperable data exchange platform which brings togeth-

[28] Laid down in Directive 2009/16/EC on Port State Control and its four implementing regulations, Directive 99/35/EC on ro-ro ferries and high-speed passenger crafts, Directive 2009/17/EC on vessel traffic monitoring, Directive 2009/15/EC on Recognised Organisations and the related Regulation(EC) No 319/2009 and, from July 2013, Directive 2009/20/EC on insurance for maritime claims and Regulation (EC) No 392/2009 on liability for the carriage of passengers.

er the existing EMSA monitoring and tracking systems that are used for maritime safety, security and protection of the marine environment (the above mentioned SSN, CSN, EU LRIT CDC plus THETIS). IMDatE is not a new stand-alone system and it does not aim to replace any of the existing EMSA systems. IMDatE is the technical framework that enhances existing capabilities and brings new services to the EMSA's maritime surveillance portfolio, allowing also the delivery of integrated maritime surveillance services to new user communities.

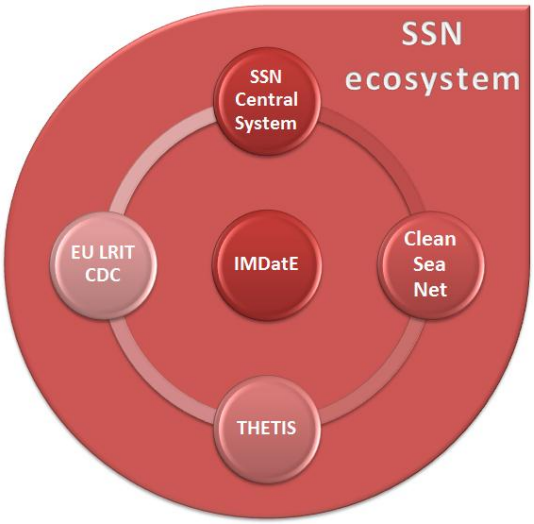


Figure 3-1: "SafeSeaNet ecosystem of systems"

3.1.1. MAIN FUNCTIONALITIES

The main functionalities provided by the "SSN ecosystem of systems" are:

- **SafeSeaNet** enables the EU Member States, plus Iceland and Norway to exchange information on vessel traffic and cargo movements, namely:
  - Port call information: Pre-arrival information sent to ports 24 hours in advance and information on ship arrivals and departures. In addition, 72 hours pre-arrival information for ships eligible for expanded inspection if no other national arrangement is in place;
  - Hazmat information: Information on the carriage of dangerous and marine polluting goods;
  - Incident information: Information on accidents and incidents which have occurred at sea and information on ships which have not delivered their ship-generated waste and cargo residues;
  - Position information: AIS, MRS and LRIT information;
  - To be implemented by 1st of June 2015, SSN will support the exchange of the following additional information:
    - Security information: Prior to ship's entry into a port of a Member State, security information should be sent in accordance with Article 6 of Regulation (EC) 725/2004 taking into account the provisions on exemptions according to Article 7 and the Annex to Directive 2010/65/EC;
    - Waste and cargo residues information: Prior to ship's entry into a port of a Member State, ship-generated waste and cargo residues information should be sent in accordance with Article 6 of Directive 2000/59/EC taking into account the provisions on exemptions according to Article 9.
- **CleanSeaNet** provides support to pollution response operations by:
  - Alerting the Participating State about any possible spill detected by CleanSeaNet including, when available, information on the possible source of the spill;
  - Providing additional information supporting the identification of potential polluters which includes overlaying satellite images with vessel position information provided by SSN;

- Providing a vessel detection system (VDS) service for identification of cooperative and non-cooperative targets;
- Giving access via the CleanSeaNet User portal to:
  - CSN products (SAR images and wind and swell derived data, …)
  - Communication tools for providing feedback and exchanging information between the Participating States and EMSA.

- **EU LRIT Cooperative Data Centre** provides (LRIT) positions of EU flagged ships worldwide and non-EU flagged ships passing or coming to Europe.
- **THETIS**[29] is the information system that supports the Member States of the Paris MoU (PMoU) in the implementation of the new regime of port State control inspections.
- **IMDatE** is not a new system but a platform allowing the above systems and applications to be integrated (as such it is in essence the same as the SSN Eco system) provides relevant and authorised users with information that might be important for improved monitoring/management of events:
  - A single graphical interface to access all maritime data;
  - Ship positioning and ship track data processing (correctness checks, correlation), fusion and enrichment;
  - Automated ship behaviour monitoring and alerts triggered, based on specific criteria such as Area of Interest (AoI), Vessels of Interest (VoI) and Event of Interest (EoI);
  - Integrated Ship Profile that aggregates information on a vessel from all EMSA applications;
  - State of the art System-to-System interfaces that allow the distribution and ingestion of not only basic maritime data but also processed information such as alerts or reports;
  - A Single Sign On mechanism allowing the users entitled to access data in more than one EMSA application to access those system via a single log-in interface;
  - A Satellite AIS (SAT-AIS) data processing module able to process SAT-AIS information from different providers and then distribute the data either as an individual stream or as part of the integrated track;
  - A LOCODEs and Reference Vessel Registry (RVR) databases, providing a consolidated reference registry for LOCODE and ships particulars which could be shared with Member States, contributing to the overall data quality in all systems at central and national level.

3.1.2. MARITIME SURVEILLANCE SERVICES

The following maritime surveillance services were developed and are available today to support user communities:

- **Anti-piracy support service for merchant fleet monitoring operations - MARSURV-1**:
  - MARSURV-1, and its predecessor PIRASAT, have been established in order to develop maritime surveillance support for EU NAVFOR through the integration of different data streams over the coast of Somalia and the Indian Ocean area for EUNAVFOR. The need for developing this type of service was recognised during discussions with EU NAVFOR, who expressed an interest in having combined maritime data products for the Gulf of Aden area. Other stakeholders engaged in maritime surveillance activities in the same area, predominantly EU Member State naval forces, have also expressed an interest in having combined data.

[29] The THETIS system supports the implementation of Directive 2009/16/EC on Port State Control 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.

- The objective of the MARSURV-1 service is to support anti-piracy operations via the correlation and integration of a wide range of vessel reporting information (LRIT, terrestrial AIS, satellite AIS, Mobile-AIS, ship reporting systems) into a customised maritime picture. On-demand, satellite vessel detection data (both radar and optical images) can be integrated in order to detect non-correlated targets in the area of interest.
- The first pilot project established to respond to the EU NAVFOR request (designated PIRASAT-1) ran from September 2009 to March 2010. Its main objective was to demonstrate that different types of ship position reporting data can be fused and correlated with earth observation data in order to produce a more complete maritime picture. The PIRASAT project entered a second phase in June 2010 (designated PIRASAT-2), when new data streams were added and demonstrations began with the Danish navy for data integration collected by on-scene naval assets.
- Following these successful initial pilot projects, EUNAVFOR requested EMSA to continue delivering and upgrading the service as their reference maritime picture for operational purposes. In January 2011 a Technical Cooperation Agreement was signed between EMSA and EUNAVFOR for setting-up a permanent service.
- The MARSURV-1 service started in April 2011 and is still in operation. In August 2012 the Satellite-AIS data stream was included as a permanent feature of the service, the data being procured by EMSA through its own contract with a commercial provider (LuxSpace) and paid by EUNAVFOR. Since January 2013, all MARSURV-1 functionalities are available to EUNAVFOR through the IMDatE platform. In addition, in the current MARSURV-1 service, additional ship contact information and anti-piracy measures undertaken on board are included as well as reported incidents (suspicious approaches, piracy incidents, hijacked vessels, etc.).

- **Border control surveillance support service - MARSURV-2**:
  - Since 2008, FRONTEX has started to work on the establishment of a European Border Surveillance System (EUROSUR) to reinforce the control of the Schengen external border, especially the southern maritime borders. Based on the tri-partite cooperation agreement signed in 2009 between EMSA, FRONTEX and EFCA and in order for FRONTEX to provide the services described under the EUROSUR framework to Member States for the EU maritime borders, EMSA was invited to provide support to EUROSUR. This support started with EMSA's participation in the European Patrol Network INDALO 2011 Joint Operation, through the MARSURV-2 pilot project, which allowed the introduction of FRONTEX surveillance information (visual sightings, interceptions at sea, etc.) into an EMSA pilot service, integrating SafeSeaNet data with satellite surveillance services.
  - In 2013, EMSA and FRONTEX signed a three-year service level agreement, under which EMSA will develop tailored monitoring services, information products and tools. Several sources of data, from EMSA's IMDatE, will be provided to FRONTEX to enable them to construct a more comprehensive overview of activities at Europe's maritime border as well as deliver this information to Member State's NCC's through EUROSUR network.
  - Currently, the FRONTEX service aims to support border surveillance activities performed based on the delivery of system-to-system services for real-time information exchange and analysis of vessel positions based on several data sources such as: Satellite AIS (S-AIS); Terrestrial AIS (T-AIS); Vessel Monitoring Service (VMS); Vessel Detection Service (VDS) from SAR and optical images; Long Range Identification and Tracking (LRIT). This service will contribute to provide an integrated maritime shipping picture to enrich the EUROSUR situational picture. EMSA will deliver services and information products and tools tailored to FRONTEX, for the common application of surveillance tools as well as related information products in to support the border surveillance. Currently, the FRONTEX service covers the Mediterranean and the North Africa/Canarias/Iberian peninsula waters.
  - During 2013, and under specific SLA, has delivered AIS and SAT-AIS WMS layers to support EUROSUR activities. For 2014, EMSA will deliver extra data streams and value-adding services such as LRIT, VMS, VDS as well as Vessel Behaviour monitoring capabilities.

- **Fisheries monitoring service - MARSURV-3**:
  - In order to support the European Commission, Member States and EFCA in a number of Joint Deployment Plan operations (JDP) for fisheries activities in the Mediterranean, North & Eastern Atlantic and the North Sea waters, EMSA developed a service, called MARSURV-3, that:

- Provides a real time maritime awareness operational picture of the target area (based on the data fusion of the different positions data sets, establishing a vessel register with common identifiers for fishery vessel);
- Allow a centralised and rapid access to a wide selection of maritime information;
- Facilitates crosschecking and correlation between VMS, Terrestrial AIS, Satellite-AIS, LRIT and visual sightings;
- Provides for a tool that can be used for behaviour analysis, risk assessment and classification of possible non-compliance;
- Investigates the utility of a general behaviour surveillance tool for fisheries control operations by testing the possibility of detecting non-corresponding data sets, the capacity to detect specific targets and to discriminate them.

– Following the success of the MARSURV-3 service, a number of Member States have requested EMSA to assist them in investigating how SSN ecosystem (on top of which MARSURV-3 is implemented) can further help them in complying with the new EU Fisheries regulations as defined in Regulation CE 1224/2009.

3.1.3. SIGNIFICANT ON-GOING DEVELOPMENTS FOR THE SUPPORT OF CISE AND OTHER USER COMMUNITIES

3.1.3.1. *"Single Window"* for Port reporting formalities and the exchange of FAL documents

It is worth to mention that as a result of "Directive 2010/65/EU on reporting formalities for ships arriving in and/or departing from ports" ([RD.5]) - which has the objective to simplify and harmonise the administrative procedures applied to maritime transport - both the SSN Central System (hosted and managed by EMSA) and the national SSN systems will be upgraded - as soon as possible and in any case no later than 1st June 2015 - in order to support the set-up at national level of a *"single window"* for port reporting formalities and the exchange of FAL documents.

This *"single window"*, linking SSN, e-Customs and other electronic systems, shall ensure that all information is reported once and made available to various competent authorities and the Member States. Member States shall also ensure that information received in accordance with the reporting formalities provided in a legal act of the Union is made available in their national SSN systems and shall make relevant parts of such information available to other Member States via the SSN system.

Within the framework of the Integrated Maritime Policy (IMP) and in accordance with the "IMP work programme 2011 and 2012", ([RD.6]), EMSA has been delegated to implement a pilot project regarding the above mentioned evolution of SSN. The main objective of this pilot project is then to evaluate and demonstrate the setting up of a simplified single window at national level and its interfaces as required by Directive 2010/65/EU. This objective will be met through the development of software and services components that will simulate: a National Single Window (NSW); the distribution of data to national authorities and; the exchange of relevant information via the central SSN Central System.

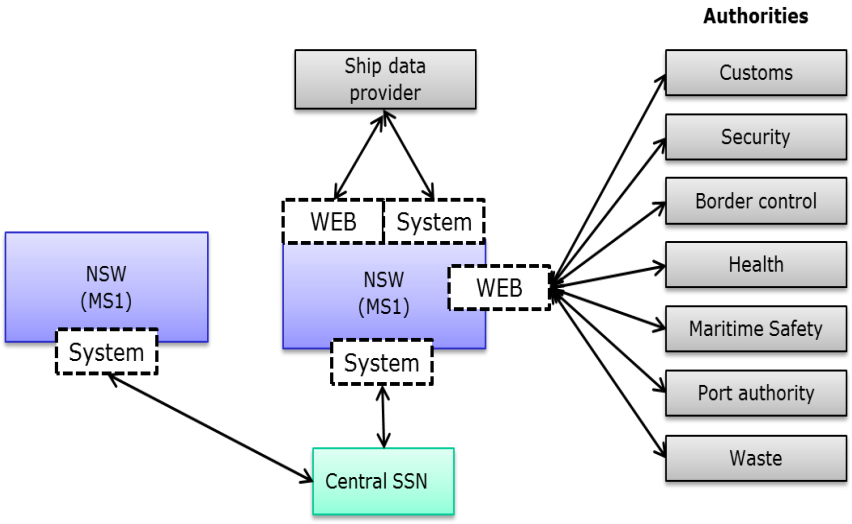


Figure 3-2: Generic architecture for the "SSN and *single window* pilot demonstration project"

3.1.3.2. EMSA's Global SAT-AIS Service

The immense potential of SAT-AIS has also been recognised by the main international fora involved, the International Telecommunication Union (ITU) and the International Maritime Organization (IMO). Both these organisations emphasize the key role that SAT-AIS will play in supporting maritime safety, particularly through its potential to improve Search and Rescue (SAR) capabilities. Additionally, there has already been considerable interest shown in obtaining SAT-AIS data by a wide range of institutional users involved in maritime safety, security and pollution response – such as Search and Rescue, coast guards, port authorities, etc. – as well as those involved in the maritime domain more broadly, such as border and fisheries control, customs, etc.

In terms of providing additional resources in maritime data, the additional SAT-AIS data source would fit well into European Commission policy in general and CISE in particular. This is clear from documents such as the Communication from the Commission on maritime transport policy to 2018[30], which states that, looking ahead, '*the capacities of the EU's maritime transport system should be strengthened by putting in place an integrated information management system to enable the identification, monitoring, tracking and reporting of all vessels at sea and on inland waterways to and from European ports*', adding that '*In a broader context, building on the resources currently available, such as AIS, LRIT, SafeSeaNet or CleanSeaNet, or those that are being developed… the EU should promote the creation of a platform to ensure the convergence of sea-, land- and space-based technologies…*'.

A study entitled 'European space-based AIS system: A user benefit analysis' (launched by EMSA in cooperation with ESA in 2010) identified that over 80% of the respondents stated that they were interested in using SAT-AIS data and acknowledged that a space-based AIS system would provide them with solutions adequate to their needs.

Following this study, EMSA undertook the technical changes that were required to the existing SSN ecosystem in order to enable it to distribute European Satellite AIS information and the SAT-AIS Data Processing Centre (SAT-AIS DPC) was born. The SAT-AIS DPC is able to process multiple inputs of SAT-AIS data streams from a variety of service providers in accordance with the needs of different user communities. EMSA is able to start processing and disseminating SAT-AIS data through IMDatE, either as a unique data stream or in combination

[30] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Strategic goals and recommendations for the EU's maritime transport policy until 2018, COM/2009/0008 final

with existing vessel traffic reporting data, to end users. This can be presented on a specialised web interface, tailored to the users' particular needs.

Currently, IMDatE provides a Satellite AIS (SAT-AIS) data processing module able to process SAT-AIS information from different providers and then distribute the data either as an individual stream or as part of the integrated track. This module will be evolved in the upcoming years (2014 onwards) to provide a service covering the entire globe.

3.1.3.3. Implementation of Copernicus Maritime Surveillance Services

According to the "Proposal for a Regulation of the European Parliament and of the Council establishing the Copernicus Programme and repealing Regulation (EU) No 911/2010" ([RD.33]), *"In the implementation of the Copernicus programme, the Commission may rely, where appropriate, on competent Union agencies, such as the European Environment Agency (EEA), the European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union (FRONTEX), the European Maritime Safety Agency (EMSA) and the European Union Satellite Centre (EUSC) or any relevant body potentially eligible for a delegation according to Article 58 of Regulation (EU, Euratom) No 966/2012 of the European Parliament and of the Council of 25 October 2012 on the financial rules applicable to the annual budget of the Union"*.

Additionally, in the same document it is stated that *"As for the Security strand on maritime surveillance, it is proposed to delegate its implementation to EMSA, the European Maritime Safety Agency. Indeed, EMSA's mandate includes some responsibilities in maritime security and an obligation to assist the Commission in related activities. EMSA has a widely recognised expertise in the implementation of CleanSeaNet, a maritime safety operational programme relying on Earth observations. It is also actively involved in several R&D projects preparing for the Copernicus Security service."*

As such, it is expected that in the near future EMSA will develop through the CleanSeaNet Data Centre and the IMDatE platform relevant capabilities based on Copernicus services and data that will support the work of other European Agencies and User Communities involved and/or with interest in sea or sea-seabed activities.

3.2. TECHNICAL CAPABILITIES

The SafeSeaNet system is designed following the SOA principle of service orientation coupled with an event driven architecture (EDA). On one side external applications provide/request information (e.g. ship positions, "port notifications", satellite imagery and satellite derived data, etc.) in canonical data formats (using system-to-system interfaces like SOAP, Web Services, and others). The information is then processed and transmitted further into the processing pipeline via a messaging system. The processing results are selectively stored in a central database and distributed to internal and external endpoints. An Enterprise Service Bus is used to provide location transparency and processing pipeline configurability.

The SSN ecosystem is able to provide a fully featured "integrated maritime awareness picture" by combining the information available in its core systems. This picture can be tailored to the end users requesting them, including geographical constraints (by member state, by region, etc.) and it is based in tools that harmonise and enhance the presentation of the domain awareness picture and provide the users with the ability to share data for safety, security, the identification of risk, environmental protection and improve logistics management.

Access to the SSN ecosystem can be gained via i) graphical web-based user interfaces, ii) SOAP-based web-services, "bare XML" and other standards-based system-to-system interfaces, and iii) other ways of data export/import such as email, PDF, CSV and other common data formats, etc.

The system-to-system interfaces available in the SSN ecosystem provide the ability of exchanging not only *basic maritime* data (e.g. AIS positions) but also *processed information* such as alerts or reports.

It is important to notice that the SSN ecosystem uses and supports (based on the use of an Enterprise Service Bus and other bespoke tools) key messaging and notifications mechanisms:

- *Notification:* Notification is a messaging pattern where a data provider gathers the necessary information to be reported and send it to the data consumer;
- *Request-Response*: Request-Response is a pattern in which the service consumer uses configured client software to issue an invocation request to a service provided by the service provider. The request results in an optional response;
- *Subscribe-Push*: In this pattern, one or more clients register subscriptions with a service to receive messages based on some criteria.

The SSN ecosystem implements comprehensive security measures ranging from physical access up to logical security: *Organisational Aspects, Access Control, Authentication, Authorisation, Traceability and accountability, Confidentiality, Integrity, Audits* and *Training.*

Access to data sets and functionalities in the SSN ecosystem – the "access rights policy" - follows complex criteria including geographic criteria or nationality of the assets involved in the information. Examples of such criteria include: *Role, Nationality of the asset, Geographic, Destination, Special agreements, EU Institutions,* and *Temporary users*.

Three noteworthy "base registries" are available in the SSN ecosystem:

- Reference Vessel Registry Database (RVR);
- LOCODEs Registry;
- Authorities Registry.

The availability of services within the SSN ecosystem is on "twenty-four hours a day, seven days a week" basis. All critical SafeSeaNet infrastructure (application servers, messaging servers, databases) are redundant and in high availability configuration.

Business Continuity is assured in the SSN ecosystem (along with performance and system availability principles enshrined in the systems) through the following entities:

- Maritime Support Services (MSS) Centre;
- Business Continuity Facility (BCF).

3.2.1. ARCHITECTURAL CHARACTERISTCS

3.2.1.1. SOA Architecture

One of the key technical capabilities of the SSN ecosystem is the use of SOA architecture and SOA tools: through the use of SOA, EMSA can deliver tailor made services in the order of weeks rather than months, all benefiting from the past investment in operational ICT infrastructure, data quality and cross-checking capabilities, and validation by the dedicated EMSA 24/7 Maritime Support Services.

The SOA framework allows EMSA and SSN users to quickly:

- Add additional streams of data (ship borne AIS, ship borne or coastal radar, VMS, etc.);
- Create new alerts and reports (email, PDF, SMS) simply by configuration;
- Configure a new graphical web interface (symbols, associated colours, user provided data);
- Allow user community specific data to be provided and displayed (i.e. ICCAT file and incidents from EFCA, ship registry from EUNAVFOR);

- Set-up ingestion and dissemination of vessel positions in a number of formats/protocols depending on the user needs (vessels characteristics, area, time window, etc.);
- Create a template of automated behaviour monitoring (based on behaviour algorithms);
- Aggregate maritime data from multiple applications (not only coming from SSN Central System, EU LRIT CDC and THETIS but also from other applications).

The value of SOA for the SSN ecosystem originates:

- Simpler systems: Service-oriented architectures are based on industry standards and can reduce complexity when compared with integrating systems on a solution-by-solution basis. They also enable future applications to mesh seamlessly with existing standards-based services;
- Lower maintenance costs: Simplicity and ease-of-maintenance means that support costs are reduced and valuable IT staff can be freed up for other work;
- Enhanced architectural flexibility: Service-oriented architectures support the building of composite solutions that consolidate numerous business processes from multiple systems in a simple user interface;
- Lower integration costs: Service-oriented architectures make it possible for organizations to develop, implement and reuse processes that are technically enabled and integrated through the use of Web services standards such as XML, SOAP and WSDL. In addition, connectivity, data exchange and process integration efforts are simplified, reducing integration-related development and support costs.

3.2.1.2. GIS Capabilities

A Geographic Information System (GIS) is a software system that allows to capture, map, model, query, display and analyse large quantities of geographically referenced information (maps, 3D virtual models, satellite images/data, tables, and/or lists). It can be quickly understood and easily shared.

GIS software most commonly used features are:

- To create and display maps;
- Integrate and display geo-referenced information;

EMSA has available internally a significant geographical information infrastructure that comprises tools from several vendors like ESRI, Jepessen and the open source community (GeoServer). This GI infrastructure serves the following main purposes:

- Supports the "Web Interfaces" of the SSN ecosystem applications;
- Provides Nautical Charts (ship routing systems, navigation aids, nautical background, administrative boundaries, dangerous areas, etc…) to the SSN ecosystem applications;
- Provides geo-referenced basic data (geographical grip – parallel and meridian lines , countries, cities, seas, traffic separation schemes), marine infrastructures data (AIS, stations, …), and ports location data;

The information displayed on the charts is configurable. Usually, the symbols displayed follows the International Hydrographical Organization (IHO) S-52 standard while the level of details follows the Electronic Chart Display and Information System (ECDIS[31]) standards for charts used on-board ships.

3.2.1.3. Enterprise Service Bus

[31] ECDIS (as defined by IHO Publications S-52 and S-57) is an approved marine navigational chart and information system, which is accepted as complying with the conventional paper charts required by Regulation V/19 of the 1974 IMO SOLAS Convention.

One of the key technical capabilities of the SafeSeaNet ecosystem is the use of Enterprise Service Bus (ESB): An ESB is a middleware solution that enables interoperability among heterogeneous environments using a service-oriented model. An ESB models an application feature as a service. The ESB may host the service agent locally, or the service may execute remotely. In both cases, the ESB provides an abstraction layer that virtualizes the service and separates it from infrastructure concerns. The ESB makes the service accessible to other applications via one or more middleware protocols. As a general rule, one of the protocols that an ESB supports is Simple Object Access Protocol (SOAP), but it doesn't require all services to communicate via SOAP. The ESB mediates interactions between service endpoints and enables dissimilar systems to interoperate.

Along with the generic benefits of an ESB, this type of tool provides to the SSN ecosystem an open and generic processing layer for data transformation and routing that allows the tailoring of services for different user communities. The data involved is not only *basic maritime data* (e.g. ship positions) but also *processed information* such as alerts or reports.

3.2.2. USER INTERFACES

Access to the SSN ecosystem can be gained via i) graphical user interfaces, ii) SOAP-based web-services, "bare XML" and other standards-based system-to-system interfaces, and iii) other ways of data export/import such as email, PDF, CSV and other common data formats, etc.

3.2.2.1. Graphical User interfaces

The graphical user interfaces of the SSN ecosystem are mostly web-based: users access the application from any computer connected to the Internet using a standard browser, instead of using an application that has been installed on their local computer. They provide features such as:

- A platform for accessing all (EMSA managed) maritime data on graphical interfaces which can be customised to add new data sources, specific symbols and panel contents;
- Introduction, Visualization and Query of the core data/services available in the SSN ecosystem:
  - Position reports: AIS, S-AIS, LRIT, coastal radar, satellite radar, VMS, ship-borne AIS;
  - Voyage and cargo information (PortPlus information);
  - Port State Control (PSC) information;
  - LRIT (other than position reports);
  - Satellite products (SAR and optical images, VDS and oil spill) and events.
- Ingestion of user specific data:
  - Additional position report feeds, e.g. local AIS feeds, VMS or coastal radar streams;
  - Specific ship particulars;
  - Geo-referenced events e.g. vessel sightings, pollution detection, known infringements.
- Real-time generation of ship tracks:
  - Based on single source of position reports;
  - Based on multiple types of position reports (AIS, LRIT, VMS etc.);
  - Ability to extrapolate (dead reckon) the future vessel position using speed and course, and interpolate between reports.
- Overlay of specific external data using WMS/WFS web services;
- An 'Event Timeline' tool to provide better awareness of temporal events and information.

The advantages of the use of web-based user interfaces are:

- Cost effective development;
- Accessible anywhere;

- Easily customisable;
- Accessible for a range of devices;
- Improved interoperability;
- Easier installation and maintenance;
- Adaptable to increased workload;
- Security.

3.2.2.2. System-to-system interfaces

Interoperability is a key requirement for CISE, and generally, an institution that offers an information infrastructure on which others can build is held in high regard in the community: system-to-system interfaces provide the means to do this. By enabling data sharing between internal IT systems and between one organisation and another, system-to-system interfaces facilitate not only the dissemination of data and information but also the design of cooperative systems in line with the principles of CISE.

Successful implementation of system-to-system interfaces in the SSN ecosystems resulted in a greater flexibility and improved ability to efficiently present outputs as useful and re-usable artefacts, creating an opportunity to share information with other maritime user communities.

The system-to-system interfaces available in the SSN ecosystem provide features such as:

- SSN ecosystem to External Systems:
  - Not only *basic maritime data* (e.g. AIS positions) can be distributed but also *processed information* such as alerts or reports.
  - Subscription to data by:
    - Source (AIS, LRIT, S-AIS, etc.)
    - Geographic area
    - Time window
  - Different formats and protocols supported:
    - XML
    - NPR proxy – IEC format
    - IVEF (Inter-VTS Exchange Format)
    - Canonical Data Format (CDF)
    - Email and PDF
    - CAP – Common Alert Protocol
- External Systems to SSN ecosystem:
  - *Usual* position data (AIS, LRIT, satellite AIS)
  - Satellite imagery and derived data
  - *New* position data (VMS, non-EU LRIT, coastal radar, ship-borne AIS and radar information, patrol vessel data)
  - New incidents and ship particulars by Excel/CSV files (or any other format)
  - Additional voyage information.

3.2.3. INTEGRATED MARITIME AWARENESS PICTURE MODEL

Within the scope of CISE, "integrated maritime awareness picture" is defined as a *"picture produced by means of collection, analysis, interpretation and visualisation – when appropriate through a graphical interface – of data and information received from and shared with different authorities, platforms and other sources in order to achieve maritime awareness and to support the reaction capability at sea."*. CISE advocates for the *following scoping options*:

- *Public authority scope: several maritime awareness pictures coexist restricted to the scope of the information held by the public authority providing this service. The information contained in these pictures is not oriented towards the specific needs of User Communities;*
- *User community scope: several maritime awareness pictures coexist restricted to the scope of the information held by the public authority providing this service. The information contained in these pictures is oriented towards the needs of User Communities;*
- *Geographic: several maritime awareness pictures coexist oriented towards the geographical scope of the Member States and possibly Sea Basins providing them.*

The SSN ecosystem is able to provide a fully featured "integrated maritime awareness picture" by combining the information available in its core systems. This picture can be tailored to the end users requesting them, including geographical constraints (by member state, by region, etc.) and it is based in tools that harmonise and enhance the presentation of the domain awareness picture and provide the users with the ability to share data for safety, security, the identification of risk, environmental protection and improve logistics management.

The SSN ecosystem "integrated maritime awareness picture" include features such as:

- State of the art graphical interface that provides in one single platform a view of all available maritime data (position information, voyage and cargo information, port state control information, etc.) and that can be customised to add new data sources, specific symbols and panel contents;
- Correlation of different vessel position information (VDS, AIS, LRIT, VMS, S-AIS, ship reporting data);
- Identification of cooperative and non-cooperative targets in a user-defined area of interest or globally;
- Display of satellite images (SAR and optical) and overlay of ship tracks;
- An 'Event Timeline' tool to provide a way to "visualize" temporal events and information;
- Presentation of external information layers (oceanographic and meteorological information, ad-hoc external information sources);
- For the purpose of ship behaviour monitoring, the user is able to define various alarms and alerts for a particular area (defined by a polygon), ship or list of ships (defined by ship(s) particulars) a combination of alerting criteria, such as:
  - time/period of the day (e.g. during the night);
  - modified rate or interrupted ship reporting (e.g. AIS, LRIT, VMS);
  - ship non-reporting;
  - at-sea encounter;
  - strong deviation from route;
  - sudden change of port of call;
  - sudden change of speed or course:
  - anchorage at abnormal location:
  - distance to the coast violation;
  - violation of traffic separation schemes;
  - Drastic change in estimated time of arrival.

3.2.4. BASE REGISTRIES

A Base Registry database stores reference information that is shared by several applications hosted by EMSA and, if so is to be decided, by MS applications interacting with the applications hosted at EMSA. Three noteworthy "base registries" are available (or will be in the near future) in the SSN ecosystem:

- Reference Vessel Registry Database (RVR);
- LOCODEs Registry;
- Authorities Registry.

The "LOCODEs" and "Authorities" registries are expected to be in operation by the end of 2014. Both registries shall be accessed by authorised users via a web interface. A set of web services will be also made available to allow CREATE/ UPDATE/DELETE and registry SUBSCRIBE actions.

3.2.4.1. Reference Vessel Registry Database (RVR)

Three of the SSN operational systems (SafeSeaNet, THETIS, and LRIT) maintain their own ship registry databases, based on their own legal basis and data collection methods. For example, the LRIT ship database was created on the basis that it is updated by Member States, while the information in the SafeSeaNet ship database comes from notifications received. In each of the reference databases, the relevant information is stored but not fully exchanged between systems.

A new Reference Vessel Registry Database (RVR) is being developed which obtains and uses data from LRIT, SafeSeaNet, THETIS (plus external sources) based on a uniform set of business rules. The result will be a consolidated reference registry for ships´ particulars which could be shared with Member States and other User Communities, contributing to the overall data quality in all systems at central and national level.

3.2.4.2. LOCODEs Registry

As in the case of "ship registry databases", several SSN operational systems use their own LOCODEs database. As such, a "LOCODEs Registry" is being set-up which will store all LOCODEs used by different applications in a single location. Each system will use its own LOCODEs (according to its own rules) but these will be shared, thus ensuring improved harmonisation.

The "LOCODEs Registry" shall include the following fields: LOCODE , Location Name, Location name without diacritics (in English alphabet), up to 4 alternative names, Country of the location, Latitude/ Longitude and source (e.g. UNECE, SSN, LRIT, Thetis) plus additional attributes of interest (e.g. port facility information if available).

3.2.4.3. Authorities Registry

The Authority Base Registry will be the central repository of information related to the administrative entities that have a relationship of any kind with EMSA: international and national organizations, bodies, associations, ministries, offices, ports, public and private companies etc. The Authority Base Registry has the primary goal to identify in a unique way one of these entities and to share its attributes with all EMSA applications.

The following data are to be included in the Authorities Registry: Authority ID , Authority English name, Authority local language name, E-mail address, Phone number, Postal address, Parent Authority ID, Country of the headquarters, Authority Type (in the various EMSA applications, e.g. SSN NCA), Contact person, 24/7 phone number, 24/7 e-mail address plus additional attributes.

3.2.5. DATA EXCHANGE MECHANISMS

The SSN ecosystem data exchange mechanisms supports:

- The relay and exchange of port state control, satellite imagery and derived data, voyage and cargo information through several and well known protocols;

- The relay and exchange ship positional information (AIS, LRIT, S-AIS, and VDS) through XML and standards-based system-to-system interfaces;
- The ingestion new streams of ship positional data (ship borne AIS, ship borne or coastal radar, VMS, etc.);
- The dissemination of alerts and reports by email, PDF, and other formats;
- The ingestion of specific data (e.g. ICCAT file and incidents from EFCA, ship registry from EUNAVFOR).

Different formats and protocols are supported (mostly standard-based):

- IEC 61162 protocol and the Comment Block (CB) extension as defined in the IEC 62320-1 standard:
  - The basis for the exchange of AIS information is the standard IEC 61162 protocol and the Comment Block (CB) extension as defined in the IEC 62320-1 standard. In particular, CBs are already used in SSN to extend the content of the standard IEC 61162 AIS messages with complete timestamp information (only partially complete when transmitted by ships).
- IVEF (Inter-VTS Exchange Format):
  - In order to facilitate VTS data exchange between various parties, the Inter VTS Exchange Format (IVEF) was defined. IVEF is an open standard that can be freely used by anyone interested in vessel traffic data exchange. IVEF supports real-time track positions, static vessel information and voyage-related information.
- EMSA Canonical Data Format (CDF):
  - A format used by EMSA to deliver data between services and within EMSA's ecosystem of systems, thereby guaranteeing a base level of interoperability.
- NAF:
  - The North Atlantic Format (NAF) is a data standard used for transmitting vessel tracking information (VTI) or vessel monitoring systems (VMS) information. The format was adopted first by NEAFC[32] and then NAFO[33]. The standard is managed by the Advisory Group for Data Communications (AGDC).
  - NAF uses internationally recognized standards for vessel types (ISSCFV), for gear (ISSCFG), and for fish species (ISSCAAP). In addition NAF uses the ISO3166 3-Alpha Codes standard for States and fishing entities including specialty developed codes for international waters and Regional Fisheries Management Organisations (RFMO's).

An example of the use of standards-based system-to-system interface is the "SSN-VMS" pilot project performed with the fishing community:

- Position reports for fishing vessels extracted from VMS are forwarded to the SSN system in NAF (North Atlantic Format) format with a frequency selected by the data providers (normal transmission is every 2 hours however this can be reduced to 1 hour).
- For the ships for which a VMS report has been sent to SSN, the SSN will forward back, transformed into NAF format, the AIS data received by SSN (using a configurable frequency of transmission up to every 6 minutes) to the FMC of the:
  - flag state of the vessel;
  - Coastal state.

Another example of system-to-system interface is provided by the "Border control surveillance support service (MARSURV-2)" where a WFS[34] interface is used to exchange georeferenced between IMDatE and EUROSUR.

[32] North East Atlantic Fisheries Commission.

[33] Northwest Atlantic Fisheries Organization.

3.2.5.1. Messaging and Notification Mechanisms

It is important to notice that the SSN ecosystem uses and supports (based on the use of an Enterprise Service Bus and other bespoke tools) key messaging and notifications mechanisms:

- *Notification:* Notification is a messaging pattern where a data provider gathers the necessary information to be reported and send it to the data consumer;
- *Request-Response*: Request-Response is a pattern in which the service consumer uses configured client software to issue an invocation request to a service provided by the service provider. The request results in an optional response;
- *Subscribe-Push*: In this pattern, one or more clients register subscriptions with a service to receive messages based on some criteria.

In the specific case of the SSN Central System, a comprehensive messaging system is in place:

- *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.
- *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.
- *Streaming*:
  - SSN is equipped with a system-to-system streaming mechanism (based on the IEC 61162 protocol and the "Comment Block" extension as defined in the IEC 62320-1 standard) which enables the near-real-time exchange of ship positions obtained via AIS networks.

[34] The Web Feature Service (WFS) is a standard created by the Open Geospatial Consortium (OGC) for creating, modifying and exchanging vector format geographic information on the Internet using HTTP. A WFS encodes and transfers information in Geography Markup Language (GML), a subset of XML.

For obvious scalability reasons, the exchange of XML messages[35] between a national SSN system and the central SSN system is implemented in an asynchronous way: when a "national SSN application" sends, via HTTPS, an XML message (notification, request or response) to the central SafeSeaNet system, the latter one will merely answer with the HTTP '202 Accepted' status code. The same applies in the opposite way (from the central SafeSeaNet system to the "national SSN applications"). As a general rule, as long as an XML message (request or response) has not been acknowledged with the HTTP '202 Accepted' status code, it's up to the sender to retry sending it (with a maximum number of retries). Finally and for security reasons:

- HTTPS with 2-way SSL authentication must be implemented when sending XML/SOAP messages and upon receiving XML/SOAP messages;
- The server(s) used for hosting the XML or SOAP interface as well as for the storing of documents that could be retrieved via a URL shall hold a valid client and server certificate issued by the EMSA certification Authority.

In the case of the IMDatE platform, several messaging mechanisms are supported, including (but not limited to):

- JMS
- SOAP
- XML
- CAP – Common Alert Protocol
- IVEF (Inter-VTS Exchange Format)
- Canonical Data Format (CDF)
- Email
- File/FTP
- IBM WebSphere MQ
- Oracle Advanced Queuing

3.2.5.2. Non-repudiation

"Non-repudiation" is a mechanism that provides protection against an individual falsely denying having performed a particular action: it provides the capability to determine whether a given individual took a particular action such as creating information, sending a message, approving information, and receiving a message.

Non-repudiation is already implemented in most of the data exchange mechanisms in the SSN ecosystem. The best example of this is at SSN Central System level: knowing that the exchange of the XML messages between the national SSN systems and SSN Central System is asynchronous, two special attributes have been defined in the Header element node of the XML messages to allow the correlation between "requests" and "responses": *SSNRefId* given by the SSN Central System; and *MSRefId* given by the national SSN systems. These attributes coupled with the "SSN_Receipt.xml message" and the fact that the exchange of the messages is performed using HTTPS with 2-way SSL authentication, provides the basis for non-repudiation. The "SSN_Receipt.xml" message is used as a confirmation message (indicating whether the notification message is compliant to the corresponding XSD and has been successfully validated and processed, or not) to every notification, request and response message received by SSN Central System from the Member States (and vice-versa to a certain extent).

[35] Every XML message exchanged between SafeSeaNet and the different Member States (and their corresponding national SSN applications) is encoded in UTF-8 format and the chosen language for the messages is English.

3.2.5.3. Email

SSN supports the exchange of information using email.

Examples of this are the "email notifications" feature of CleanSeaNet and "ship notification reports" delivered to the customs authorities under the "Blue Belt" pilot project.

3.2.5.4. Chat and Whiteboard

The SSN ecosystem does not have at the moment any chat and whiteboard capabilities.

3.2.5.5. Video

The SSN ecosystem has limited any video capabilities at the moment i.e. the exchange of video files.

3.2.6. USER MANAGEMENT

User management and data access in the SSN ecosystem is typically addressed (but not exclusively) at two levels:

- EMSA as the system administrator provides access to "competent authorities" and determines rights for creating national users;
- A "competent authority" manages their users within the profiles and access limits granted to that particular "competent authority".

The user management categories take into consideration the following concepts:

- Users;
- Tasks;
- Roles;
- Groups (of users/roles); and
- Data access/permissions.

The general principles applied are defined below:

- Each user can be member of zero or more groups; vice versa each group is composed of zero or more users;
- Each role is composed of one or more functional rights ("tasks");
- Each user or group can be granted one or more roles;
- Each dataset has specific access rights (read, modify, delete, etc.) towards one user, one (or more) groups, one (or more) roles and all users ("world").

3.2.6.1. User Registry and Single Sign-On

User credentials (login/password) are stored in a LDAP directory server – the "user registry". User authentication is made only against this "user registry" and "Single Sign-on" (SSO) mechanisms are also made available based on Oracle technology.

3.2.6.2. Authentication

A reliable authentication mechanism is implemented to uniquely identify SSN users:

- For web interfaces 1-way SSL is used; and
- For machine-to-machine interfaces, 2-way SSL is used.

3.2.6.3. Authorisation

The EU Commission is responsible for the management and development at policy level of the SafeSeaNet and CleanSeaNet systems plus the IMDatE platform, and for the oversight of those systems in cooperation with Member States. The EU LRIT CDC follows the policies established at IMO and THETIS the policies established by the Paris MoU agreement.

With respect to access rights, EMSA and National Competent Authorities (NCAs) comply with the requirements of the relevant legal framework when managing access to the systems. As an example, in case of SafeSeaNet itself, the following legal instruments are to be considered:

- Directive 2002/59/EC as amended (establishing a Community vessel traffic monitoring and information system);
- Directive 2000/59/EC (on port reception facilities for ship-generated waste and cargo residues);
- Directive 2009/16/EC (on port State control);
- Regulation (EC) No 725/2004 (on enhancing ship and port facility security); and
- To be implemented by 1st June 2015, Directive 2010/65/EU (on reporting formalities for ships arriving in and/or departing from ports of the MSs).

"Access rights" (and the related "access rights policy") support the accomplishment of the objectives and functions identified in the legal framework and provide a basis for the operation and administration of the system in hand. "Access rights" also implement the notion "functional roles", "responsibilities" and "functions" defined or derived from the legal framework that support the system.

Hence, through the appropriate "access rights", the "competent authorities" designated to perform the "functions" or "roles" have the appropriate access to perform their responsibilities within the system in accordance with the legal framework. Within each "competent authority", individual persons, persons with the same function and position or systems are identified as "users".

3.2.7. ACCESS RIGHTS

Access to data sets and functionalities in the SSN ecosystem – the "access rights policy" - follows complex criteria including geographic criteria or nationality of the assets involved in the information. Examples of such criteria include:

- *Role*: EMSA (the system administrator) assign to "competent authorities" one or more functional roles within the system. Each role relates to certain specific system responsibilities in accordance with the legal framework. The assigned roles correspond to effective operational functions within the organisation concerned.
- *Nationality of the asset*: the user (e.g. Member State using an application) may have access uniquely to data regarding ships with its own flag;
- *Geographic*:
  - The user may have access uniquely to information within its administrative area of responsibility (which may vary between applications, type of users, nationality);
  - The user may have access to information within an ad-hoc visualization area (based on polygons or locations);
- *Destination*: a port authority may have access uniquely to data on ships bound to it;
- *Special agreements*: Within an application and data sets, different users or countries may have special arrangements not following the same rules applying to the rest.

Other user management configurations are also available:

- *EU Institutions*: EU institutions may have access to the data and functionalities depending from the decisions taken at policy level or provided by a specific legislation;
- *Other agencies and bodies* authorised to receive or visualize data;
- *Temporary users* allowed receiving or visualising data and accessing functionalities for the purpose of specific projects.

Access to information by users of other systems that are connected to the SSN ecosystem is granted only for the information relevant to their operation (as defined in their legal mandate and respecting the maximum access rights per role).

Access may be granted, either on an ad hoc basis (to satisfy a given need during a given period), or in the form of an agreement (MOU), to allow access to SSN systems by specific users who are involved in pilot projects, but who are outside the legal framework.

3.2.8. SECURITY MECHANIMS

The SSN ecosystem implements comprehensive security measures ranging from physical access up to logical security.

The security policies used by the SSN ecosystem applications include issues such as:

- *Organisational Aspects*, including security management and security implementation issues;
- *Access Control*, defining an access rights policy and the need for keeping records of individuals that access the system;
- *Authentication*, defining*:*
  - A reliable authentication mechanism to uniquely identify the users;
  - Naming conventions for User IDs, Password policy and mechanisms for the review of credentials;
  - The need to use 2-way SSL for machine-to-machine interfaces.
- *Authorisation*, defining the rules for *who should be* allowed to access the system.
- *Traceability and accountability*, defining the rules for verification of the history, location, or application of the information from the mandatory system functionalities. The following actions are traced and the records are available to the data provider of the information upon request: "Receipt of the information"; "Modification of the information"; and "Requests for the information". The information recorded includes attributes such as "User identification"; "Time stamp"; and "Description of action".
- *Confidentiality*, defining data protection procedures.
- *Integrity*, defining procedures to ensure that the information is authentic and complete and to prevent denial of service attacks, the introduction of 'malware', or other malicious events with the potential of compromising system functionalities.
- *Audits*, defining that security audits on the system implementation and usage are to be carried out on a regular basis or in case of events where security is deemed to be compromised.
- *Training*, defining that Authorities should ensure that all system users within its jurisdiction are aware of the security requirements of the system and have the knowledge and competencies to fully discharge their obligations.

3.2.9. INTEROPERABILITY

The scope of interoperability is to:

- Implement services and create datasets that can be seamlessly integrated into several business processes, and;

- Establish a framework where one or more user communities can share and make their products "discoverable".

The concept of "interoperability" can be simply translated as the ability of services to work together (interoperate). This means that interoperable services are those who have been implemented in such a way that:

- It is straightforward to discover and thereafter call their functionalities, and;
- They exchange meaningful information.

Within this context the greater the extent to which services are able to work together automatically (i.e. without or with minimal human intervention), the easier it is to integrate functionalities into business processes meeting operational needs. An example would be the possibility for an authorised user within a Member State to make a system-to-system request establishing a service for oil spills detected within a time frame and a geographical area through a generic client and/or standard interface – i.e. without the need to implement a specific client and/or interface.

A pre-condition to the implementation of the aforementioned scenario is the requirement to have services and datasets readily "discoverable". To this extent it is necessary that the description (i.e. the metadata elements) of both the service and of the associated dataset are themselves "discoverable", in a standardised way and within the context of a one or more user communities.

3.2.9.1. SSN ecosystem Approach to interoperability

Within the SSN ecosystem, the following 3 approaches are (or will in the future) be used for the implementation and delivery of interoperable maritime services: i) ad-hoc services; ii) standard services, and; iii) semantic services.

The next sections will briefly describe these 3 approaches.

3.2.9.1.1. Interoperable ad-hoc services

The design and implementation of ad-hoc maritime services follows the requirement to address and maintain a number of existing interfaces and processes. The advantage of this type of integration is that the services provided using the ad-hoc service approach are tailored based on the use case needs. Nevertheless to design, procure, implement, deploy and maintain this ad-hoc process can be rather expensive.

3.2.9.1.2. Interoperable Standard services

Within the context of this type of integration, the SSN ecosystem makes use of agreed services following standard specifications (for example OGC specifications, IVEF, etc.). The advantages of using and providing services based on agreed standards are multiple. At service provider level the main one being that the SSN ecosystem uses software components (services and clients) that are usually more robust, performant, easier to maintain, and do not depend on specific providers. At user level it provides services accessible without the need to implement specific clients and/or interfaces.

This type of interoperability approach highlights the need to create a standard service layer within the SSN ecosystem infrastructure which extends and complements the previously described ad-hoc approach. This need is made apparent also by the growing demand from the Member States administrations to have direct access to EMSA's data through standard services (see for example the IMDatE-FRONTEX WMS interface or Germany's request to access CSN- services via W*S). The SSN ecosystem is indeed already delivering a set of standard services to Member States for them to be included directly into their own systems and applications.

3.2.9.1.3. Interoperable Semantic services

An interoperability approach based on standards (or ad-hoc services) can be implemented if all the stakeholders belong to the same user community, as they are able to exchange meaningful information based on a common and pre-agreed data model. Unfortunately the process to define a common data model cannot be further extended if cross-sector interoperability is required, as it implies a rather dramatic increase in the overall complexity of the data model, which in turns has substantial implications in the management of the services and business processes it serves.

A semantic interoperable approach provides a technological domain for the description, cataloguing and access of resources, these being both services and datasets. These resources may well belong to different domains, different application systems and hence different underlying technologies and can be consumed by different user communities. One example of such a semantic service is Linked Data, which provides a recommended best practice for exposing, sharing, and connecting pieces of data, information, and knowledge, and is increasingly used by different user communities within public and private sectors to deliver integrated type of services.

3.2.9.2. The road to interoperable services

The first two types of interoperable approaches have already been implemented within the context of the SSN ecosystem. Whereas the implementation of standard services needs to be further extended, it is important to note that the work did so far can already provide data and services that can be seamlessly be integrated into operational business processes.

The implementation of interoperable semantic services will be in addressed in the near future. The objective is to create within the SSN ecosystem a framework to make both products and resources "discoverable" (services and datasets) to users and organisations within different user communities.

3.2.10. BUSINESS CONTINUITY

Business Continuity is assured in the SSN ecosystem (along with performance and system availability principles enshrined in the systems) through the following entities:

- Maritime Support Services (MSS) Centre;
- Business Continuity Facility (BCF);

3.2.10.1. Maritime Support Services (MSS)

The Maritime Support Services (MSS) Centre is a 24/7 facility located at EMSA headquarters in Lisbon.

The main day-to-day task of the MSS is the provision of support to the SafeSeaNet ecosystem (SSN Central System – the EU vessel traffic monitoring and information system; EU LRIT Data Centre; the CleanSeaNet oil spill monitoring and vessel detection system; THETIS - port state control database and the IMDatE platform).

The work involves the following:

- System monitoring:
  - Monitoring of system performance;
  - Data quality assessment.
- Administration of systems:
  - Administration and validation of user accounts, access rights and digital certificates;
  - Administration and validation of reference lists (LOCODEs …).
- Complementary activities:
  - Reporting and statistics on system data, system activity and performance;
  - Support to development teams (in testing new software releases, compiling feedback from users on corrections and identifying future developments).
- Helpdesk 24/7:
  - Receiving calls and requests relating to the operation of the systems;
  - Assisting users in operating the system or accessing the information;
  - Informing users in case of problems, new releases, upgrades or programmed maintenance of the system;

- Providing an alert function to address major technical failures, or risk of failure, and also monitoring the resolution of problems;

- Coordination Centre for Maritime Emergencies:
  - In addition to its system monitoring and support role, the MSS is also EMSA's coordination centre for maritime emergencies. It is the single point of contact via which Member States and the European Commission can request support when there has been an accident or incident at sea. The information comes from Member States in the form of POLREPs (for pollution-related incidents) and SITREPs (for safety-related incidents), and also from external accident/incident monitoring systems and the 24/7 emergency telephone/fax/email system.
  - When there is substantial oil pollution at sea, the MSS immediately notifies the EMSA oil pollution response vessel services so that the appropriate vessels can be activated. These have a surface oil recovery capacity which is much larger than most Member State oil pollution response vessels, and they are contracted to be fully equipped and available to sail to a spill within 24 hours. The MSS also provides additional support, as required, for the duration of the emergency.
  - Additionally, it is essential to note that EMSA has a Contingency Plan – where MSS is a key element - which provides support to the Member States – via CleanSeaNet – by delivering satellite imagery and derived products at a global level.

3.2.10.2. Business Continuity Facility (BCF)

EMSA's Business Continuity Facility (BCF) is hosted in Porto in the premises of a commercial hosting provider. The BCF is a fully equipped replica of the main site in terms of servers, network equipment, internet connectivity, storage and middleware, and as such it may function as either the main production site for an application, or as back-up site. This choice may be made on a per application basis and depends on the EMSA needs, the application's replication design and capabilities, and the desired service level.

3.2.10.3. System Availability

The availability of services within the SSN ecosystem is on "twenty-four hours a day, seven days a week" basis. There are small variations regarding Key Performance Indicators of those services:

- For SafeSeaNet Central System the availability of the system shall be maintained at a minimum of 99% over a period of one year, with the maximum permissible period of interruption being 12 hours;
- CleanSeaNet is required to be maintained in operation twenty-four hours a day, seven days a week. The availability of the CSN DC is defined at a minimum of 97.5% over a period of one year, with the maximum permissible period of interruption being 12 hours.
- The EU LRIT DC has a required availability of:
  - 99% over any 1 month;
  - 95% over any 24 hour period.
- Finally, the IMDatE platform availability is established at:
  - 97.5% of the time over any 24-hour period;
  - 99.5% over any 1 month; and
  - 99.9% over a year.

CHAPTER 4
ANALYSIS OF CISE DATA SETS, PRINCIPLES AND REQUIREMENTS

CISE documentation and the TAG data mapping created in Step 2 of the CISE roadmap[36] establish:

- 9 CISE Principles;
- 41 CISE Requirements;
- 500+ CISE data elements.

In the first tasks of the study, these CISE *Principles*, *Requirements* and *Data Elements* were analysed in order to identify the evolutions required of SSN ecosystem to support CISE, and, consequently to support information exchange with other communities. The following chapters provide the major findings of this analysis.

4.1. CISE PRINCIPLES

By analysing the principles listed in the "CISE Architecture Visions Document, Version 2.01" ([RD.4]), we conclude that EMSA's SSN ecosystem has the technical capabilities to fulfil 8 (out of 9) CISE's Principles. The only exception is related to the handling of "highly secure" data, a feature which is not required within EMSA's SSN ecosystem mandate (all systems being "unclassified systems" according to the Commission Decision 2001/844/EC of 29 November 2001).

[36] *"CISE Architecture Visions Document", version 2.01 dated 25/02/2013*, and *"Mapping of Data Sets and Gap Analysis", TAG, Step 2 of the CISE Roadmap*.

4.1.1. FULFILMENT MATRIX

The following table provides a detailed Fulfilment Matrix between the "CISE Principles" listed in the "CISE Architecture Visions Document, Version 2.01" ([RD.4]) and the capabilities of the SSN ecosystem.

Table 4-1: Fulfilment Matrix between CISE principles and SSN ecosystem

	CISE Principle	CISE Description	Fulfils?	Assessment Notes
1	CISE must allow interlinking any public authority in the EU and in the EEA involved in maritime surveillance	The objective of CISE is to improve maritime awareness by improving the maritime User Communities' abilities to monitor, detect, identify, track and understand occurrences at sea in order to find reasoned grounds for reaction measures on the basis of combining new information with existing knowledge.	Yes	The technical infrastructure that supports the SSN ecosystem is able to support the interlinking of any public authority in the EU and in the EEA involved in maritime surveillance. The use in the SSN ecosystem of the SOA principle of service orientation, coupled with Web Services and other data exchange mechanisms, complemented by robust security and access rights management policies, provides a basic infrastructure that can support the exchange of data between EU and EEA public authorities.
2	CISE must increase maritime awareness based on need-to-know and responsibility-to-share principles.	The need-to-know principle promotes the idea of User Communities needing and being able to access information from other communities in order to enhance their integrated maritime awareness picture. The responsibility-to-share principle promotes the idea of User Communities having an obligation to share information with other communities, following appropriate access rights policy, to support them in their decision-making processes by contributing to a more complete integrated maritime awareness picture.	Yes	EMSA has promoted through several "pilot projects" ("Blue Belt", "SSN-VMS" and "SSN-Radar") and maritime surveillance services ("Antipiracy Support For Merchant Fleet Monitoring MARSURV-1", "Border Control Surveillance Support Service MARSURV-2" and "Fisheries Monitoring Service MARSURV-3") the notion of data sharing between user communities (i.e. other than the "maritime safety and security" one). This has been implemented by following the "need-to-know" and "responsibility-to-share" principles as established by CISE.

	CISE Principle	CISE Description	Fulfils?	Assessment Notes
3	CISE must privilege a decentralised approach at EU-level.	CISE must be based on a decentralised approach, meaning that public authorities should be able to work interoperable, based on common standards, while respecting access rights to the exchanged information.	Yes	The SSN ecosystem is able to support the "CISE decentralised approach". In fact the SSN ecosystem is a prime example of a set of systems for the interchange of information where public authorities are able to work interoperable, based on common standards, while respecting access rights to the exchanged information. Additionally, the fact that a system like SafeSeaNet Central System "has a central role of gathering and redistributing data" is not contrary to the "decentralised approach" proposed by CISE: in fact, any other system could connect directly to the SSN Central System to gather the information as performed by the National SSN systems. From a technical perspective this is not forbidden. Also, it is not clear to us why SSN ecosystem systems - viewed as systems that provides information - by itself and/or collected from other systems - cannot be a part of any decentralised approach, where this system is treated like any other system at national or other level. Finally, from a technical perspective, the use in the SSN ecosystem of the SOA principle of service orientation and the use of common standards (SOAP, WMS, WFS, XML …) and well defined interfaces supports the principle of a decentralised CISE.

	CISE Principle	CISE Description	Fulfils?	Assessment Notes
4	CISE must allow interoperability among civilian and military information systems.	CISE must support interactions between civilian and military systems to allowing for the most complete integrated maritime awareness picture.	Yes	From a technical perspective, the SSN ecosystem provides mechanisms (well know Web Services interfaces, as an example) that allow the interchange of information with other systems including military systems. This is not limited to the provision of information abut also to the ingestion of information. An example of this interlinking of SSN ecosystem and military information systems was the PIRASAT/MARSURV-1 services where the SSN ecosystem provided to EU NAVFOR users capabilities such as fusing of satellite imagery together with LRIT, Satellite AIS and voyage data to optimize positional accuracy, but also AIS information collected from a transponder on board the Danish Frigate 'Esbern Snare' was integrated into SafeSeaNet. Additional to this, Incidents spots for 'Pirating', 'Attacks', and 'Pirate Action Groups (PAG)' was integrated into the MARSURV-1 services (based on information provided by EU NAVFOR systems): a new file schema for data exchange was agreed with EU NAVFOR who sends files with updated incident information. Incidents are shown in the web interface as a circle around the incident location. The circle colour corresponds to the risk category and the incidents are deleted after 1 or 2 weeks depending on the type of incident. The circle radius is defined by the input data. A field "source" indicates who has introduced the information, as EU NAVFOR plans for the system to be used by additional users.
5	CISE must allow interoperability among information systems at the European, national, sectorial and regional level.	Improving maritime awareness requires making information available to maritime authorities that previously encountered barriers in trying to obtain that information. CISE participants must be able to access information from national, regional, sectorial and European authorities in a flexible way.	Yes	The principle of interoperability between information systems at the national, regional, sectorial and European level is engraved in all of the SSN ecosystem services and applications (SSN Central System, CleanSeaNet, EU LRIT CDC, THETIS and IMDatE).

	CISE Principle	CISE Description	Fulfils?	Assessment Notes
6	CISE must privilege reuse of existing tools and technologies.	CISE must build on prior work and should favour reusing existing tools, technologies and systems as much as possible.	Yes	The use in SSN of common standards and the SOA principle of service orientation supports the CISE goal of reusing of existing tools and technologies: new services can be built and deployed in the SSN infrastructure making use of the existing capabilities and services. The SSN ecosystem Service-oriented architecture is based on industry standards and can reduce complexity when compared with integrating systems on a solution-by-solution basis. This also enables future applications to mesh seamlessly with existing standards-based services. Also, the SSN ecosystem Service-oriented architectures support the building of composite solutions that consolidate numerous business processes from multiple systems in a simple user interface and make it possible for organizations to develop, implement and reuse processes that are technically enabled and integrated through the use of Web services standards such as XML, SOAP and WSDL. In addition, connectivity, data exchange and process integration efforts are simplified, reducing integration-related development and support costs.
7	CISE must allow seamless and secure exchanges of any type of information relevant for maritime surveillance.	CISE must be able to handle all types of information relevant to maritime information, including non-sensitive, sensitive and highly-secure information.	Partial	According to the Commission Decision 2001/844/EC of 29 November 2001, SSN is an "unclassified system", which means (among other things) that is does not handle secure information. However, the SSN ecosystem applications regularly manages sensitive information which is exchanged between maritime authorities in Member States, and which falls into "commercial sensitive information" and "personal data" categories. To address this need, the SSN ecosystem provides mechanisms for implementing the appropriate security and access management policies. With respect to the handling of "highly-secure information", there may be the need to build additional mechanisms on top of the existing ones (2-Way SSL and Encryption mechanisms), depending on the requirements associated to this type of data.

	CISE Principle	CISE Description	Fulfils?	Assessment Notes
8	CISE must be system neutral.	All User Communities should have equal participation in CISE, without requiring them to modify their own internal structures and systems (apart from what may be required to implement as minimum commonly agreed elements of CISE).	Yes	We analysed this principle from a technical perspective and not from a governance point of view, as all systems in one way or another are "governed" either by a specific user/administration/agency/UC, and as such it's "neutrality" is debatable: we don't envisage a reason where the use of the SSN capabilities underlies the principle of neutrality as compared with the use of any other system developed by any other user/administration/agency/UC. From a technical perspective, through the principle of service orientation, the "SSN ecosystem" does not oblige the providers/consumers of information to use a specific technology or product, and the participation of the SSN ecosystem systems in CISE will not require significant change to their own internal structures apart from what may be required to implement commonly agreed elements of CISE, the best example being the mechanisms for translating the "SSN ecosystem data model" into the "CISE data model".
9	CISE must make it possible for information providers to change their service offering.	Information providers are at all times free to decide on the services they offer.	Yes	In the SSN ecosystem, the available security and access rights mechanisms cater for the need of controlling the services offered with a granularity that usually go to the level of a specific user. From a technical perspective, the need for a services catalogue that simplifies the "change of the service offering" for the whole SSN ecosystem is identified and EMSA plans to develop such capabilities in the near future. However, and as stated before, a services catalogue (or registry) is not the only way "for information providers to change their service offering" and to be "free to decide on the services they offer": this can be also accomplished through other mechanisms like appropriate security and access management policies (which are currently available in the SSN ecosystem).

4.1.2. ADDRESSING THE SHORTCOMINGS

The only CISE Principle partially or not fulfilled by the SSN ecosystem is the one that states that "*CISE must allow seamless and secure exchanges of any type of information relevant for maritime surveillance […] including non-sensitive, sensitive and highly-secure information*": the SSN ecosystem partially fulfils this principle since there may be the need to build additional security mechanisms on top of the existing ones (2-Way SSL and Encryption mechanisms), depending on the requirements associated to this type of data.

Secure information handling is important for CISE when such information is exchanged and stored among various parties and/or systems. For some specific situations, secure e-mail by encrypted server-to-server channels is sufficient; for other scenarios, only the transportation of data by encrypted devices meets the applicable confidentiality standard.

For system-to-system information exchanges "two-way authentication" is the preferred mechanism to be put in place. Security solutions using "two-way authentication" and digital certificates[37] rely on public key cryptography in which each user has a pair of cryptographic keys: one private key that is kept private by the user and one related public key made widely available. This certified public key can be used to encrypt confidential information by the certificate owner and/or to verify digital signatures generated by the certificate owner.

However, these mechanisms do not address all the risks related to the handling of highly-secure information inside an organisation. Unlike the external attacker who tries to infiltrate an organisation through the network, people inside an organisation have more opportunities to interact with the sensitive information and thus are more likely to disclose the information to non-trusted parties, either unintentionally or deliberately. This kind of threat, called insider attack, cannot be stopped effectively by traditional methods like firewalls and intrusion detection systems. Examples of information theft are downloading sensitive files into personal removable media, copy-and-paste of confidential file content, screen capture of protected document image, etc. To address these threats and vulnerabilities Enterprise Digital Rights Management (E-DRM) solutions need to be put in place.

E-DRM tools protect sensitive information by managing and enforcing access and usage rights to the information throughout its lifecycle, no matter where the information is distributed. E-DRM solutions provide information owners with the capability to specify fine-grained rights - such as view, copy and edit - with specific files that need to be protected and to enforce these rights at the time when the files are accessed. For example, the information owner can specify whether the file content can be copied, whether copy-and-paste is allowed, or even how long a particular user can view the file content. Once the rights are specified, they can travel with the protected files together and stay effective until the information owner or privileged users change them.

EMSA's SSN ecosystem implements comprehensive security measures ranging from physical access up to logical security. Access to data sets and functionalities in the SSN ecosystem – the "access rights policy" underlying the information handling policy - follows complex criteria including geographic criteria or nationality of the assets involved in the information. Examples of such criteria include:

- *Role*: EMSA (the system administrator) assign to "competent authorities" one or more functional roles within the system. Each role relates to certain specific system responsibilities in accordance with the legal framework. The assigned roles correspond to effective operational functions within the organisation concerned.
- *Nationality of the asset*: the user (e.g. Member State using an application) may have access uniquely to data regarding ships with its own flag;
- *Geographic*:
  - The user may have access uniquely to information within its administrative area of responsibility (which may vary between applications, type of users, nationality);
  - The user may have access to information within an ad-hoc visualization area (based on polygons or locations);
- *Destination*: a port authority may have access uniquely to data on ships bound to it;

[37] A Digital Certificate is a digitally signed statement that certifies the binding between the owner's identity information and his/her electronic public key.

- *Special agreements*: Within an application and data sets, different users or countries may have special arrangements not following the same rules applying to the rest.

Finally, it is worth to mention that EMSA already has a Public Key Infrastructure (PKI) in place that is able to support "two-way authentication"[38]. The EMSA PKI is a particular infrastructure devoted to the EMSA maritime application user communities and provides the following services:

- A set of trusted procedures and of associated services to create, renew and revoke public key certificates;
- Availability of the public keys associated with each user, under the form of Public Key Certificates (PKC) guaranteed by the EMSA Certification Authority (CA);
- Availability of Certification Revocation List (CRL), allowing the user to check the validity of a given certificate.

EMSA's PKI architecture is based on market standards:

- Certificates follow the X.509 V3 standard and CVC certificates according to EAC 1.11 (BSI TR-03110);
- Compatible with the PKIX standard.

Compared to the general organisation of a PKI, the EMSA PKI adds the following concepts:

- Closed User Group (CUG): the creation of a CUG means that the stringent requirements imposed by the CA on Public Registration Authorities can be relaxed towards the needs of the CUG. The CA will only sign EMSA-CUG certificates for the users who have been approved by the relevant Registration Authority (RA), which goal is to verify the identity of the users requesting the certificate, and approving or rejecting the certificate request. In the frame of central SSN system and its interfaces with the national SSN systems , there will be a single RA played by the EMSA Maritime Support Services;
- Suspension and Revocation Authority (SRA): the SRA's goal is to handle all revocation requests of the CUG users. The SafeSeaNet SRA is represented by the EMSA Maritime Support Services.

As stated before, the principle that "***CISE must allow seamless and secure exchanges of any type of information relevant for maritime surveillance [...] including non-sensitive, sensitive and highly-secure information***" is only partially fulfilled by the SSN ecosystem as:

- SSN is an "unclassified system", which means (among other things) that is does not handle secure information; and
- Not all system-to-system information exchanges are currently being performed over a "secure channel" (e.g. using a "Two-way SSL").

Additionally, and for the specific scenario of handling "highly-secure information" depending on the detailed requirements associated to this type of data, there may be the need to build additional mechanisms (through Electronic Digital Rights Management mechanisms) on top of those already in the SSN ecosystem.

In summary, to fully address the CISE principle of "CISE must allow seamless and secure exchanges of any type of information relevant for maritime surveillance", the SSN ecosystem may need to:

- Implement a secure information exchange protocol (e.g. "Two-way SSL", "HTTPS over TLS") for all the system-to-system interfaces that handle sensitive and highly-secure information; and
- Provide Electronic Digital Rights Management mechanisms, if the need is to control properly not only the system-to-system interfaces but also enforcing access and usage rights on the sensitive information throughout its lifecycle.

[38] Also known as "mutual Authentication" or "Two-way SSL", refers to two parties authenticating each other through verifying the provided digital certificate so that both parties are assured of the others' identity. In technology terms, it refers to a client system authenticating themselves to a server system and that server also authenticating itself to the client through verifying the public key certificate/digital certificate issued by the trusted Certificate Authorities (CAs).

4.2. CISE REQUIREMENTS

The following table synthesises the key figures resulting from our analysis: SSN ecosystem fulfils 29 CISE requirements, partly fulfils 7 and doesn't fulfil 5. The requirements which are not fulfilled are related to: a) secure video/audio/instant messaging/white-boarding communication and b) handling of sensitive and highly secure information.

Table 4-2: CISE requirements: Fulfilment Matrix Summary

CISE requirements	Number of Reqs.	Fulfils	Partially fulfils	Doesn't fulfil
Sharing of Information	14	13	1	0
Discovery of Information	5	2	2	1
Information Assurance	5	3	2	0
Information Security	9	6	2	0
Collaboration between CISE participants	6	2	0	4
Organisational aspects	2	2	0	0
Total	**41**	**29**	**7**	**5**

From an overall perspective, the SSN ecosystem fulfils (or partially fulfils) with 36 of the 41 CISE requirements as listed in the "CISE Architecture Visions Document, Version 2.01".

The evaluation of the SSN ecosystem fulfilment of each of the 41 requirements is detailed in the next section.

4.2.1. FULFILMENT MATRIX

The following sections provides a detailed Fulfilment Matrix between the "CISE Requirements" listed in the "CISE Architecture Visions Document, Version 2.01" ([RD.4]) and the capabilities of the SSN ecosystem.

4.2.1.1. Sharing of Information

Table 4-3: Fulfilment Matrix - CISE requirements: Sharing of information

Requirement		Description	Fulfils?	Notes
SI1	CISE must facilitate building and exchanging an integrated maritime awareness picture by authorities at national, Sea Basin, User Community or in the EU maritime domain level.	CISE must facilitate building and exchanging an integrated maritime awareness picture by authorities at national, Sea Basin, User Community or in the EU maritime domain level.	Yes	The principle of interoperability between information systems at the national, regional, sectorial and European level is a fundamental principle of all of the SSN ecosystem services and applications members (SSN, CleanSeaNet, EU LRIT CDC, THETIS and IMDatE). Additionally, the use of common standards and the SOA principle of service orientation supports the CISE goal of facilitating the building and exchanging of integrated maritime awareness picture. It is important to note that the SSN ecosystem provides services to different user communities (other than the "maritime safety and security" one) by offering an "integrated maritime awareness picture". This is produced by means of collection, analysis, processing, interpretation and visualisation – when appropriate through a graphical interface – of data and information received from and shared with different authorities, platforms and other sources. The SSN ecosystem is able to provide functionalities like: • A single graphical interface to access different types of maritime data; • Ship positioning and ship track data processing (correctness checks, correlation), fusion and enrichment; • Automated ship behaviour monitoring and alerts triggered, based on specific criteria such as Area of Interest (AoI), Vessels of Interest (VoI) and Event of Interest (EoI); • Integrated Ship Profile that aggregates information on a vessel from all EMSA applications and – if available – from external sources; • Position reports: AIS, S-AIS, LRIT, VMS, ship-borne AIS, local AIS feeds, VMS or coastal radar streams; • Voyage and cargo information; • Port State Control (PSC) information; • Satellite products (SAR and optical images, VDS and oil spill); • Geo-referenced events e.g. vessel sightings, pollution detection, known infringements.

Requirement		Description	Fulfils?	Notes
SI2	CISE must support sending information upon request, subscription or spontaneously.	CISE must support sending information upon request, subscription or spontaneously.	Yes	The SSN ecosystem provides a set of state-of-the-art system-to-system interfaces (XML, SOAP, CDF, Email, CAP – Common Alert Protocol, WMS, WFS, CSW, IVEF, IEC) and technical capabilities (use of Enterprise Service Buses) that supports the sending information upon request, subscription or spontaneously. All systems that comprise the SSN ecosystem implement information exchange through publish/subscribe and/or pull/push mechanisms.
SI3	CISE must support sending notifications upon subscription or spontaneously.	A CISE participant must be able to send a notification. A notification is used to inform other participants of an event. Events can relate to the maritime domain (e.g. a collision, an oil-spill, a suspect ship entering European waters, etc.) or to anything related to the sender of the notification (e.g. a notification to inform about a service that is or will be temporarily unavailable, the availability of a new information or data, etc.). Sending notifications spontaneously can be done to one or more participants at the same time using access profiles (see requirement "IS1").	Yes	All systems that comprise the SSN ecosystem implement information exchange through publish/subscribe and/or pull/push mechanisms, subject to the compliance of pre-defined access rights.
SI4	CISE must support requesting information.	CISE must support requesting information.	Yes	The use in the SSN ecosystem of known interfaces, common standards and the SOA principle of service orientation supports the CISE requirement for the support of information request. Access to the SSN ecosystem can be gained via i) graphical web-based user interfaces, ii) SOAP-based web-services, "bare XML" and other standards-based system-to-system interfaces, and iii) other ways of data export/import such as email, PDF, CSV and other common data formats, etc.

Requirement		Description	Fulfils?	Notes
SI5	CISE must support subscribing and unsubscribing to information at any time.	CISE must support subscribing and unsubscribing to information at any time.	Yes	The availability of tools like Enterprise Service Bus (ESB) and other Message Oriented Middleware (MOM) in the SSN ecosystem allows the subscription and unsubscription to information published at any time by "information consumers": the ESB will route data to active data event "Subscribers" from active data event "Publishers". The well-known publish/subscribe interaction pattern supports one of the key principles of service oriented architectures – loose coupling. In the context of publish/subscribe, the publisher or producer of a message or event does not know about any potential subscriber or consumer of that message or event. Only a topic couples the publisher and subscriber; publishers publish to a topic and subscribers subscribe to a topic. The underlying MOM or ESB is responsible for delivery from publisher to subscribers. Subscriptions may remain in effect over long periods before being cancelled or revoked.
SI6	CISE must support subscribing and unsubscribing to notifications at any time.	Similar to subscriptions to information, participants can also subscribe to notifications. This allows them to remain aware of events in the maritime domain or of events related to any participant, without having to receive a set of information to process.	Yes	Additionally to the publish/subscribe mechanisms described above, the SSN ecosystem provides the ability to implement notifications mechanisms through the use of OASIS Common Alerting Protocol (CAP). The Common Alerting Protocol (CAP) provides an open, XML-based non-proprietary digital message format for all types of alerts and notifications. The CAP format is compatible with Web services. CAP allows a consistent warning message to be disseminated simultaneously over many different warning systems. The CAP message format can be converted to and from the "native" formats of all kinds of sensor and alerting technologies, forming a basis for a technology-independent "warning internet."

	Requirement	Description	Fulfils?	Notes
SI7	CISE must support requesting or subscribing to information without knowing who the provider of the information is.	In order to reduce situations in which authorities are unable to make a sound decision due to a lack of information and not knowing where this information could be requested, CISE must support requesting information without first having to know whom to contact. A multicast or broadcast system supports sending requests to multiple authorities at once. Authorities that have the requested information can then reply. CISE information requests can for instance be used to request information on (these examples are non-exhaustive): • A vessel. Information about a vessel must be able to be requested using any of the existing vessel identification means (a unique ID, a name and country, etc.). • An area. Information about a particular area can be requested using a commonly agreed geographic identification system. • An action by a maritime authority (any maritime intervention, possibly in response to an event).	Yes	The SSN ecosystem provides mechanisms (based on the use of Enterprise Service Bus functionalities, coupled with CAP - Common Alerting Protocol) that support the multicast and broadcast of information requests and alerts without knowing who is the information provider or alert recipient.

	Requirement	Description	Fulfils?	Notes
SI8	CISE information requests can specify the time-frame for which the information is requested.	There is no time limitation on information shared through CISE; it can be historical or current. CISE participants should be able to request information from a specific period.	Yes	The SSN ecosystem supports information requests from a specific period, although as usual in systems that handle a large volume of information, some of this information may not be stored online, hence may require time-consuming procedures to provide the access. For instance in SafeSeaNet Central System, the data is immediately available for: • A minimum of 5 years for information related to incidents and accidents and; • A minimum of 2 months from the departure of the ship for information related to port calls and hazmat; and from the reporting date for ship position information; In any case, the data in SafeSeaNet Central System is archived for at least 5 years, down-sampled when necessary. As for CleanSeaNet, all data sets are available on line for 2 years. Pollution information is available on line for 10 years. Access to other data stored can be obtained on request within 5 working days during the same 10 year period. The EU LRIT CDC complies with the following requirements regarding data availability and storage: • Archive LRIT information from ships which transmit the information to the centre for at least one year and until such time as the Maritime Safety Committee reviews and accepts the annual report of the audit of its performance by the LRIT Coordinator. However, the archived LRIT information should provide a complete record of the activities of the centre between two consecutive annual audits of its performance; • For LRIT information archived within the last 4 days, the information is sent within 30 min of receiving a request; • For LRIT information archived between 4 and 30 days previously, the LRIT information is sent within 1 h of receiving a request; • For LRIT information archived more than 30 days previously, the LRIT is sent information within 5 days of receiving a request.

	Requirement	Description	Fulfils?	Notes
SI9	CISE must rely on a common data model for information exchanges which is as language-neutral as possible.	Information shared through CISE must be made available using a common data model so that all CISE participants can understand and use the information. This common data model must be language neutral, meaning that it should not favour any of the languages of the European Union and that it can be used with any of the languages of the European Union. The common data model should facilitate multiple versions of the data model and should guarantee backward compatibility.	"Not Applicable" or "Partial"	Considering that a "CISE common data model" does not exist yet (or it is publicly available), this requirement cannot be currently fulfilled by SSN ecosystem and by all existing systems that may contribute to CISE. However, all SSN ecosystem applications provide known data models that can be used for information exchange. Of course that the data models underlying the SSN ecosystem are best understood within the "maritime safety and security" community, but most of the concepts in that data model is also shared with other user communities. Nevertheless, the need for a "common data model that all CISE participants can understand" may lead in the future to changes in the SSN ecosystem in order to provide a "mapping" between the concepts in the ecosystem and the CISE ones. The use of ontology – a formal representation of knowledge as a set of concepts within a domain, using a shared vocabulary to denote the types, properties and interrelationships of those concepts – and Web Ontology Language (OWL)[39], being currently promoted by W3C for semantic webs, should be investigated in order to address this requirement.

[39] The OWL Web Ontology Language is designed for use by applications that need to process the content of information instead of just presenting information to humans. OWL facilitates greater machine interpretability of Web content than that supported by XML, RDF, and RDF Schema (RDF-S) by providing additional vocabulary along with a formal semantics. OWL has three increasingly-expressive sublanguages: OWL Lite, OWL DL, and OWL Full.

Requirement		Description	Fulfils?	Notes
SI10	CISE must rely on a common messaging protocol for information exchanges.	CISE participants must use a commonly agreed messaging protocol to exchange information in support of transport characteristics such as integrity and reliability. The common messaging protocol should facilitate multiple versions of the protocol and should guarantee backward compatibility.	Yes	Access to the SSN ecosystem can be gained via i) graphical web-based user interfaces, ii) SOAP-based web-services, "bare XML" and other standards-based system-to-system interfaces, and iii) other ways of data export/import such as email, PDF, CSV and other common data formats, etc. The system-to-system interfaces available in the SSN ecosystem provide the ability of exchanging not only *basic maritime data* (e.g. AIS positions) but also *processed information*. In addition, the SSN ecosystem is also able to ingest and process 3rd party data/information – using also XML and standards-based system-to-system interfaces - in accordance with their associated data access rights and either fuse or display this data separately, as required.
SI11	CISE must rely on common standards for information processing.	To promote a common understanding of information relevant to maritime surveillance, CISE must foster the use of common standards to interpret and process exchanged information (by performing e.g. aggregation, correlation or fusion on the information). This is e.g. important to build an integrated maritime awareness picture.	Yes	The SSN ecosystem provides a standards-based data exchange platform which brings together the existing EMSA monitoring and tracking systems as well as other external systems (e.g. satellite AIS), and in the end provides an extensive and integrated maritime awareness picture by providing functionalities like: • A single graphical interface to access all maritime data; • Ship positioning (coming from AIS, S-AIS, LRIT, ship-borne AIS, local AIS feeds, VMS or coastal radar streams)and ship track data processing (correctness checks, correlation), fusion and enrichment; • Automated ship behaviour monitoring and alerts triggered, based on specific criteria such as Area of Interest (AoI), Vessels of Interest (VoI) and Event of Interest (EoI); • Integrated Ship Profile and other Reference Registries (LO-CODEs, …); • Voyage and cargo information; • Port State Control (PSC) information; • Satellite products (SAR and optical images, VDS and oil spill); • Geo-referenced events e.g. vessel sightings, pollution detection, known infringements.

Requirement		Description	Fulfils?	Notes
SI12	CISE participants must be able to approve information requests or subscriptions manually.	Typically, everything is done automated for effectiveness. But sometimes manual approval might be needed. This is an exception, however.	Yes	In order to assess the compliance of SSN ecosystem with this requirement additional information is required on how this mechanism of "information request approval" is to be implemented in CISE: since the information available is very limited, we cannot categorically state that the SSN ecosystem fulfils or not the requirement since there are mechanisms in place in the SSN ecosystem applications that caters for such a requirement, obviously built for the purposes of the aforementioned applications. Information provision in a services oriented platform like the SSN ecosystem can be fully automated or based on a workflow that encompasses human interaction for approvals. To enable access to the provided services, the SSN ecosystem offers an integration layer and an Enterprise Service Bus, which provides a standards-based interface to multiple systems and also "human service providers". This last feature can be achieved through many ways (a manual workflow step, for example), and it is based on the principle of asynchronous services: it is possible to implement a human workflow service that makes people and manual steps look like any other asynchronous service from the perspective of the process. With this approach, user interactions can range from simple scenarios, such as a manual approval step in a process, to a complex scenario, where data must be entered by the user before the process can continue. As an example, a mechanism for the manual approval and provision of information is in place at SSN Central System level.
SI13	CISE must support exchanges of large files.	Information exchanges must support exchanging files of varying size. This is necessary to support the exchange of large satellite images and maps for example. The maximum supported file size can only be established as part of a technical analysis of relevant file sizes however.	Yes	The need for exchanging large files – like satellite images and maps - is etched in some way or another in all of the SSN ecosystem members. As an example, the exchange and handling of satellite images and metadata is a key requirement in CleanSeaNet.

Requirement		Description	Fulfils?	Notes
SI14	CISE participants providing information must provide statistics per service on information exchanged through CISE.	A CISE participant exposing services should offer statistical information on that service. This allows for a performance analysis of the service and can provide insights in how to best evolve the service. CISE participants must have access to the statistical information on exposed services. This provides them with insights on the performance of a service and supports them in making a sound decision on if and how to use the service.	Yes	The need for monitoring the behaviour of systems and providing statistics on their use is supported by all of the SSN ecosystem members. As an example, the SSN Central System has a "data warehouse" component that allows the creation of a large number of metrics, such as "number of AIS position reports", "number of Port Plus messages", filtered by several dimensions like date (day, month, quarter, …), source (member state, flag, LOCODE, …), etc.

4.2.1.2. Discovery of Information

Table 4-4: Fulfilment Matrix - CISE requirements: Discovery of information

Requirement		Description	Fulfils?	Notes
DI1	Member States and User Communities must provide one or more points of access that facilitate standardised discovery of the services they provide to CISE participants.	CISE must try to hide as much organisational, semantic and technical complexity from its participants as possible. Organisational complexity is an important barrier to information sharing that cannot be reduced or eliminated by mere technical means. An organisational change, by providing one or more points of access for a larger group of CISE participants, will support other participants in discovering the services of such a group.	No	As stated before, the need for a services catalogue for the whole SSN ecosystem will be addressed by EMSA in the near future. Regarding the issue of hiding "hide as much organisational, semantic and technical complexity from its participants as possible", by following the SOA principle of service orientation, the complexity and inner workings of the services offered by the SSN ecosystem are effectively hidden from the service consumers. Additionally, the technical capabilities of tools like Enterprise Service Bus and Application Servers that are used in the SSN ecosystem cater for the need to have multiple points of access for users accessing the services.
DI2	CISE must allow retrieving contact information about CISE participants.	The maritime domain is characterised by a large number of varied stakeholders. To promote collaboration, CISE must provide a means to look-up contact information for the involved stakeholders so that they can contact each other more easily than today. A contact directory, a "phone-book", to look-up contact details can support this.	Yes	The SSN ecosystem is able to provide a means to look-up contact information for the involved users, always in accordance with the principles of personal data protection as defined in Directive 95/46/EC. The SSN ecosystem already has in place a "user and authorities registry" which may provide "contact directory" functionality.

Requirement		Description	Fulfils?	Notes
DI3	CISE must allow looking up what information CISE participants can provide and how they can provide that information.	To allow CISE participants to discover information more easily, CISE must provide a means to look-up what information is available from which CISE participant. By having an overview of what information is available through CISE; participants can more easily discover information to help them improve their maritime awareness.	Partial	The SSN ecosystem today provides a way to users discover the information provided at technical level (well-known Web Services and other standardized data exchange mechanisms) and through the various "pilot projects" and "maritime surveillance services" has demonstrated this capability to other User Communities. As stated before the best technical way to "allow looking up what information can be provided" by a system is a service catalogue, which - as mentioned before - will be implemented in the SSN ecosystem in the near future. This service catalogue will enable other systems to quickly, easily, and dynamically find and carry out transactions that make use of the SSN ecosystem service offering. However, the current mechanisms available in the SSN ecosystem (the above mentioned well-known Web Services and other standardized data exchange mechanisms) partially fulfil this requirement, and because no further details are provided on how the requirement should be addressed, we consider it "partially fulfilled" by the SSN ecosystem.
DI4	CISE must allow information providers making available how their services can be used, including parameters such as the refresh rate.	The usage details of the services exposed through CISE by each participant CISE should be documented and be made available to all participants. This documentation allows participants to assess more easily of if the offered services are useful.	Partial	As stated before the future SSN ecosystem service catalogue will cater for full automated fulfilment of this requirement. Today, the system-to-system interfaces provided by the SSN ecosystem are properly documented.
DI5	CISE must allow verifying if the services offered by CISE participants are available.	CISE participants must be able to verify if any of the services exposed through CISE is available. If a participant depends on a service to make decisions related to an event in the maritime domain, it must be able to verify the availability of the service so that it can take corrective actions if the service is not available.	Yes	An EMSA structure named "Maritime Support Services" (MSS) is in place that is able to provide information on the status of the SSN ecosystem applications to EMSA management and decision makers in the EU institutions and elsewhere. The availability of services within the SSN ecosystem is on "twenty-four hours a day, seven days a week" basis. All critical SafeSeaNet infrastructure (application servers, messaging servers, databases) are redundant and in high availability configuration. A Business Continuity Facility (BCF) is also in place. The use of Common Alert protocol (available in the SSN ecosystem) the can also be considered to implement the mechanisms to support this requirement.

4.2.1.3. Information Assurance

Table 4-5: Fulfilment Matrix - CISE requirements: Information Assurance

Requirement		Description	Fulfils?	Notes
IA1	CISE information exchanges must include a confidence value and must indicate who provided it. The confidence value must be a commonly agreed coded value.	A confidence value is used to indicate the quality of and the trust in the information shared through CISE. The confidence value is an opinion, which is why the provider of the confidence value also needs to be identified in the information exchange. The combination of the confidence value and its provider supports the receiver of the information in making its decision as to use the information or not.	Partial	Currently not all SSN ecosystem interfaces include such "confidence value" for all the exchanged information. Nevertheless in some specific interfaces such data qualification metric is used (for instance in CleanSeaNet).
IA2	CISE information requests must include a priority level reflecting the urgency of the request. The priority level must be a commonly agreed coded value.	Some requests or notifications will likely have a higher priority than others. For example, in the case of a collision or an oil-spill, immediate action is required and any information requests or notifications should be treated first by all involved CISE participants. The priority level is used to indicate the urgency of the request.	Partial	Currently not all SSN ecosystem interfaces include such "priority level" for all the exchanged information, given that the underlying information is usually treated immediately/automatically. Nevertheless in some specific interfaces – such as the ones related with oil spills notifications in CleanSeaNet and access to historical information in SSN – such data qualification metric are already in place.
IA3	CISE information exchanges must contain relevant characteristics about the information.	To allow CISE participants to adequately use information received through CISE, the information exchanges must describe the characteristics of the information. This meta-information, e.g. the provenance of the information, the time it was collected, updated or sent, it's precision or its level of detail, should be part of the information exchange. Information exchanges must also be able to refer to each other. This supports CISE participants e.g. in providing feedback on information sent or in sending updates to, rectifications of or notifications on earlier exchanged information.	Yes	The existing SSN ecosystem system-to-system interfaces include meta-information describing the characteristics of the information being exchanged, including a timestamp and a unique ID which allows implementing mechanisms for non-repudiation and the provision of feedback on the quality of the exchanged information. As an example, very XML message exchanged between the SSN Central System and the National SSN systems is composed of a "root element", "header" and "body". The "header" provides "non-business" information about the SafeSeaNet transaction (such as reference id for correlation, sending and expiration DateTimeUTC, global status code and status message…). The "body" includes the "business" information of the message and consists of one or more node element(s) containing different attributes.

Requirement		Description	Fulfils?	Notes
IA4	CISE participants must be able to acknowledge information received.	The provider of information needs assurance as to whether the information was successfully received by other participants in some cases. This might e.g. be the case when the sender is liable for sharing information in due time. Acknowledgements by the receiver can be automated or manual.	Yes	The existing SSN Central System is the clear example of a system that caters for non-repudiation: a mechanism for acknowledgement of the received/sent messages is included in the system-to system interfaces where relevant.
IA5	CISE participants must be able to provide feedback on the quality of the information received to the information provider.	To support CISE participants in improving the exchanged information, CISE must support sending feedback on the quality of the information. If the information was e.g. invalid or not up-to-date, the receiver must be able to share this feedback with the provider to allow them to improve their information. The commonly agreed information exchange model must define taxonomy to categorise useful feedback categories (e.g. data invalid, corrupt, etc.).	Yes	The SSN ecosystem has several mechanisms that allow receiving feedback about the exchanged information: this is achieved both at the technical level – with some of the interfaces including mechanisms for providing such feedback – and at a governance level – with EMSA's "Maritime Support Services" performing internal data quality assessments on the provided/received data and at the same time being able to "process" the feedback provided by other means by users. As an example of the above, the SSN central and national systems implement data quality checks and procedures to: • Prevent mistaken data to enter into SSN: before sending the SSN data to the central SSN system, the Member State's SSN national applications will perform a complete set of checks based on specific predefined rules ensuring the data cohesion; • During the checking process, the national SSN application will verify that the message corresponds to the expectations. If no conflict detected the message will be send to the central SSN system, otherwise it will be rejected by giving a relevant warning to the message originator about the nature of the mistake. To address the above quality checks and procedures, specific fields are used in the SSN XML protocol. Additionally, when receiving an XML message, the SSN central and national systems must check whether it is a "Well Formed" XML document (i.e. a document that conforms to the XML syntax rules) and must validate it against its XML Schema definition (XSD). If an error is detected, an 'InvalidFormat' status code must be returned within the XML message that should normally follow in the flow of the transaction.

4.2.1.4. Information Security

Table 4-6: Fulfilment Matrix - CISE requirements: Information Security

Requirement		Description	Fulfils?	Notes
IS1	CISE information exchanges must respect agreed data access rights through access profiles.	A CISE information exchange needs to use an access profile. The access profile determines if the requester of the information is entitled to access it. Management, both technical and organisational, of the information systems of the CISE participants and in particular of their own users is not addressed by CISE however. This means that CISE participants will need to assign their own users a CISE access profile which will be used if they exchange information using CISE (the user's identify at the authority is not available in the information exchange, only the user's organisation and the user's CISE access profile are part of the exchange). CISE participants do not need to change their internal user profiles, the existence of a mapping to the CISE access profiles is sufficient.	Yes	The current "data access rights" mechanisms available in the SSN ecosystem is a combination between "Role-Based Access Control" and "Access Control Lists" and provides several "variables" that are/can be used for the definition of access profiles: authority, groups of users, roles of users, applications, tasks, and geographical locations (including location of user and origin of information).
IS2	CISE must support information access rights that can be changed dynamically (respecting a commonly agreed Service Level Agreement (SLA) by the information owner.	Access rights should be managed dynamically to allow for sufficient flexibility in determining who can access what information. The purpose of dynamic access rights is to support crisis situations that necessitate giving temporary access to information that would not be accessible to certain participants under normal circumstances.	Yes	The current "data access rights" mechanisms available in the SSN ecosystem can be changed dynamically.
IS3	CISE must support information providers providing a service to allow requesting access to their information.	Similar to IS2, this requirement allows CISE to be a dynamic environment. CISE participants can expose a service to allow others, who believe they can benefit from the exposed service but that cannot access it yet, to request access to that service without having to establish a bi-lateral agreement.	Yes	The SSN ecosystem has in place governance mechanisms that cater for the need of providing access to system functionalities to users that to not have it at a given time, following agreed security principles and organizational aspects.

Requirement		Description	Fulfils?	Notes
IS4	CISE information exchanges are authenticated at the level of the CISE participants and in respect of the CISE access profiles.	Authentication is performed at the level of the CISE participant. This means that it is an authority (in case an information system of that authority) that is authenticated, not an individual end-user within that authority. However, it is likely that different individuals within the same authority have different access rights and privileges. These differences are also supported at CISE level by giving authorities the vision of assigning a CISE access profile to their end-user. The combination of the authenticated participant and the CISE access profile of the end-user will determine whether or not an information request will be authorised.	Yes	The current "data access rights" mechanisms available in the SSN ecosystem can implement access rights mechanisms based only a defined "CISE access profiles of end-users".
IS5	CISE information exchanges must respect a commonly agreed information classification scheme supporting security levels from up to EU secret.	CISE interconnects a large number of varied authorities in the maritime domain. This variety necessitates an environment that supports the exchange of non-secure, confidential, secure and highly-secure information. Different channels will be needed to support this requirement; these channels will be linked to the commonly agreed information classification scheme. Over-classification, i.e. classifying information as secure while it is not and could use a non-secure channel, should be avoided. CISE participants, each likely with their own classification scheme, need to map their own internal scheme to the CISE classification scheme when sharing information. The objective is to have a common understanding of what a certain classification scheme means. CISE participants do not need to change their internal classification scheme, the existence of a mapping to the CISE classification scheme is sufficient.	Partial	The SSN ecosystem supports currently the exchange of data apart "highly secure" data. The SSN data classification scheme is suitable to a commonly agreed information classification scheme.

Requirement		Description	Fulfils?	Notes
IS6	CISE information requests and subscriptions can use different access profiles to request or subscribe to the same information.	An information exchange needs to support multiple access profiles in that it should be possible for an information provider to identify multiple, different access profiles that are authorised to receive its information.	Yes	The current "data access rights" mechanisms available in the SSN ecosystem can to support multiple access profiles in that it should be possible for an information provider to identify multiple, different access profiles that are authorised to receive its information. Access to data sets and functionalities in the SSN ecosystem – the "access rights policy" - follows complex criteria including geographic criteria or nationality of the assets involved in the information. Examples of such criteria include: Role, Nationality of the asset, Geographic, Destination, Special agreements, EU Institutions, Temporary users.
IS7	CISE must use a messaging protocol that ensures a minimum level of integrity of information exchanges between consumer and provider. The messaging protocol must also ensure higher levels of integrity depending on the classification level of the information.	While confidentiality techniques ensure that the content of an information item or exchange is kept "hidden" from unauthorized individuals, it does not ensure that the information item has not been modified. This is accomplished with integrity techniques. Integrity techniques protect against unauthorized modifications, but they do not protect against unauthorized access and disclosure.	Partial	The SSN ecosystem provides currently information exchange mechanisms based in the use of SSL/HTTPS which cater fully to the integrity of data exchanges. Additionally, commonly used methods to protect data integrity like hashing the data received and comparing it with the hash of the original message, are available in the SSN ecosystem. However, currently this mechanism is not used on all SSN ecosystem information exchanges: it is used for instance in CleanSeaNet for the exchange of satellite imagery.
IS8	The communication channels between CISE participants must support non-repudiation.	Non-repudiation means that CISE participants will not be able to deny having sent information to another participant.	Yes	Through the use of SSL/HTTPS and mechanisms at protocol level – use of unique IDs in exchanged messages – SSN is able to support non-repudiation.
IS9	CISE must support interconnecting networks of different security levels, including public and private networks.	CISE must support interconnecting the various networks of existing initiatives, such as CCN/CSI, sTESTA and EU OPS WAN. These networks can use different technologies and security levels.	Yes	The SSN ecosystem is today interconnected with several types of networks of different national authorities. However, the support to networks with specific communication stacks (like in the case of CCN/CSI) needs to be studied in detail. In case of TCP/IP-based communication networks (like the case of sTESTA), no major integration problem is foreseen.

4.2.1.5. Collaboration between CISE participants

Table 4-7: Fulfilment Matrix - CISE requirements: Collaboration between CISE participants

Requirement		Description	Fulfils?	Notes
CO1	CISE must support secure exchange of unstructured information independent of the format the information is in.	Unstructured information is any information that cannot be directly expressed using the commonly agreed information exchange model. An example is a normal file, e.g. a MS Word document. CISE participants must be able to securely exchange information that cannot be exchanged through an exposed service, without any limitations on the format of the file other than those agreed by all CISE participants (see CO2). Example file format include PDF, DOCX, PNG, etc.	Yes	The SSN ecosystem supports the secure exchange of unstructured information through available mechanisms like FTPS, Email, PDF, Portable Network Graphics files, CSV, and any other Computable Data Format file.
CO2	CISE participants should agree on a common set of file formats in order to maximise the usability of exchanged information.	Although CISE does not impose any restriction on the types of information or files changed, it is highly recommended that CISE participants themselves agree on a common set of file formats to be used. Agreement on a set of common file formats will maximise interoperability as participants only need to implement the tools or information systems to process an exhaustive list of file formats. If they do, they are ensured that all received information will be understandable.	Yes	The SSN ecosystem is able to cater for a wide ranging of types of information (from AIS messages up to satellite imagery and derived data) and exchange protocols: SOAP-based web-services, "bare XML" and other standards-based system-to-system interfaces, and other ways of data export/import such as, Email, PDF, Portable Network Graphics files, CSV, and any other Computable Data Format file, etc. The system-to-system interfaces available in the SSN ecosystem provide the ability of exchanging not only basic maritime data (e.g. AIS positions) but also processed information.
CO3	CISE must support secure audio communication.	CISE must provide a means for participants to easily interact with each other using audio tools (e.g. using a computer and a headset).	No	Being an "unclassified system" according to the Commission Decision 2001/844/EC of 29 November 2001, SSN did not had the need up to now to implement secure audio/video/instant messaging/white-boarding communication.
CO4	CISE must support secure video communication.	CISE must provide a means for participants to easily interact with each other using video tools (e.g. using a computer and webcam).	No	Being an "unclassified system" according to the Commission Decision 2001/844/EC of 29 November 2001, SSN did not had the need up to now to implement secure audio/video/instant messaging/white-boarding communication.
CO5	CISE must support secure instant messaging.	CISE must provide a means for participants to easily interact with each other using text-based tools (e.g. a chat tool).	No	Being an "unclassified system" according to the Commission Decision 2001/844/EC of 29 November 2001, SSN did not had the need up to now to implement secure audio/video/instant messaging/white-boarding communication.

Requirement		Description	Fulfils?	Notes
CO6	CISE must support secure white-boarding.	CISE must provide a means for participants to easily interact with each other using online collaboration tools such as a white-boarding tool that can be concurrently used by the CISE participants.	No	Being an "unclassified system" according to the Commission Decision 2001/844/EC of 29 November 2001, SSN did not had the need up to now to implement secure audio/video/instant messaging/white-boarding communication.

4.2.1.6. Organisational Aspects

Table 4-8: Fulfilment Matrix - CISE requirements: Organisational Aspects

Requirement		Description	Fulfils?	Notes

OA1	CISE must support an encompassing governance body that is required to maintain all the commonly agreed elements.	The realisation of CISE will require a number of common elements between the CISE participants. These need to be agreed on by the CISE participants but they also need to be maintained (e.g. the delivery of a new version, the operational oversight on a commonly agreed element, etc.). An encompassing governance body should take on the responsibility of maintaining the commonly agreed elements.	Yes	All SSN ecosystem applications have underlying governance bodies that cater for the commonly agreed elements of those systems.
				
				The SSN central system is a good example of the above through two governance bodies:
				• The High Level Steering Group on SafeSeaNet (HLSG, chaired by EC) – The group is defined in Annex III of Directive 2002/59/EC (as amended), and comprises MS and Commission representatives, and has the tasks defined in Commission decision 2009/584/EC of 31 July 2009. The HLSG shall:
				  ○ make recommendations to improve the effectiveness and security of SafeSeaNet;
				  ○ provide appropriate guidance for the development of SafeSeaNet;
				  ○ Assist the Commission in reviewing the performance of SafeSeaNet.
				• SafeSeaNet Group (SSN group, chaired by EMSA) - Comprises representatives from MS, Commission and EMSA. Representatives from other organisations and industry may be invited to participate as observers. EMSA chairs and is responsible for managing this governance body which aims to (among other things):
				  ○ regularly report to Member States, European Commission and other governance bodies on SSN activities;
				  ○ define user requirements, monitor the system and support its adaptation to users' requirements;
				  ○ define the necessary modification and adaptation of the system in order that it complies with the latest regulations;
				  ○ coordinate the network of SSN users;
				  ○ define new system functionalities and user interfaces as requested by the relevant governance bodies;
				  ○ Develop and update SSN technical and operational documentation.

Requirement		Description	Fulfils?	Notes
OA2	CISE participants should agree with availability and service levels defined in a bilateral, multilateral or community Service Level Agreement.	If a CISE participant exposes a service, they should also commit to an availability level defined in a (SLA). Defining an SLA is useful if a service is required to deliver high availability or particularly fast transmission of information.	Yes	The principle of providing a service under a Service Level Agreement is enshrined in the SSN ecosystem: as an example, the maritime surveillance services delivered by IMDatE for specific user communities are done through the stipulation of a Service Level Agreement which identifies all service delivery parameters. From a technical and organisational point of view, the availability of services within the SSN ecosystem is on "twenty-four hours a day, seven days a week" basis. All critical SafeSeaNet infrastructure (application servers, messaging servers, databases) are redundant and in high availability configuration. Also, the SSN ecosystem integrates mechanisms for business continuity (with a business continuity facility along with continuous monitoring of the underlying IT infrastructure in place through internal entities – EMSA's Maritime Support Services – and external contractors), which make working under a defined SLA a structural way of working for SSN.

4.2.2. ADDRESSING THE SHORTCOMINGS

The CISE requirements that are partially fulfilled by the SSN ecosystem are related to:

- *Sharing of Information:* Use of a common data model:
  - *SI9 - CISE must rely on a common data model for information exchanges which is as language-neutral as possible;*
- *Discovery of Information*: Looking up what information can be provided and how the services can be used:
  - *DI3 CISE must allow looking up what information CISE participants can provide and how they can provide that information;*
  - *DI4 CISE must allow information providers making available how their services can be used, including parameters such as the refresh rate;*
- *Information Assurance*: Confidence value and priority level for the exchanged information.
  - *IA1 CISE information exchanges must include a confidence value and must indicate who provided it. The confidence value must be a commonly agreed coded value;*
  - *IA2 CISE information requests must include a priority level reflecting the urgency of the request. The priority level must be a commonly agreed coded value;*
- *Information Security*: Integrity of all information exchanges and handling of "highly secure information".
  - *IS5 CISE information exchanges must respect a commonly agreed information classification scheme supporting security levels from up to EU secret;*
  - *IS7 CISE must use a messaging protocol that ensures a minimum level of integrity of information exchanges between consumer and provider. The messaging protocol must also ensure higher levels of integrity depending on the classification level of the information.*

The CISE requirements which are not fulfilled by the SSN ecosystem are:

- *Discovery of Information*:
  - *DI1 Member States and User Communities must provide one or more points of access that facilitate standardised discovery of the services they provide to CISE participants;*
- *Collaboration between CISE participants:*
  - *CO3 CISE must support secure audio communication;*
  - *CO4 CISE must support secure video communication;*
  - *CO5 CISE must support secure instant messaging;*
  - *CO6 CISE must support secure white-boarding.*

4.2.2.1. Discovery of Available Information and Services

CISE requirements "***CISE must allow looking up what information CISE participants can provide and how they can provide that information***" (DI3) and "***CISE must allow information providers making available how their services can be used, including parameters such as the refresh rate***" (DI4) cater for the need for the systems involved in the information exchange to provide an easy way for other systems to find what *services* and what *information* are available.

The SSN ecosystem today provides a way to users discover the information provided at a non-automated level through well-known Web Services and other system-to-system interfaces. However, in order for a system to connect to those Web Services or other types of systems-to-system interfaces, the system developers need to have prior knowledge of the web services or system-to-system "definition information". The same can be said about the *information* itself: a common understanding of the *data* and *information* being shared is provided through available "data dictionaries" – understood here as the definition of the data being shared: among other

things, what data is exchanged, name, description, and characteristics of each data element, types of relationships between data elements, access rights and frequency of access.

In order to address the issue of automated discovery of available services, the following solutions are available:

- Service Catalogue; and
- Semantic Web Services.

The Service Catalogue is the tool through which systems can provide clear, easy-to-access services and support for other systems striving to exchange data, information or executing business processes. A "service catalogue" is a *Universal Description, Discovery, and Integration* (UDDI[40]) registry that contains a list of all the Web services available in a given application. This includes all participant manifest properties, such as the Uniform Resource Identifiers (URI) of the Web service, its name, Web Service Definition Language URI, credential and authentication types, and the policy document to associate with the Web service, if any.

The Semantic Web is the extension of the World Wide Web that enables people and systems to share *content* beyond the boundaries of applications. What is meant by "semantic" in the phrase Semantic Web is not that machines are going to understand the meaning of anything and everything, but that the logical pieces of *meaning* can be mechanically manipulated by a computer system to useful ends.

The convergence of semantic Web with service oriented computing is manifested by Semantic Web Services (SWS) technology. It addresses the major challenge of automated, interoperable and meaningful coordination of Web Services to be carried out by intelligent software agents.

Semantic web services are built around standards for the interchange of semantic data – *data ontologies*[41] or *linked data*[42] – which makes it easy for systems to combine data from different sources and services without losing meaning. Interpretation of terms in data or definitions is usually taken for granted. Ontologies are the means to avoid the misinterpretation of terms by formally describing a conceptualization. Ontologies explicitly describe terms using logical expressions and guarantee that the information in any instance of communication is consistently interpreted by both involved parties and therefore facilitate semantic integration of data and information.

EMSA already has plans for developing a service catalogue for the web services available in the SSN ecosystem and an ontology for the data required and made available by those web services (and later in general for all the SSN ecosystem data).

When such capabilities are available in the SSN ecosystem, the CISE requirements about discovery of available services and their parameters and discovery of available information will be considered fulfilled.

4.2.2.2. Confidence value for exchanged information

Currently not all SSN ecosystem interfaces include a "confidence value" for all the exchanged information.

According to the CISE requirement in discussion "*a confidence value is used to indicate the quality of and the trust in the information shared through CISE. The confidence value is an opinion, which is why the provider of the confidence value also needs to be identified in the information exchange. The combination of the confidence value and its provider supports the receiver of the information in making its decision as to use the information or not.*"

[40] UDDI is an XML-based standard for describing, publishing, and finding Web services. The UDDI specifications define a registry service for Web services and for other electronic and non-electronic services. A UDDI registry service is a Web service that manages information about service providers, service implementations, and service metadata. Service providers can use UDDI to advertise the services they offer. Service consumers can use UDDI to discover services that suit their requirements and to obtain the service metadata needed to consume those services.

[41] In computer science and information science, ontology formally represents knowledge as a set of concepts within a domain, using a shared vocabulary to denote the types, properties and interrelationships of those concepts.

[42] Linked Data describes a method to share information which can be read automatically by computers. It builds on Web standard technologies such as HTTP, RDF and URI's, enabling data from different sources to be connected and queried. In short, URIs and RDF are ways of exposing, sharing, and connecting pieces of data, information, and knowledge on the Semantic Web – in other words, a way to create "linked data".

Currently in the SSN ecosystem only specific interfaces possess "data qualification metrics" (for instance in CleanSeaNet) that can be used for providing a "confidence value".

In order to provide a "confidence value" for all the pertinent information to be exchanged in the scope of CISE, a thorough analysis of the data to be exchanged, origin of that data and availability of a way to create the "confidence value" needs to be performed.

Additionally, attention such be given to the benefits of such "confidence value" for each of the involved data sets, as not all data requires such "confidence value" and it most cases a way to determine such "confidence value" is not cost effective or even possible.

4.2.2.3. Priority Level for urgency of requested information

The SSN ecosystem partially fulfils the CISE requirement on "information requests must include a priority level reflecting the urgency of the request", because only a small subset of the ecosystem interfaces use such a parameter.

Additionally, the SSN ecosystem – as the majority of computer applications - usually treats information requests on a "first in – first served automatic" basis.

This type of parameter – priority level for urgency of requested information – only makes sense for certain type of data requests, for instance requests for data stored in "historical" or "offline" databases – that may require human intervention (as opposed to "automatic and almost immediate" computer processing).

As with the "Confidence Level", and in order to provide a "priority level for urgency of requested information" for all the SSN ecosystem pertinent information to be exchanged in the scope of CISE, a thorough analysis of that data, need for the "priority level" and ways to implement such mechanism is required.

4.2.2.4. Use of Commonly Agreed information classification scheme

The SSN ecosystem is partially compliant with the CISE requirement about "the use of information classification schemes" ("*CISE information exchanges must respect a commonly agreed information classification scheme supporting security levels from up to EU secret*"), due to the fact although it can support a commonly agreed classification scheme, there is currently no support for the handling of "highly secure-information" required by *EU secret* level.

As stated before, in order to be able to handle "highly-secure information" the SSN ecosystem will need to a) implement a secure information exchange protocol (e.g. "Two-way SSL", "HTTPS over TLS") for all the system-to-system interfaces that handle sensitive and highly-secure information; and b) implement Electronic Digital Rights Management mechanisms, if there is the need to enforce access and usage rights throughout the lifecycle of information usage.

4.2.2.5. Integrity of Information Exchanges

Integrity of information exchanges – "*CISE must use a messaging protocol that ensures a minimum level of integrity of information exchanges between consumer and provider. The messaging protocol must also ensure higher levels of integrity depending on the classification level of the information*" - involves two different aspects:

- *Identification of the sender*: the receiver can identify the sender performing the data transmissions;
- *Confidentiality of the transmission*: the information involved in the data transmission is accessible only to the sender and to the receiver, even though a public network might have been used to deliver the message.

A solution to ensure integrity of information exchanges over public networks is through the use of "two-way SSL" and Public Key Infrastructure (PKI) mechanisms.

Secure Sockets Layer (SSL) provides secure connections by allowing two applications connecting over a network connection to authenticate the other's identity and by encrypting the data exchanged between the applications.

Authentication allows a server and optionally a client to verify the identity of the application on the other end of a network connection. Encryption makes data transmitted over the network intelligible only to the intended recipient.

HTTPS (Hypertext Transfer Protocol over Secure Socket Layer or HTTP over SSL) is a mechanism that provides encrypted communication and secure identification of the communication participants, through the implementation of the Hypertext Transfer Protocol (HTTP) on top of the SSL/TLS protocol, thus adding the security capabilities of SSL/TLS to standard HTTP communications.

TLS (Transport Layer Security) is an IETF standards track protocol, first defined in 1999 and last updated in March 2011. It is based on the earlier SSL specifications (1994, 1995, and 1996). TLS uses stronger encryption algorithms and has the ability to work on different ports compared with SSL.

The terms SSL and TLS are often used interchangeably or in conjunction with each other (TLS/SSL), but one is in fact the predecessor of the other — SSL 3.0 served as the basis for TLS 1.0 which, as a result, is sometimes referred to as SSL 3.1.

Given the existence at EMSA of a Public Key Infrastructure (PKI), a solution to ensure integrity of information exchanges over public networks is through the use of "two-way SSL/TLS".

4.2.2.6. Secure Audio/Video/Instant Messaging/White-Boarding

Currently the SSN ecosystem does not provide a means for participants to easily interact with each other for:

- Secure audio communication: e.g. using a computer and a headset;
- Secure video communication: e.g. using a computer and webcam;
- Secure instant messaging: e.g. a chat tool;
- Secure white-boarding: online collaboration tools.

In order to provide Secure Audio/Video/Instant Messaging/White-Boarding capabilities in the SSN ecosystem, a commercial off-the-shelf tool (COTS) needs to be acquired. Examples of such tools are GoToMeeting from Citrix and Acrobat Connect Pro, from Adobe.

The rationale for the above approach is based on the following:

- *Cost*: EMSA can save considerable money and resources by purchasing COTS solutions, versus building them;
- *Quality*: Because the customer base of COTS providers is so broad, quality standards rapidly advance as the huge pool of users request enhancements that the companies are quick to incorporate. Also, "build" is not a core IT competency of EMSA. Its human assets are better directed toward mission-focused objectives, especially when there are COTS alternatives;
- *Speed*: COTS offerings get to users quicker than "purposely built solutions" because they are already available.

4.3. CISE DATA SETS

4.3.1. OVERALL TOP RESULTS

This chapter highlights the main results from the comparative analysis of SSN ecosystem with "CISE Framework", being focused on the analysis of 130 data groups, as previously explained.

Two scenarios have been tested: a weighted scenario where certain variables assume a higher weight than others (e.g. data need for operational tasks) and a baseline scenario to test the sensitivity of parameters. Analysis had confirmed that data groups more likely to be shared ("top results", above median, upper 50%) are not influenced by "weighting scenario", although the ordering within top results (upper 50%) is affected.

High scoring data groups (i.e. top results, corresponding to the up 50% of the 130 data groups where likelihood foe exchange is high) for all UCs, independently on scenario considered, include:

- "Ship position" data;
- "Ship pollution" data;
- "Resources localization for maritime interventions";
- "Maritime infrastructures" data; and
- "Legal maps" data.

The following table presents the "ranking in relevancy and likelihood to be exchanged of the 130 data groups" according the "comparative analysis" methodology (described earlier) and for all user communities:

Table 4-9: Relevance of CISE/TAG data sets to all user communities

TAG code	Data group description	Score	Ranking
A.1.1.1	Commercial ships position reporting (incl fishing vessel's AIS reports)	91,92	1
A.1.1.2	Fishing ships VMS position reporting	91,92	2
A.1.1.5	Other position reporting ships (yachts…)	89,77	3
A.2.1	Voyage-related Route data	89,77	4
B.1.5	Legal maps (SRR, EEZ, TW, ICES areas, RFMO areas, etc…)	86,32	5
A.2.2	Voyage-related Goods on board data	86,20	6
B.2.1	Meteo-oceanic data	85,31	7
A.1.3	Fishing Activity additional near-real time data	84,77	8
C.1.1	Position and tracking of assets (ships, aircrafts…)	82,45	9
A.2.4	Voyage-related Fishing data	81,20	10
A.1.2	Ship detection data (non-cooperative position data)	80,37	11
A.3.1.2	Fishing ships Characteristics (PERMANENT)	79,77	12
B.1.2	Maritime infrastructures	78,70	13
C.5.1	Pollutant	78,43	14
C.5.12	Identity of observer/reporter. Identity of ships on scene	77,95	15
B.2.3	Real Time Closure (RTC) of fishing areas	77,81	16
C.5.17	Intervention resources availability and location	77,00	17
A.3.1.1	Commercial ships Characteristics (PERMANENT)	76,02	18
A.2.3	Voyage-related Persons on board data	75,85	19
A.3.2.3	Other ships (yachts…) ownership and operation data	75,85	20
C.5.6	Behaviour of pollutant (floats, sinks, evaporates, dissolves, …)	75,57	21
C.5.7	Hazards related to the polluting substance	75,57	22
C.5.8	Characteristics of pollution	75,57	23
C.5.9	Source and cause of pollution	75,57	24
C.5.10	Drift of pollution (past/ expected)	75,57	25
C.5.11	Impact forecast	75,57	26
C.5.13	Action taken	75,57	27
A.3.3.1	Commercial ships identification data	75,13	28
A.3.3.2	Fishing ships identification data	75,13	29
C.5.18	To where assistance should be rendered and how	74,86	30

TAG code	Data group description	Score	Ranking
A.3.2.2	Fishing ships ownership and operation data	74,60	31
A.3.3.3	Other ships (yachts…) identification data	74,42	32
C.5.2	Anti-pollution resources	74,14	33
C.5.3	Position and/or extent of pollution on/ above/in the sea	74,14	34
C.2.5	Satellite Imagery - RADAR	73,94	35
B.1.3	Meteorological maps (winds, rain, squalls, visibility, etc., per season)	73,76	36
B.1.4	Oceanographic maps (tides, wave height, direction, period) per season	73,76	37
A.3.4.1	Commercial ships Historical data	73,70	38
A.3.1.3	Other ships (yachts…) Characteristics (PERMANENT)	72,99	39
C.1.2	Characteristics of assets	72,63	40
C.1.3	Contact details of assets	72,63	41
C.5.16	Pre-arrangements for the delivery of assistance	72,00	42
A.1.1.4	Governmental ships position reporting data (law enforcement missions)	71,74	43
A.1.1.3	Military ships position reporting data	71,74	44
B.1.1	Hydrographical maps (standard mandated)	71,62	45
C.4.6	Passengers and crew lists, Survivors found and rescued	71,56	46
C.5.4	Initial pollutant properties	71,29	47
C.5.5	Emulsion properties	71,29	48
C.5.15	Names of other states and organisations informed	71,29	49
A.3.2.1	Commercial ships ownership and operation data	70,85	50
C.2.6	Satellite Imagery - OPTIC	70,19	51
C.6.4	IUU Fishing	69,60	52
A.3.4.2	Fishing ships Historical data	69,42	53
C.7.7	Actual locations of merchant and fishing ships	69,24	54
C.6.6	navigation safety infringements	69,02	55
C.2.12	Intelligence	68,35	56
C.4.1	Accident/ incident report	67,81	57
C.4.2	Information associated with other distress situations	67,81	58
C.5.14	Photographs or samples	67,48	59
C.3.4	Company security officer	67,27	60
C.3.5	Ship security officer	67,27	61
C.3.8	Ship Security Plan (ISPS)	67,27	62
C.1.4	Ports of refuge data	66,56	63
C.3.7	Declaration of Security (DoS, as per SSPS risk asset)	66,27	64
C.5.19	Interfacing with existing Community Information portals	65,86	65
A.4.3	Fish farms, fish cages (idem)	65,67	66
C.3.1	Security alert	65,49	67
C.3.9	Ship specific security equipment	65,27	68
C.2.9	Electromagnetic signal localisation and interception (phones, VHF...)	64,48	69
C.8.2	Oil recovery and surveillance	63,70	70
B.1.10	protected Areas	63,52	71
C.3.3	Security certification (ISS certificate, initial ship sec asset report, last verification report, expiring date)	63,52	72
C.3.6	Security level	63,52	73
C.8.1	Environmental INCIDENT (BASIC DATA)	63,29	74
C.2.4	EOS pictures from airplanes or drones	62,69	75
C.3.2	Security measures taken	62,63	76
C.7.12	Data base that couples ship ID to ship description.	62,63	77
C.11.4	Hospitals	62,04	78
C.11.5	Medical care	62,04	79
C.11.6	Relief aid logistic management	62,04	80
A.4.1	Off-shore rigs data (position, operations, goods and persons on board, characteristics, ownership and operations, identification, historic…)	61,92	81
C.2.1	radar tracks from coast or ships	61,69	82
C.2.2	EOS pictures from coast or ships	61,69	83
C.2.3	radar tracks from airplanes or drones	61,69	84
B.1.11	protected/ endangered species	61,20	85
C.1.5	Pre-established SAR Coordination Plans	60,67	86
C.9.2	Required restricted area for shipping	60,60	87
C.3.10	Alert/ expiry of SSC (incl. possible grace period)	60,10	88
C.7.8	Actual locations of naval patrol ships and a/c	59,60	89
C.6.3	Terrorist threat	59,17	90

TAG code	Data group description	Score	Ranking
C.7.1	Initial Attack Report (IMO MSC1/ circ 1333)	58,88	91
C.7.2	Follow-up Attack Report (IMO MSC1/ circ 1334)	58,88	92
C.8.3	Sample collection	58,52	93
C.7.4	Maps (annotated) of piracy incident distribution per season.	58,35	94
C.6.1	Maritime Illegal migration	58,17	95
C.4.3	Ship security and evacuation equipment (slides, life rafts...)	57,81	96
B.2.2	Biochemical data	57,63	97
B.1.9	Possible seabed hazards (incl possible ancient mines, wrecks with dangerous goods, dumped ammunitions etc.)	57,45	98
C.7.3	Information about past piracy incidents (location, time, description of boats, what happened, etc.)	57,45	99
C.7.10	Locations of bases of patrol assets	57,45	100
C.7.9	Pirate ships/ attacks locations	56,92	101
C.10.1	Reasons of the evacuations (tsunami…)	56,86	102
A.3.4.3	Other ships (yachts…) Historical data	56,74	103
C.4.4	Rescue plans	55,67	104
A.4.2	Energy production plants (above or below water) idem	55,31	105
A.4.4	Dredging barges, floating cranes etc.	55,31	106
C.7.5	Maps of ship traffic distribution per ship type and per season	55,01	107
C.7.6	Shore bases of pirates and their current activity level	54,60	108
C.6.2	Organised crime	54,42	109
C.7.11	Maps (annotated) of past non-piracy incidents distribution per season (trafficking, smuggling, illegal fishing, terrorism…), not only on sea but also on the shores.	54,06	110
C.10.2	Pre-existing contingency plans	53,52	111
C.10.3	Decisions done	53,52	112
C.10.4	Alarm systems	53,52	113
C.10.5	Reaction actions	53,52	114
C.10.6	Movement to an area of refuge or an assembly station means	53,52	115
C.10.7	Transportation systems put on place	53,52	116
C.10.8	Evacuation orders	53,52	117
C.9.1	Explosive ordinance device detection / neutralisation	53,52	118
B.1.8	Remnant pollution (from shore, from wrecks…)	52,45	119
B.1.6	Marine resources (exploited)	51,26	120
B,1,7	Marine resources potential	50,55	121
C.2.8	Underwater detection and tracking (sonar)	50,37	122
C.2.10	Meteorological forecast/ very specific zone	47,52	123
C.6.5	Maritime Customs frauds	46,56	124
C.2.11	Samples	42,50	125
C.2.7	Acoustic signature(s), voice recordings…	41,67	126
C.4.5	Evacuation plan	40,42	127
C.11.2	Hazards mapping and tracking (chemical or nuclear clouds...)	39,64	128
C.11.1	Pre-existing contingency plans	36,79	129
C.11.3	Sealift planning and management	36,79	130

A first aspect to highlight from the analysis is that top results are not sensitive to weightings and that the top results (i.e. above median) are in its majority kept independent of the scenarios. However the relative positioning within the top results does present some difference.

There is however some few data groups in which this conclusion doesn't apply, i.e. data groups that are sensitive to the weights:

Data groups ranking high in weighted scenario (i.e. showing the importance of UC dependent variables as "operational use" and "data need") includes:

- Ship detection data (non-cooperative position data)
- Voyage-related Persons on board data
- Other ships (yachts…) ownership and operation data
- Identity of observer/reporter. Identity of ships on scene

- Satellite Imagery - RADAR
- Meteorological maps (winds, rain, squalls, visibility, etc., per season)
- Oceanographic maps (tides, wave height, direction, period) per season
- Governmental ships position reporting data (law enforcement missions)
- Military ships position reporting data
- Hydrographical maps (standard mandated)
- Satellite Imagery - OPTIC

On the other hand, data groups ranking higher in baseline scenario, i.e. that reflect the attenuation effect of weights of two variables (operational use and data need refer to:

- Characteristics of assets
- Contact details of assets
- Initial pollutant properties
- Emulsion properties
- Names of other states and organisations informed
- Commercial ships ownership and operation data
- IUU Fishing
- Ship Security Plan (ISPS)
- Company security officer
- Ship security officer
- Environmental INCIDENT (BASIC DATA)
- Hospitals
- Medical care
- Relief aid logistic management

As the sensitivity analysis to weight criteria confirms that top results are not influenced by the scenario selection, all the analysis conducted takes as reference scenario the "weighted" one, as the one that shows in a more evident way the relevance for each UC.

4.3.2. "COMPARATIVE ANALYSIS" PER USER COMMUNITY

It can note that there are some minor differences in the ranking when evaluating specifically each of the User Communities, as it could be expected. However such differences are not relevant at the point of impacting the identification of data groups more likely to be shared. The figure (*Figure 4-1: Results of data group ranking per UC*) below shows the results of data group scoring for each UC.

The red boxes of the chart show the proportion of data groups that had median or above median scores. These are the top results and represent the data groups of most likely to be exchanged for that UC. The white boxes show the scores below the median, those data groups the ones with less relevance for exchange for that UC.

While the red and white "boxes" show the middle or most typical results, the vertical lines plot the highest and lowest values i.e. the range of scores. In general the length of the lines indicates visually the extent of the range between maximum and minimum values from the median.

From the chart differences between the relevance that each UC attributes to data groups can be observed, clearly identifying 2 extreme patterns:

- Cases where the red boxes are larger and the vertical lines smaller (i.e. the case of UC Fisheries and Marine Environment), meaning a concentration of scores between the median and third quartile. This pattern indicates that most of top results in those UC are pertinent for the respective operational tasks;
- Cases where the red box is small and distance to maximum value (red line) is bigger (i.e. the case of UC Customs) which means that scores from median to maximum value are dispersed. This indicates there is a considerable difference between the pertinent data groups for the operational tasks (those with maximum score) and all other data groups scored above the median.

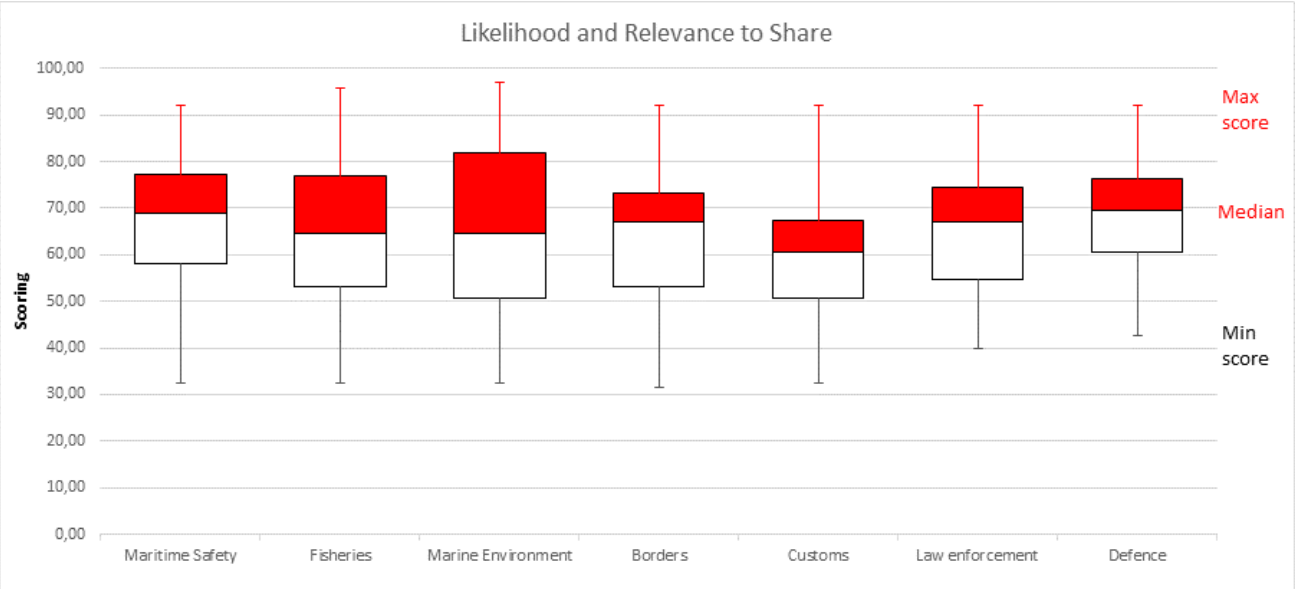


Figure 4-1: Results of data group ranking per UC

Upper 25% results for each UC are below detailed.

Table 4-10: Upper 25% results for UC "Maritime Safety"

TAG code	Data group description	Score
A.1.1.1	Commercial ships position reporting (incl. fishing vessel's AIS reports)	91,92
A.1.1.2	Fishing ships VMS position reporting	91,92
A.1.1.5	Other position reporting ships (yachts…)	91,92
A.2.1	Voyage-related Route data	91,92
A.2.2	Voyage-related Goods on board data	91,92
C.1.1	Position and tracking of assets (ships, aircrafts…)	88,17
A.3.1.1	Commercial ships Characteristics (PERMANENT)	88,17
B.2.1	Meteo-oceanic data	88,17
B.1.5	Legal maps (SRR, EEZ, TW, ICES areas, RFMO areas, etc…)	87,75
C.5.17	Intervention resources availability and location	87,00
C.6.6	navigation safety infringements	86,17
A.2.3	Voyage-related Persons on board data	84,42
A.3.2.1	Commercial ships ownership and operation data	84,42
A.3.4.1	Commercial ships Historical data	84,42
C.1.4	Ports of refuge data	84,42
C.4.6	Passengers and crew lists, Survivors found and rescued	84,42
B.1.2	Maritime infrastructures	84,42
A.1.3	Fishing Activity additional near-real time data	81,92
C.1.2	Characteristics of assets	81,92
C.1.3	Contact details of assets	81,92
A.1.2	Ship detection data (non-cooperative position data)	81,08
C.2.5	Satellite Imagery - RADAR	81,08
B.2.3	Real Time Closure (RTC) of fishing areas	80,67
C.7.7	Actual locations of merchant and fishing ships	80,67
A.4.3	Fish farms, fish cages (idem)	80,67
C.1.5	Pre-established SAR Coordination Plans	80,67
C.4.1	Accident/ incident report	80,67
C.4.2	Information associated with other distress situations	80,67
C.4.3	Ship security and evacuation equipment (slides, life rafts…)	80,67
B.1.1	Hydrographical maps (standard mandated)	77,33
B.1.3	Meteorological maps (winds, rain, squalls, visibility, etc., per season)	77,33
B.1.4	Oceanographic maps (tides, wave height, direction, period) per season	77,33
C.2.6	Satellite Imagery - OPTIC	77,33

Table 4-11: Upper 25% results for UC "Fisheries"

TAG code	Data group description	Score
B.2.3	Real Time Closure (RTC) of fishing areas	95,67
A.1.1.1	Commercial ships position reporting (incl fishing vessel's AIS reports)	91,92
A.1.1.2	Fishing ships VMS position reporting	91,92
A.1.3	Fishing Activity additional near-real time data	91,92
A.2.1	Voyage-related Route data	91,92
A.2.4	Voyage-related Fishing data	91,92
A.3.1.2	Fishing ships Characteristics (PERMANENT)	91,92
C.1.1	Position and tracking of assets (ships, aircrafts…)	88,17
A.3.2.2	Fishing ships ownership and operation data	88,17
B.2.1	Meteo-oceanic data	88,17
C.6.4	IUU Fishing	88,17
B.1.5	Legal maps (SRR, EEZ, TW, ICES areas, RFMO areas, etc…)	87,75
A.1.1.5	Other position reporting ships (yachts…)	86,92
A.2.2	Voyage-related Goods on board data	86,92
B.1.2	Maritime infrastructures	84,42
C.2.5	Satellite Imagery - RADAR	81,08
C.7.7	Actual locations of merchant and fishing ships	80,67
A.4.3	Fish farms, fish cages (idem)	80,67
B.1.10	protected Areas	80,67
A.2.3	Voyage-related Persons on board data	79,42
B.1.1	Hydrographical maps (standard mandated)	77,33
B.1.3	Meteorological maps (winds, rain, squalls, visibility, etc., per season)	77,33
B.1.4	Oceanographic maps (tides, wave height, direction, period) per season	77,33
C.2.6	Satellite Imagery - OPTIC	77,33
C.5.1	Pollutant	77,00
C.5.6	Behaviour of pollutant (floats, sinks, evaporates, dissolves, …)	77,00
C.5.7	Hazards related to the polluting substance	77,00
C.5.8	Characteristics of pollution	77,00
C.5.9	Source and cause of pollution	77,00
C.5.10	Drift of pollution (past/ expected)	77,00
C.5.11	Impact forecast	77,00
C.5.13	Action taken	77,00

Table 4-12: Upper 25% results for UC "Marine Environment & Pollution"

TAG code	Data group description	Score
C.5.1	Pollutant	97,00
C.5.2	Anti-pollution resources	97,00
C.5.3	Position and/or extent of pollution on/ above/in the sea	97,00
C.5.4	Initial pollutant properties	97,00
C.5.5	Emulsion properties	97,00
C.5.6	Behaviour of pollutant (floats, sinks, evaporates, dissolves, ...)	97,00
C.5.7	Hazards related to the polluting substance	97,00
C.5.8	Characteristics of pollution	97,00
C.5.9	Source and cause of pollution	97,00
C.5.10	Drift of pollution (past/ expected)	97,00
C.5.11	Impact forecast	97,00
C.5.13	Action taken	97,00
C.5.16	Pre-arrangements for the delivery of assistance	97,00
C.5.17	Intervention resources availability and location	97,00
C.5.18	To where assistance should be rendered and how	97,00
C.5.12	Identity of observer/reporter. Identity of ships on scene	93,67
A.1.1.1	Commercial ships position reporting (incl fishing vessel's AIS reports)	91,92
A.1.1.2	Fishing ships VMS position reporting	91,92
A.2.1	Voyage-related Route data	91,92
C.5.14	Photographs or samples	90,33
C.1.1	Position and tracking of assets (ships, aircrafts...)	88,17
B.2.1	Meteo-oceanic data	88,17
B.1.5	Legal maps (SRR, EEZ, TW, ICES areas, RFMO areas, etc...)	87,75
C.5.15	Names of other states and organisations informed	87,00
A.1.1.5	Other position reporting ships (yachts...)	86,92
B.1.2	Maritime infrastructures	84,42
C.8.2	Oil recovery and surveillance	84,42
C.8.1	Environmental INCIDENT (BASIC DATA)	84,00
A.1.3	Fishing Activity additional near-real time data	81,92
A.2.2	Voyage-related Goods on board data	81,92
A.3.1.2	Fishing ships Characteristics (PERMANENT)	81,92
C.1.2	Characteristics of assets	81,92
C.1.3	Contact details of assets	81,92

Table 4-13: Upper 25% results for UC "Borders"

TAG code	Data group description	Score
A.1.1.1	Commercial ships position reporting (incl fishing vessel's AIS reports)	91,92
A.1.1.2	Fishing ships VMS position reporting	91,92
A.1.1.5	Other position reporting ships (yachts…)	91,92
A.2.1	Voyage-related Route data	91,92
B.2.1	Meteo-oceanic data	88,17
C.1.1	Position and tracking of assets (ships, aircrafts…)	88,17
B.1.5	Legal maps (SRR, EEZ, TW, ICES areas, RFMO areas, etc…)	87,75
A.2.3	Voyage-related Persons on board data	84,42
A.3.2.3	Other ships (yachts…) ownership and operation data	84,42
A.3.3.1	Commercial ships identification data	84,42
A.3.3.2	Fishing ships identification data	84,42
A.3.3.3	Other ships (yachts…) identification data	84,42
A.1.3	Fishing Activity additional near-real time data	81,92
A.2.2	Voyage-related Goods on board data	81,92
A.2.4	Voyage-related Fishing data	81,92
A.1.2	Ship detection data (non-cooperative position data)	81,08
C.2.5	Satellite Imagery - RADAR	81,08
C.2.6	Satellite Imagery - OPTIC	77,33
C.5.13	Action taken	77,00
C.5.15	Names of other states and organisations informed	77,00
C.5.17	Intervention resources availability and location	77,00
C.5.18	To where assistance should be rendered and how	77,00
C.1.2	Characteristics of assets	76,92
C.1.3	Contact details of assets	76,92
C.2.12	Intelligence	76,92
C.3.1	Security alert	76,92
C.3.2	Security measures taken	76,92
C.7.9	Pirate ships/ attacks locations	76,92
A.3.4.1	Commercial ships Historical data	74,42
A.3.4.2	Fishing ships Historical data	74,42
C.4.6	Passengers and crew lists, Survivors found and rescued	74,42
C.5.12	Identity of observer/reporter. Identity of ships on scene	73,67
A.1.1.3	Military ships position reporting data	73,17
A.1.1.4	Governmental ships position reporting data (law enforcement missions)	73,17

Table 4-14: Upper 25% results for UC "Customs"

TAG code	Data group description	Score
A.1.1.1	Commercial ships position reporting (incl fishing vessel's AIS reports)	91,92
A.1.1.2	Fishing ships VMS position reporting	91,92
A.1.3	Fishing Activity additional near-real time data	91,92
A.2.1	Voyage-related Route data	91,92
A.2.2	Voyage-related Goods on board data	91,92
A.2.4	Voyage-related Fishing data	91,92
A.3.1.2	Fishing ships Characteristics (PERMANENT)	91,92
A.3.1.1	Commercial ships Characteristics (PERMANENT)	88,17
C.6.4	IUU Fishing	88,17
A.1.1.5	Other position reporting ships (yachts…)	86,92
A.3.1.3	Other ships (yachts…) Characteristics (PERMANENT)	84,42
A.3.3.1	Commercial ships identification data	84,42
A.3.3.2	Fishing ships identification data	84,42
A.3.3.3	Other ships (yachts…) identification data	84,42
A.1.2	Ship detection data (non-cooperative position data)	81,08
A.3.2.2	Fishing ships ownership and operation data	78,17
B.2.1	Meteo-oceanic data	78,17
B.1.5	Legal maps (SRR, EEZ, TW, ICES areas, RFMO areas, etc…)	77,75
C.5.1	Pollutant	77,00
B.1.11	protected/ endangered species	76,92
C.2.12	Intelligence	76,92
A.3.2.1	Commercial ships ownership and operation data	74,42
A.3.2.3	Other ships (yachts…) ownership and operation data	74,42
B.1.2	Maritime infrastructures	74,42
C.6.3	Terrorist threat	74,17
C.5.12	Identity of observer/reporter. Identity of ships on scene	73,67
A.1.1.3	Military ships position reporting data	73,17
A.1.1.4	Governmental ships position reporting data (law enforcement missions)	73,17
C.6.1	Maritime Illegal migration	73,17
B.2.3	Real Time Closure (RTC) of fishing areas	70,67
C.6.2	Organised crime	69,42
C.6.5	Maritime Customs frauds (please develop the specific data supporting such investigations)	69,42
B.1.1	Hydrographical maps (standard mandated)	67,33

Table 4-15: Upper 25% results for UC "Law Enforcement"

TAG code	Data group description	Score
A.1.1.1	Commercial ships position reporting (incl fishing vessel's AIS reports)	91,92
A.1.1.2	Fishing ships VMS position reporting	91,92
A.1.1.5	Other position reporting ships (yachts…)	91,92
A.2.1	Voyage-related Route data	91,92
A.2.2	Voyage-related Goods on board data	91,92
A.2.4	Voyage-related Fishing data	91,92
A.3.1.2	Fishing ships Characteristics (PERMANENT)	91,92
C.1.1	Position and tracking of assets (ships, aircrafts…)	88,17
A.3.1.1	Commercial ships Characteristics (PERMANENT)	88,17
A.3.2.2	Fishing ships ownership and operation data	88,17
B.1.5	Legal maps (SRR, EEZ, TW, ICES areas, RFMO areas, etc…)	87,75
A.2.3	Voyage-related Persons on board data	84,42
A.3.1.3	Other ships (yachts…) Characteristics (PERMANENT)	84,42
A.3.2.1	Commercial ships ownership and operation data	84,42
A.3.2.3	Other ships (yachts…) ownership and operation data	84,42
A.3.3.1	Commercial ships identification data	84,42
A.3.3.2	Fishing ships identification data	84,42
A.3.3.3	Other ships (yachts…) identification data	84,42
B.1.2	Maritime infrastructures	84,42
A.1.3	Fishing Activity additional near-real time data	81,92
A.1.2	Ship detection data (non-cooperative position data)	81,08
B.2.3	Real Time Closure (RTC) of fishing areas	80,67
C.7.7	Actual locations of merchant and fishing ships	80,67
B.2.1	Meteo-oceanic data	78,17
B.1.1	Hydrographical maps (standard mandated)	77,33
C.5.1	Pollutant	77,00
C.2.12	Intelligence	76,92
C.7.12	Data base that couples ship ID to ship description.	76,92
C.7.4	Maps (annotated) of piracy incident distribution per season.	76,92
A.3.4.1	Commercial ships Historical data	74,42

Table 4-16: Upper 25% results for UC "Defence"

TAG code	Data group description	Score
A.1.1.1	Commercial ships position reporting (incl fishing vessel's AIS reports)	91,92
A.1.1.2	Fishing ships VMS position reporting	91,92
A.1.1.5	Other position reporting ships (yachts…)	91,92
B.2.1	Meteo-oceanic data	88,17
B.1.5	Legal maps (SRR, EEZ, TW, ICES areas, RFMO areas, etc…)	87,75
B.1.2	Maritime infrastructures	84,42
C.5.12	Identity of observer/reporter. Identity of ships on scene	83,67
A.1.3	Fishing Activity additional near-real time data	81,92
A.1.2	Ship detection data (non-cooperative position data)	81,08
C.2.5	Satellite Imagery - RADAR	81,08
C.7.7	Actual locations of merchant and fishing ships	80,67
C.2.9	Electromagnetic signal localisation and interception (phones, VHF…)	77,33
B.1.1	Hydrographical maps (standard mandated)	77,33
B.1.3	Meteorological maps (winds, rain, squalls, visibility, etc., per season)	77,33
B.1.4	Oceanographic maps (tides, wave height, direction, period) per season	77,33
C.2.6	Satellite Imagery - OPTIC	77,33
C.5.1	Pollutant	77,00
C.5.2	Anti-pollution resources	77,00
C.5.3	Position and/or extent of pollution on/ above/in the sea	77,00
C.5.6	Behaviour of pollutant (floats, sinks, evaporates, dissolves, …)	77,00
C.5.7	Hazards related to the polluting substance	77,00
C.5.8	Characteristics of pollution	77,00
C.5.9	Source and cause of pollution	77,00
C.5.10	Drift of pollution (past/ expected)	77,00
C.5.11	Impact forecast	77,00
C.5.17	Intervention resources availability and location	77,00
C.5.18	To where assistance should be rendered and how	77,00
A.2.1	Voyage-related Route data	76,92
A.2.2	Voyage-related Goods on board data	76,92
C.2.12	Intelligence	76,92
C.3.1	Security alert	76,92
C.7.12	Data base that couples ship ID to ship description.	76,92
C.7.4	Maps (annotated) of piracy incident distribution per season.	76,92

4.3.3. AVAILABILITY OF THE CISE DATA GROUPS IN THE SSN ECOSYSTEM

For the "comparative analysis" of the SSN ecosystem available data against the "CISE data sets" an evaluation of SSN coverage was done. It should be remembered that the assessments herewith conducted are done for the 130 data groups and not for all the CISE data sets.

The analysis considers as "SSN coverage" all the data groups provided directly by the SSN ecosystem (i.e. *Commercial ships position reporting*) and the data groups provided by other UCs, but for which the SSN ecosystem is capable to ingest, process and/or disseminate through the Maritime Services in SSN ecosystem (i.e. *Fishing ships VMS position reporting).*

Figure 4-2 shows the overall SSN coverage considering top results (i.e. upper 50%) and upper results (i.e. upper 25%) of the 130 data groups.

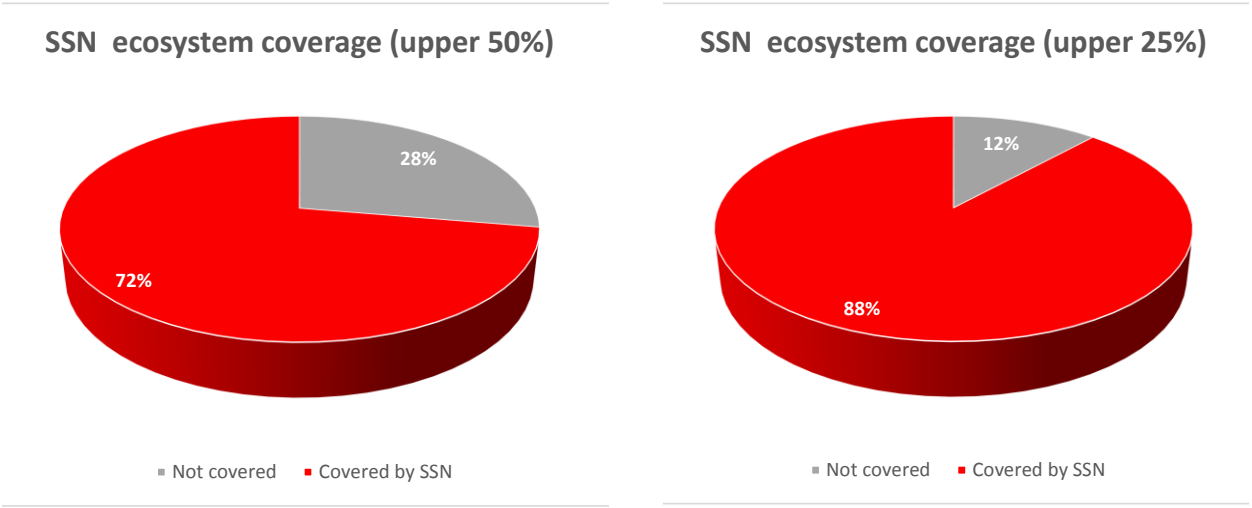


Figure 4-2: Overall assessment of SSN coverage (all UC) for top and upper results

Figure 4-3 below shows the overall SSN coverage per UC while Figure 4-4 separates the SSN coverage between data groups directly provided by SSN and data groups processed via SSN through maritime services.

Figure 4-3 clearly shows that for the data groups most likely to be shared (i.e. upper 50%), coverage (and/or capacity to ingest, process and exchange) by SSN ecosystem is high across all the UCs, being particularly high for the UC "Fisheries".

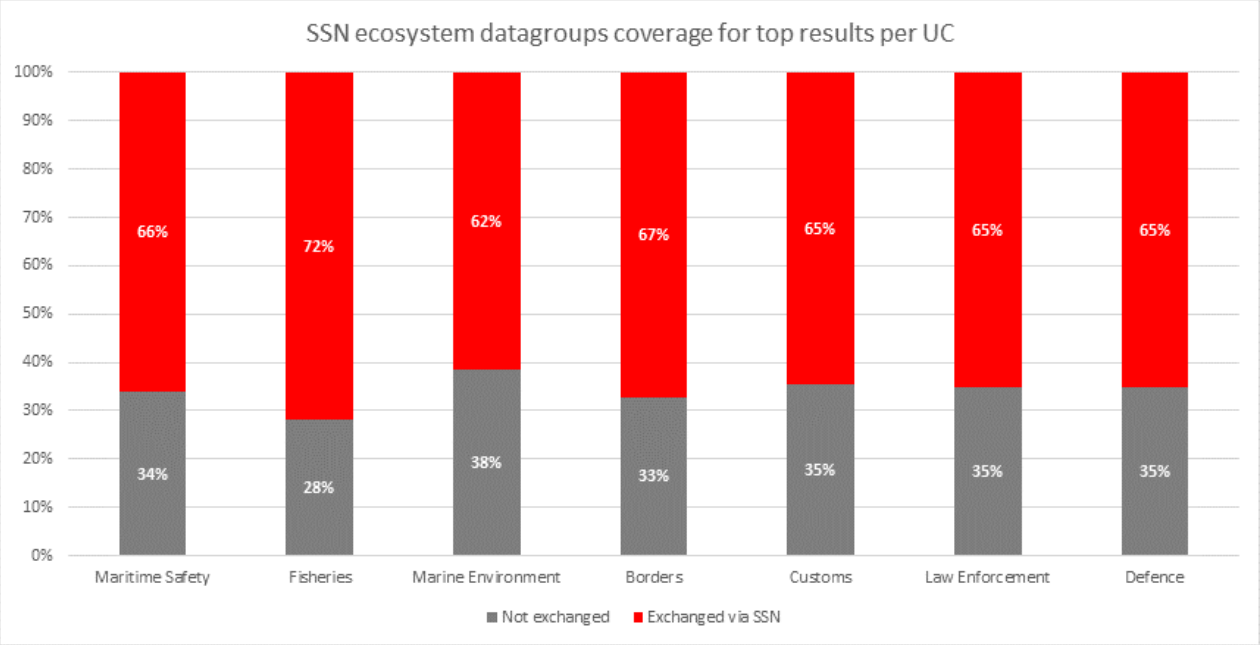


Figure 4-3: Overall assessment of SSN coverage per UC

When separating the data groups covered by SSN (in red in figure above) between those that are endogenous to SSN ecosystem (in red) and those that are provided via Maritime Services (in green), the results confirm the important role fulfilled by the SSN ecosystem as provider of tailored services for the different UC as shown in Figure 4-4.

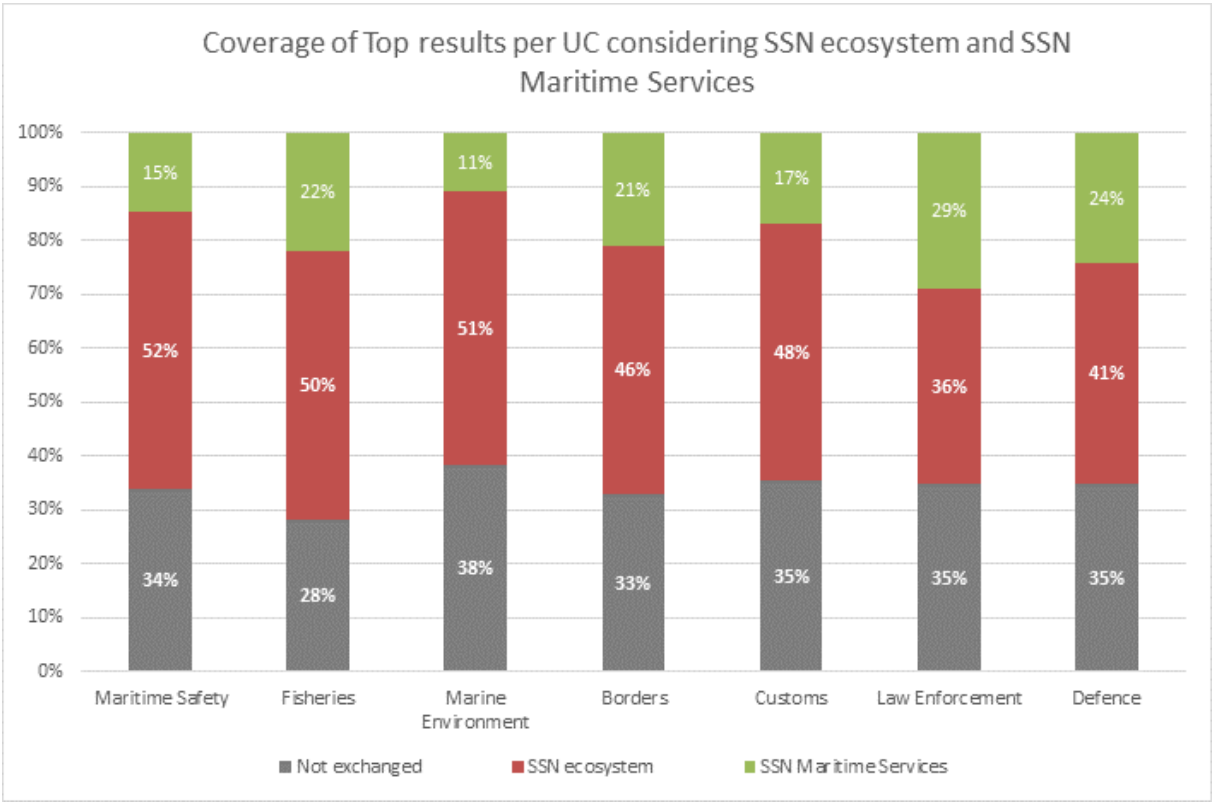


Figure 4-4: SSN coverage of Top results per UC (SSN ecosystem and SSN Maritime Services)

The added value that SSN usage for exchanging data is even clearer when it was evaluated against the data currently owned by each UC as highlighted in Figure 4-5.

As can be observed, and already acknowledged by the TAG and also in Task 1 report of current study, there are substantial differences regarding the amount of data owned by each community, with Maritime Safety and Defence as the communities with more data owned. This situation is more accentuated when observing only the results ranked as top ones.

When considering that subset of data groups, Law Enforcement and Customs clearly present the lowest amount of data owned, consequently being the two communities for which the added value of using SSN data is higher (as it would greatly increase the amount of data available to those communities), while for communities with high data owned, the added value of data exchanged via SSN is lower.

The added value that SSN ecosystem possesses for exchanging data is even clearer when it was evaluated against the data currently owned by each User Community (UC). The data groups covered by the SSN ecosystem represent a substantial value for all the UCs, catering for the coverage of at least more 32% (defence) up to 64% (law enforcement) of data groups most likely to be shared, compared to the ones covered by own data.

At the same time the below figure clearly shows that the two user communities having access to and managing most of the data are Maritime Safety and Defence. Hence there is a gap identified in how the (relevant) information, in particular the one held by the defence, could be exchanged/shared with the other (civilian) communities.

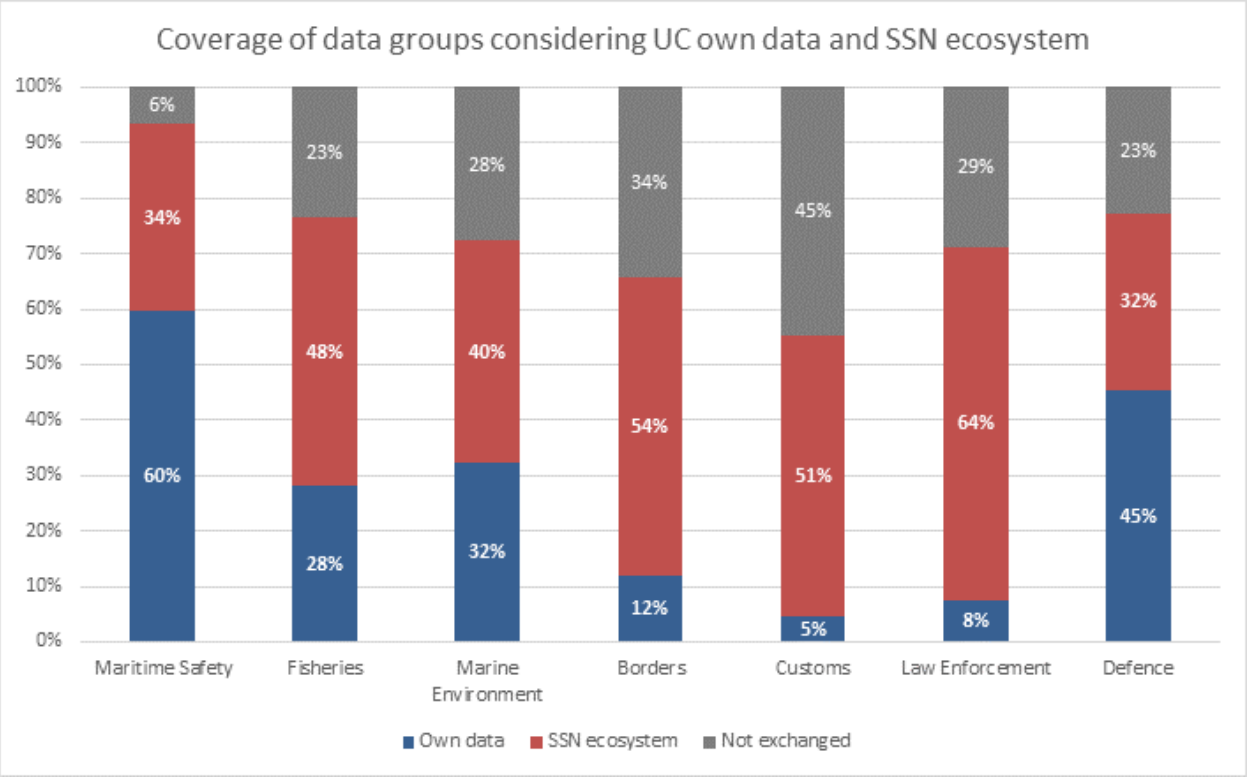


Figure 4-5: SSN coverage per UC considering data owned by the UC, for the Top results

4.3.4. ANALYSIS OF THE RESULTS

The "comparative analysis" assessment highlighted that the data groups more likely to be shared for all user communities are the data groups related to:

- "Ship position" data;

- "Voyage-related" data;
- "Maritime infrastructures" data; and
- "Legal maps" data.
- At the same time fig 4-5 SSN coverage per UC considering data owned by the UC, clearly shows that the two user communities having most 'own' data are maritime safety and defence. Hence there is a gap identified in how the (relevant) information, in particular held by the defence, could be exchanged/shared with the other (civilian) communities.

As described above, in the *"Mapping of Data Sets and Gap Analysis"* ([RD.8]) the TAG compiled a "*representative but non-exhaustive inventory of all types of maritime surveillance relevant data across sectors and borders within the EU"*. It is important to highlight some issues about this list:

- The data set list is not "balanced": some data sets have a high level of detail (e.g. "A.1.1.1 - Commercial ships position reporting (incl. fishing vessel's AIS reports)") while others do not have any detail at all (e.g. "B.2.1.7 - Ice information)";
- Some data sets are not sufficiently detailed in order to understand unequivocally the full extent of what that data covers: e.g. "C.2.12 – Intelligence", "C.11.5 – Medical care", etc.;
- Some data sets may have different meanings for different user communities, e.g. "C.2.11 Samples" may be understood differently by the "Marine Environment" and "Law Enforcement" user communities.

It is also important to differentiate in our analysis which data sets are provided natively by the SSN ecosystem - e.g. "*A.1.1.1 - Commercial ships position reporting (incl. fishing vessel's AIS reports)*" - and the data sets that are provided by other user communities, but which the SSN ecosystem ingests, processes and/or disseminates - e.g. "*A.1.1.2 - Fishing ships VMS position reporting*".

Before assessing in detail the results for the 130 data groups it is worth to mention again that within these data groups, some data is of more interest to maritime user communities than other, either because that data is currently under a "legal obligation to collect" and/or collected and recorded in an information system. However, the 130 data groups include not only this type of data but also data deemed relevant in the context of CISE which is not currently reported in any information system. As such the overall comparison of the SSN ecosystem data is relevant not with the overall 130 data groups but with the data groups "more likely to be shared" as these data groups represent the core of the data for all the involved user communities.

Taking these considerations into account, the "comparative analysis" of the SSN ecosystem available data against the "CISE data sets compiled by TAG" has yielded the following results[43]:

- Of the 130 data groups, 45% are available in the SSN ecosystem, of which:
  - 27% are "native" to the ecosystem;
  - 18% have origin in other user communities.

[43] See deliverable "D3.2 – Task 3 Comparative Analysis" for further information – [RD.9].

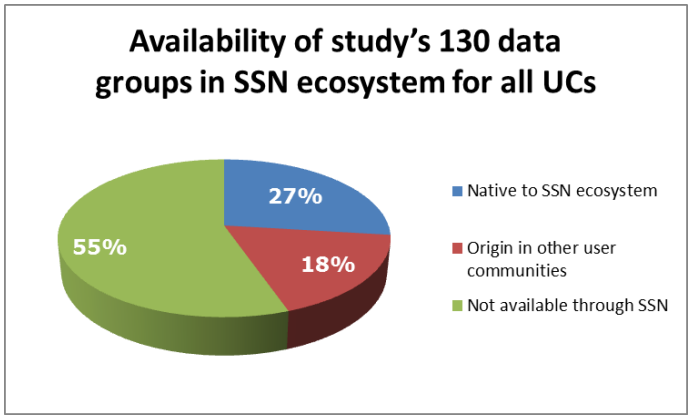


Figure 4-6: Availability of study's 130 data groups in SSN ecosystem for all UCs – All data groups

- Of the "top results" (i.e. the 50% of the 130 data groups with the highest scores), 72% are/can be exchanged through the SSN ecosystem, of which:
  - 54% are "native" to the ecosystem;
  - 18% have origin in other user communities.

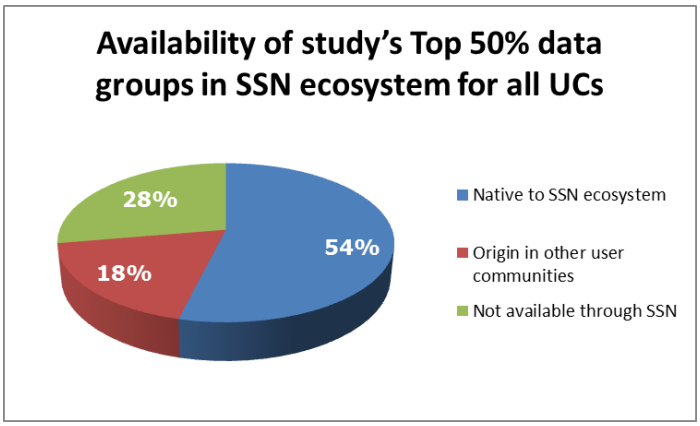


Figure 4-7: Availability of study's 130 data groups in SSN ecosystem for all UCs - Top 50%

- Of the "top 25%" (i.e. the 25% of the 130 data groups with the highest scores), 88% can be exchanged through the SSN ecosystem, of which:
  - 67% are "native" to the ecosystem;
  - 21% have origin in other user communities.

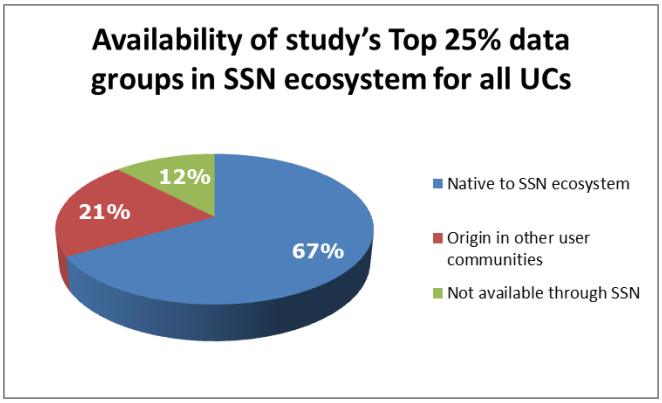


Figure 4-8: Availability of study's 130 data groups in SSN ecosystem for all UCs - Top 25%

The following table summarises the results above.

Table 4-17: Availability of study's 130 data groups in SSN ecosystem for all UCs

Type	All Data Groups		Top 50%		Top 25%	
Native to SSN ecosystem[44]	35	27%	35	54%	22	67%
Origin in other user communities[45]	23	18%	12	18%	7	21%
Not available through SSN	72	55%	18	28%	4	12%
	130	100%	65	100%	33	100%

Based on the table above, **it can be inferred is clear that SSN ecosystem data is a powerful system within the context of exchanging data between different users/communities,** since of the 130 data groups analysed, 45% of them are native or exchanged through the SSN ecosystem. This percentage grows even further if the highest ranked data groups are used: 72% in the case of the "Top 50%" and 88% for the "Top 25%" results.

This is also illustrated in the graph below by the increasing significance of the aforementioned data as a proportion of the data groups with respect to the "likelihood and relevance to share" for all user communities.

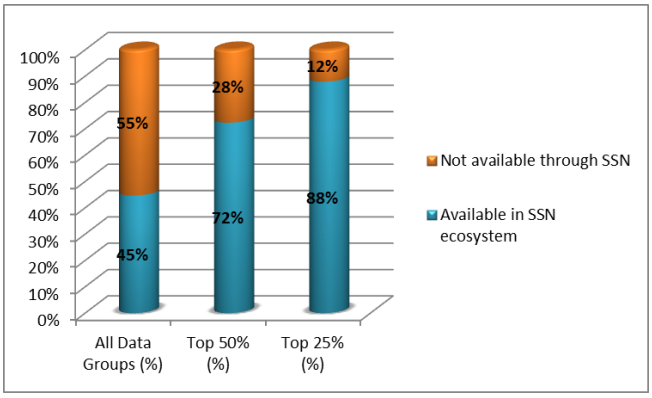


Figure 4-9: Relevancy of SSN ecosystem data

[44] Information available or created in SSN, CSN, EU LRIT CDC, THETIS and IMDatE.

[45] Data available in the SSN ecosystem, but with origin in (external) systems other than SSN, CSN, EU LRIT CDC, THETIS and IMDatE. Example: fishing vessels positioning information obtained through VMS.

4.3.4.1. Data Groups not Exchanged/Available in the SSN ecosystem

4.3.4.1.1. Top 25% ranked data groups

In the "Top 25%" data groups more likely to be shared, the 12% which are not currently available *in* or *through* the SSN ecosystem are:

- "A.2.4 - Voyage-related Fishing data";
- "B.1.2 – Maritime infrastructures";
- "B.2.3 – Real Time Closure (RTC) of fishing areas"; and
- "A.3.2.3 – Other ships (yachts…) ownership and operation data".

Regarding the "B.2.3 - Real Time Closure (RTC) of fishing areas" data group, no additional detail is provided in the CISE documentation, but for the other data groups, the following elements are enumerated:

- "A.2.4 - Voyage-related Fishing data":
  - A.2.4.1 Gear - type & mesh size (on-board/in use)
  - A.2.4.2 Destination - Crossing EEZ (COE/COX)
  - A.2.4.3 Destination - Checkpoint (CON)
  - A.2.4.4 Catch on board by species
  - A.2.4.5 Catch to be landed by species
- "B.1.2 - Maritime infrastructures":
  - B1.2.1 oil rigs
  - B1.2.2 wind farms
  - B1.2.3 underwater mining
  - B1.2.4 other permanent infrastructure
- "A.3.2.3 - Other ships (yachts…) ownership and operation data":
  - A.3.2.3.1 Type, class (As per A.1.2.2)
  - A.3.2.3.2 Name, number
  - A.3.2.3.3 Port of registry
  - A.3.2.3.4 Other registrations (optional national registers, specific licences...)
  - A.3.2.3.5 Flag state - current
  - A.3.2.3.6 Home Port
  - A.3.2.3.7 Ship owner / charterer
  - A.3.2.3.8 Ship company
  - A.3.2.3.9 skipper / known passengers
  - A.3.2.3.10 Vessel mobile phone 2G, 3G etc.
  - A.3.2.3.11 Vessel Satellite Phone
  - A.3.2.3.12 International Radio Call Sign
  - A.3.2.3.13 Latest Port State control
  - A.3.2.3.14 Current classification society
  - A.3.2.3.15 global characteristics (length, beam, draught, max passengers, range without refuelling, propulsion power, maximum speed…)
  - A.3.2.3.16 Identification clues (colour, marking etc.) (picture, text..)
  - A.3.2.3.17 Elements of suspicion, eventual antecedents etc.

It can be noted that two of these data groups ("B.2.3 - Real Time Closure (RTC) of fishing areas" and "A.2.4 - Voyage-related Fishing data") are specific to the Fisheries user community and the need to collect these elements was not part of the SSN ecosystem scope. From a technical perspective and based on the information available, it is technically feasible to exchange both data groups through the SSN ecosystem. This could be un-

dertaken by making use of IMDatE capabilities and extending the existing "Fisheries monitoring service" to ingest and disseminate the aforementioned information (which is technically feasible to do it within the IMDatE platform.

The information required in data group "A.3.2.3 - Other ships (yachts…) ownership and operation data" is similar to the information required in data group "A.3.2.1 - Commercial ships ownership and operation data" which is already available in the SSN ecosystem. As such, ingesting and disseminating the data on data group "A.3.2.3" is not foreseen to create any major difficulties or require major changes in the SSN ecosystem.

The "B.1.2 - Maritime infrastructures" data group appear in the TAG classification under "B.1 - Charts and Maps (permanent data)". Assuming that this refers to charts and maps of maritime infrastructures, the main problem in this case is not how SSN ecosystem is able to ingest and disseminate information, is how to gather the information since the data related to these infrastructures is either not available of dispersed in several entities (public and private). From a technical perspective, the SSN ecosystem has sufficient geographical information system (GIS) capabilities to ingest, store and disseminate this type of information. This geographical information infrastructure (from several vendors like ESRI, Jepessen and the open source community) serves the following main purposes:

- Supports the "Web Service" Interfaces (W*S) of the SSN ecosystem applications;
- Provides Nautical Charts (e.g. ship routing systems, navigation aids, nautical background, administrative boundaries, dangerous areas) to the SSN ecosystem applications;
- Provides geo-referenced basic data (e.g. geographical grip – parallel and meridian lines, countries, cities, seas, and traffic separation schemes), marine infrastructures data (e.g. AIS, stations), and ports location data.

4.3.4.1.2. Top 50% ranked data groups

Besides the ones mentioned in the section above (for the "Top 25% ranked data groups"), the data groups in the "Top Results" (Top 50% ranked data groups) currently not available or exchanged through the SSN ecosystem are the following:

- "B.1.3 - Meteorological maps (winds, rain, squalls, visibility, etc., per season)"
- "B.1.4 - Oceanographic maps (tides, wave height, direction, period) per season"
- "A.3.1.3 - Other ships (yachts…) Characteristics (PERMANENT)"
- "A.1.1.4 - Governmental ships position reporting data (law enforcement missions)"
- "A.1.1.3 - Military ships position reporting data"
- "C.2.12 – Intelligence"
- "C.4.2 - Information associated with other distress situations"
- "C.3.4 - Company security officer"
- "C.3.5 - Ship security officer"
- "C.3.8 - Ship Security Plan (ISPS)"
- "C.1.4 - Ports of refuge data"
- "C.3.7 - Declaration of Security (DoS, as per SSPS risk asset)"

The following analysis and remarks can be made about these data groups:

- Regarding groups "B.1.3 - Meteorological maps (winds, rain, squalls, visibility, etc., per season)" and "B.1.4 - Oceanographic maps (tides, wave height, direction, period) per season": from a technical perspective, the SSN ecosystem has sufficient geographical information system (GIS) and database capabilities to provide this type of information if required, however it is important to note that EMSA's focus is make use of existing met-ocean information systems at MS level (or at EU level) and avoid any unnecessary ingestion and storage of data. Within this context the SSN ecosystem has the possibility to interface with such met-ocean systems and deliver the required information to the users without duplication of effort;

- The information required concerning yachts ("A.3.1.3 - Other ships (yachts…) Characteristics (PERMANENT)") is similar to the one available in the SSN ecosystem "Vessel Reference Registries". Therefore ingesting, processing and disseminating this information – from a technical perspective – is not expected to create unsurmountable problems;
- The same can be said of "A.1.1.4 - Governmental ships position reporting data (law enforcement missions)" and "A.1.1.3 - Military ships position reporting data" which are similar to SSN ecosystem's "A.1.1. - Commercial ships position reporting (incl fishing vessel's AIS reports)";
- No information is provided in the TAG documentation[46] about "C.4.2 - Information associated with other distress situations" to deduct detailed needs and technical limitations of the SSN ecosystem;
- With respect to "C.3 - Security of commercial shipping" data groups (C.3.4, C.3.5 and C.3.8) it is worth highlighting that security (ISPS) related information is considered "sensitive" or "confidential". Accordingly, secure information exchange mechanisms needs to be put in place in the SSN ecosystem to handle this type of information;
- Regarding the "C.1.4 - Ports of refuge data" data group under "C.1 - Resources localisation for Maritime interventions", it is worth highlighting that this data is classified as "sensitive" or even "confidential" in certain Member States, so the handling of this information requires mechanisms for treating highly-secure information. Additionally, certain Member States have complex decision-support systems to determine what place of refuge a given vessel should be sent to depending on various variables that may include vessel type, cargo on board, meteo-oceanographic conditions, structural conditions of the vessel and availability and location of rescue and repair equipment. This means that the information of "ports of refuge" alone may not be sufficient or may be even misleading to support maritime interventions;

Regarding "C.5.19 - Interfacing with existing Community Information portals […]" – a data group classified as "not available in the SSN ecosystem" in the "Top 50%" ranked data groups – the remark is that this refers to a "system capability" and not to a "data set available in the system". This capability (of interfacing with other IT systems) is intrinsic to the SSN ecosystem as it provides wide-ranging system-to-system interfaces. This is demonstrated by the various operational services already provided to user communities using the capabilities of the ecosystem and in particular the IMDatE platform, where the SSN ecosystem was interconnected to a variety of other information systems.

4.3.5. CONCLUSIONS

In order to assess the capabilities of the SSN ecosystem to exchange information within CISE and with other user communities, a "comparative analysis" was performed using the data sets defined by TAG during "Step 2 of the CISE Roadmap" and described in *"CISE Architecture Visions"* and *"Mapping of Data Sets and Gap Analysis"* documents. These documents establish a set of 9 "Principles", 41 "Requirements" (derived from those "Principles" and other sources like EU legislation) and 500+ "Data Elements" of interest.

The conclusion of this analysis is that the SSN ecosystem data is a powerful system within the context of CISE supporting the exchanging data between different users/communities:

- In the "top 50%" (i.e. the highest ranked 50% of the 130 data groups used in the analysis – "top results"), 72% are available in the SSN ecosystem;
- In the "top 25%" (i.e. the highest ranked 25%), 88% are available in the SSN ecosystem;
- Of the 58 data groups out of 130 where data is available in the SSN ecosystem:
  - 35 are native to the SSN ecosystem;
  - 23 have origin in other user communities;

[46] *"Mapping of Data Sets and Gap Analysis"*, TAG, Step 2 of the CISE Roadmap - JRC Maritime Data Supply Demand

An analysis was also made to understand if - for the data that is not available in the SSN ecosystem in the "top 50%" data groups more likely to be shared (see "4.3.4 - Analysis of the results") - there are mechanisms in place to handle that exchange. The conclusion is that the technical mechanisms to handle the exchange of this data are available in the SSN ecosystem, apart the ones related to the handling of highly-secure information.

CHAPTER 5
POSSIBILITIES FOR THE DEVELOPMENT OF SAFESEANET ECOSYSTEM

5.1. ENVISIONED EVOLUTIONS FOR THE SAFESEANET ECOSYSTEM

In order to assess and evaluate the developments required of the SSN ecosystem to deliver benefits to the other maritime-related user communities, this report starts by identifying the envisioned evolutions[47] of the SafeSeaNet ecosystem, at two different levels:

- New/improved/potential services;
- New/improved/potential functionalities and technical capabilities in existing services[48].

Please note that these "envisioned evolutions" include intended changes to the SSN ecosystem that may or may not materialize in the future due to unforeseen circumstances or changes in EMSA's mandate. Namely, the remarkable technological advancement in the area of software engineering, computers and related devices create unforeseen situations, needs and opportunities that may lead to new services, functionalities and technical capabilities in the SSN ecosystem that are not listed in the following sections.

5.1.1. NEW/IMPROVED/POTENTIAL SERVICES

The provision of the following new/improved/potential services is envisioned for the near future in the SSN ecosystem:

- **Implementation of Copernicus Maritime Surveillance Services**: According to the "Proposal for a Regulation of the European Parliament and of the Council establishing the Copernicus Programme and repealing Regulation (EU) No 911/2010" ([RD.33]), EMSA will develop through the CleanSeaNet Data Centre and the IMDatE platform additional Maritime Surveillance capabilities based on Copernicus services and data that will support the work of other European Agencies and Maritime User Communities.
- **Upgraded service to support FRONTEX activities**: an upgraded service is being developed to provide data and information to support FRONTEX activities, namely to increase the probability and reliability of early detection of ships and boats used for illegal purposes.
- **Upgraded service for the support of the Fisheries user community**: the "fisheries monitoring service" will evolve in order to support the fisheries user community in complying with new EU fisheries regulations (for instance, through the integration of more fisheries controls specific information such as the catch information).
- **Upgraded Blue Belt service[49]**: as in the case of the "fisheries monitoring service", the Blue Belt service will be upgraded to provide further functionalities relevant to the involved user communities – Customs.
- **New Global SAT-AIS data coverage service**: Currently, the SSN ecosystem provides a Satellite AIS (SAT-AIS) data processing module able to process SAT-AIS information from different providers and then

[47] In the scope of this report, the SSN ecosystem "envisioned evolutions" include not only changes to the involved systems that are already *defined and planned* but also changes *intended but not yet planned*. It also includes policies that may lead to relevant changes and/or new functionalities/capabilities to be developed.

[48] In the scope of this report, a service is a general term that describes a coherent set of functionalities within a system. As an example, the Blue Belt is a service provided by the SSN ecosystem.

[49] Blue Belt service enhancements are dependent on a legal framework being agreed regarding implementation.

distribute the data either as an individual stream or as part of a ship integrated track. This module will be evolved in the upcoming years (2014 onwards) to provide a service covering the entire globe.

- Service to support the verification of the **International Convention for the Control and Management of Ships' Ballast Water and Sediments (BWM)**: work is under way to develop a service for the verification of the International Convention for the Control and Management of Ships' Ballast Water and Sediments (BWM).
- EU system for **monitoring, reporting and verifying (MRV) emissions (sulphur oxides – Sox - and nitrogen oxides – Nox) from large ships using EU ports**: work is under way to develop a service for the MRV of Sox/Nox emissions from large ships using EU ports.
- **The Torremolinos International Convention for the Safety of Fishing Vessels and the Cape Town Agreement of 2012** ([RD.10]): whilst no system or service is planned, it could be anticipated that EMSA could be assigned a role in the future monitoring of the Torremolinos International Convention for the Safety of Fishing Vessels and the Cape Town Agreement of 2012.
- **Monitoring, reporting and verifying (MRV) of International Labour Organization's recommendations related to fishing activities** ([RD.11]): whilst no system or service is planned it could be anticipated that EMSA could eventually be assigned a role in the future monitoring, reporting and verifying (MRV) of International Labour Organization's recommendations related to fishing activities.

5.1.2. NEW/IMPROVED/POTENTIAL FUNCTIONALITIES AND TECHNICAL CAPABILITIES

The following new/improved/potential functionalities and technical capabilities are envisioned for the near future in the SSN ecosystem:

- **Exchange of FAL forms information through SSN**: According to the Directive 2010/65/EU, Member States shall accept the fulfilment of reporting formalities in electronic format, and their transmission via a single window. The Directive requires Member States to ensure that information received in accordance with the reporting formalities required by a legal act of the Union is made available to other Member States via SSN. Accordingly, SSN will be upgraded to support the exchange of such information.
- Development of **common information repositories** to support internal and external end users, such as a LOCODE and AUTHORITIES registries and an Enhanced Ship Database.
- **New capabilities to support Search and Rescue**: new capabilities are being created in the IMDatE platform in order to cater for specific "Search and Rescue" functionalities, namely the retrieval of the last position of the vessel in distress plus the polling of different data sources to determine closest vessels to the vessel in distress.
- **Ingestion, processing and display of new data and information**. New functionalities are being developed in the SSN ecosystem to allow the ingestion, processing and display of information related to vessels, ports or areas of interest:
  - New AIS data messages (e.g. Aids to Navigation, AIS-SART, application specific messages for the display of meteorological and hydrographic data);
  - New information types (e.g. recorded and live video streams, aerial assets tracking information, satellite imagery reports – reports from service providers with intelligence collected from satellite imagery);
  - New information sources (from unmanned/remote piloted vehicles/aerial/patrol assets);
  - A geoportal[50] will be developed in the SSN ecosystem in order to provide the means to search and view (subject to access restrictions) for spatial data sets and spatial data services available in the ecosystem.
  - New capabilities are planned to be developed in the SSN ecosystem in order to cater for the distribution of alerts through GeoRSS[51] (currently CAP – Common Alerting Protocol – is supported).

[50] A geoportal is a type of web portal used to find and access geographic information and associated geographic services via the Internet.

[51] In simple terms, GeoRSS is a way of geo-enabling, or tagging, "really simple syndication" (RSS) feeds with location information. Using GeoRSS, it is possible to search for web content based on geographic locations. In addition, GeoRSS facilitates the dissemination of RSS feeds to specific users based on event type and location.

- **Integration of Oil Spill Drift Models**: Oil spill drift models constitute an essential element in contingency planning and in preparing effective response strategies to combat oil spills at sea. Such models rely on the ability to predict meteo-marine conditions of the sea through the use of atmospheric, wave and hydro-dynamical numerical models. In combination with information on the location, rate, nature and characteristics of an oil spill, the derived forecasted fields are used to provide information on the fate and track that the oil slick will follow in time.
- **Processing and display of meteo, hydrographic and oceanographic data from satellite and in-situ buoys**: CleanSeaNet, as the Earth Observation backbone for EMSA maritime applications, will be further developed to receive, process and integrate meteo, hydrographic and oceanographic data. These data could be directly procured by EMSA, but could also stem from international organisations, Member States, industry and R&D products. Besides being valuable information *by itself*, this information is also an important input of oil spill drift models.
- **Processing and display of new high resolution radar (SAR) and optical satellite-based imagery and data:** New satellite imagery (both radar – SAR - and optical systems) made available by new satellite payloads capable of mapping the Earth with high resolution and wide area coverage will be incorporated in the CleanSeaNet Data Centre in order to improve VDS capabilities and to detect "marine-based illegal/suspicious/unlawful activity" – e.g. transhipments, piracy.
- **Creation of data ontology and semantic web services**: The development of a data ontology – a formal representation of knowledge as a set of concepts within a domain, using a shared vocabulary to denote the types, properties and interrelationships of those concepts – and semantic web services - services built around standards for the interchange of semantic data/data ontologies which makes it easy for systems to combine data from different sources and services without losing meaning - is planned for the SSN ecosystem.
- **Development of "Mobile Applications for accessing the services provided by the SSN ecosystem" for laptops/smartphones/tablets**: The access to functionalities of the SSN ecosystem through laptops/smartphones/tablets will be developed in the future. This will be achieved through either responsive graphical web applications or tailor-made mobile applications.

5.2. "TECHNICAL ANALYSIS"

In order to rank the different possibilities for the development of the SSN ecosystem to support CISE, two multi-criteria analyses were performed on the different aspects of the required changes:

- Changes required by CISE Principles and Requirements not currently fulfilled or fulfilled partially by the SSN ecosystem;
- Envisioned evolutions for the SSN ecosystem at service, functionality and technical levels.

These analyses resulted in the following recommendation of changes to the SSN ecosystem:

- The more pertinent upgraded/new/potential services in the SSN ecosystem level in light of the interest for CISE and the sharing of information with other user communities are:
  - *New Global SAT-AIS data coverage service*
  - *Upgraded Blue Belt service*[52]
  - *Implementation of Copernicus Maritime Surveillance Services*
  - *Upgraded service for the support of the Fisheries user community*
  - *Upgraded service to support FRONTEX activities*
- The more pertinent upgraded/new/potential functionalities and technical capabilities in the SSN ecosystem level in light of the interest for CISE and the sharing of information with other user communities are:
  - *Ingestion, processing and display of new data and information*

[52] The Blue Belt service enhancements are depended on a legal framework being agreed regarding implementation.

- *Processing and display of new high resolution radar (SAR) and optical satellite-based imagery and data*
- *Common Information Repositories*
- *Creation of data ontology and semantic web services*
- *Exchange of FAL forms information through SSN*

- The more pertinent changes in order to address the SSN ecosystem shortcomings at the CISE Principles and Requirements level are the ones related with:
  - *Discovery of Available Information*
  - *Discovery of Available Services*
  - *Integrity of Information Exchanges*
  - *Use of commonly agreed information classification scheme*
  - *Confidence Value for Exchanged Information*
  - *Priority Level for urgency of requested information.*

The following sections present the detailed multi-criteria analysis performed on "envisioned evolutions of the SSN ecosystem" and on the changes required by CISE Principles and Requirements not currently fulfilled or fulfilled partially by the SSN ecosystem.

5.2.1. CISE PRINCIPLES AND REQUIREMENTS

The following table presents the result of the multi-criteria analysis performed on the changes required by CISE Principles and Requirements not currently fulfilled or fulfilled partially by the SSN ecosystem. The "Top Results" (results above the median[53]) are highlighted with a light red background in the column "Rank"[54]. The presented "scoring" was calculated using the weighted sum method.

Table 5-1: Scoring for CISE Principles and Requirements" necessary changes

Description	Origin of Capability	Changes to Data Sets	Impact Data Access/Security Policies	Impact Capacity	Impact Administration / Operation	Impact Governance	Impact Legal Framework	Required system changes	Scoring	Rank
Handling of Highly-Secure Information	CISE Principle	Medium	High	Medium	Medium	Yes	Yes	High	11,25	8
Discovery of Available Information	CISE Requirement	Low	Low	Low	Low	No	No	Medium	55,00	1
Discovery of Available Services	CISE Requirement	Low	Low	Low	Low	No	No	Medium	55,00	1
Confidence Value for Exchanged Information	CISE Requirement	High	None	Low	Low	No	No	High	50,00	4
Priority Level for urgency of requested information	CISE Requirement	High	None	Low	Low	No	No	High	50,00	4
Use of commonly agreed information classification scheme	CISE Requirement	High	Low	None	Low	No	No	High	50,00	4
Integrity of Information Exchanges	CISE Requirement	Low	Medium	Low	Low	No	No	Medium	51,25	3
Secure Audio/Video/Instant Messaging/White-Boarding	CISE Requirement	Low	High	Medium	Low	No	No	Low	48,75	7

[53] The median is the middle value of a set of numbers when the numbers are arranged in either ascending or descending order.

[54] Please note that due to the fact that the sample is small and that several items have the same score, the number of "Top Results" is not sometimes equal to 50% of the number of items in the sample.

5.2.2. SSN ECOSYSTEM "ENVISIONED EVOLUTIONS"

5.2.2.1. Services Level

The following table presents the multi-criteria analysis performed on the SSN ecosystem "planned evolutions" at Services level in light of the interest for CISE and the sharing of information with other user communities.

Table 5-2: Scoring for "SSN ecosystem envisioned evolutions": Services level

Description	UCs involved	Changes to Data Sets	Impact Access / Security	Impact Capacity	Impact Administration / Operation	Impact Governance	Impact Legal Framework	Required system changes	Significance for CISE and other UCs	Scoring	Rank
Implementation of Copernicus Maritime Surveillance Services	All User Communities	Medium	Low	Medium	Medium	No	Yes	High	High	47,50	3
Upgraded service to support FRONTEX activities	Border Control	Medium	Medium	Low	Low	No	Yes	Medium	High	46,50	4
Upgraded service for the support of the Fisheries user community	Fisheries Control	Medium	Low	Medium	Low	No	Yes	Medium	High	46,50	4
Upgraded Blue Belt service	Customs	Low	Low	Low	Low	No	Yes	Low	High	56,50	2
New Global SAT-AIS data coverage service	All User Communities	Low	Low	Medium	Low	No	No	Low	High	67,50	1
Support to the International Convention for the Control and Management of Ships' Ballast Water and Sediments (BWM)	Marine Environment	High	Medium	High	Medium	No	Yes	High	Low	16,50	6
EU system for monitoring, reporting and verifying (MRV) emissions (sulphur, CO2 and NOC) from large ships using EU ports.	Marine Environment	High	Medium	High	Medium	No	Yes	High	Low	16,50	6
Torremolinos International Convention for the Safety of Fishing Vessels and the Cape Town Agreement	Fisheries Control	High	Medium	High	Medium	No	Yes	High	Low	16,50	6
Monitoring, reporting and verifying (MRV) of International Labour Organization's recommendations related to fishing activities	Fisheries Control	High	Medium	High	Medium	No	Yes	High	Low	16,50	6

5.2.2.2. Functionalities and Technical Capabilities Levels

The following table presents the multi-criteria analysis performed on the SSN ecosystem "planned evolutions" at Functionalities and Technical Capabilities levels in light of the interest for CISE and the sharing of information with other user communities.

Table 5-3: Scoring for "SSN ecosystem envisioned evolutions": Functionalities + Technical Capabilities levels

Description	UCs involved	Changes to Data Sets	Impact Access / Security	Impact Capacity	Impact Administration / Operation	Impact Governance	Impact Legal Framework	Required system changes	Significance for CISE and other UCs	Scoring	Rank
Exchange of FAL forms information through SSN	All User Communities	Low	Low	Medium	Medium	No	Yes	Medium	High	55,00	4
Common Information Repositories	Maritime Safety and Security	Low	None	None	Low	No	No	Low	Low	56,50	3
New capabilities to support Search and Rescue	Maritime Safety and Security	Low	Low	Low	Low	No	No	Low	Low	46,50	8
Processing and display of meteo, hydrographic and oceanographic data from satellite and in-situ buoys	Maritime Safety Security and Marine Environment	Low	Low	Low	Low	No	No	Low	Low	48,00	7
Ingestion, processing and display of new data and information	All User Communities	Medium	Medium	Medium	Low	No	No	Medium	High	57,50	1
Integration of Oil Spill Drift Models	Maritime Safety Security and Marine Environment	Medium	Low	Medium	Low	No	No	Medium	Low	38,00	9
Processing and display of new high resolution radar (SAR) and optical satellite-based imagery and data	All User Communities	Low	Low	Medium	Low	No	No	Low	Medium	57,50	1
Creation of data ontology and semantic web services	All User Communities	Medium	Low	Low	Medium	No	No	High	High	55,00	4
Development of "Mobile Applications for accessing the services provided by SSN ecosystem" for laptops/smartphones/tablets	All User Communities	Low	Medium	Low	Low	No	No	Low	Low	52,50	6

5.2.3. CONCLUSIONS AND RECOMMENDATIONS

The analysis performed in the study identified that the more significant SSN ecosystem evolutions required to address the CISE Principles and Requirements are the ones related with:

- *Discovery of available information*
- *Discovery of available services*
- *Integrity of Information exchanges*
- *Use of commonly agreed information classification scheme*
- *Confidence value for exchanged Information*
- *Priority level for urgency of requested information*

In the context of sharing information between different user communities and different information systems, it is easily understandable that the *integrity of the information exchanges* and the *use of a commonly agreed information classification scheme* are of uttermost importance for assuring that the information received by the consumer is exactly the same as the one sent by the provider.

But in order to find which information or services are available in any given system, a mechanism is required for discovering them: this can be provided through a services catalogue and data ontology that allows a common understanding of the available data and where their *meaning* become relevant (web semantics).

Finally the implementation of a *confidence value* and a *priority level* for the requested/exchanged information – albeit relevant – will require extensive changes in the data sets currently available in the SSN ecosystem as such levels needs to be computed and added to the available (computer) system interfaces.

It is also important to note that the "Handling of Highly-Secure Information" does not appear in the list of the more pertinent changes to be made in the SSN ecosystem. This is caused by the impacts on the access and security mechanisms, legal framework and overall required changes that need to be put in place in order to address the handling of such type of information, namely:

- Implement a secure information exchange protocol (e.g. "Two-way SSL", "HTTPS over TLS") for all the system-to-system interfaces that handle sensitive and highly-secure information; and
- Provide Electronic Digital Rights Management mechanisms, if the need is to control properly not only the system-to-system interfaces but also enforcing access and usage rights on the sensitive information throughout its lifecycle.

Having analysed the way do address the shortcomings of SSN ecosystem with respect to CISE Principles and Requirements it is then important to prioritize – from a CISE and sharing information with user communities perspective – the developments envisioned to the ecosystem. Considering that Blue Belt service enhancements are dependent on a legal framework being agreed regarding implementation, this analysis has held that the more pertinent evolutions are the ones related with:

- New services provided by the SSN ecosystem to user communities (including the Maritime Safety one):
  - *New Global SAT-AIS data coverage service*
  - *Implementation of Copernicus Maritime Surveillance Services*
  - *Upgraded service for the support of the Fisheries user community*
  - *Upgraded service to support FRONTEX activities*
- New functionalities and technical capabilities in the existing SSN ecosystem services:
  - *Ingestion, processing and display of new data and information*

- *Processing and display of new high resolution radar (SAR) and optical satellite-based imagery and data*
- *Common Information Repositories*
- *Creation of data ontology and semantic web services*
- *Exchange of FAL forms information through SSN*

Although it is clear why the above envisioned evolutions are pertinent for CISE and the sharing of information with other user communities, it is worth analysing why some proposed evolutions do not score high enough to appear on the list:

- *New capabilities to support Search and Rescue*, *Processing and display of meteo, hydrographic and oceanographic data from satellite and in-situ buoys* and *Integration of Oil Spill Drift Models*: these capabilities score relatively low in our analysis mainly due to the fact that it is of interest to a specific user community – *Maritime Safety and Security (in the case of New capabilities to support Search and Rescue*) or – in the other two cases - to only two user communities - *Maritime Safety and Security* and *Marine Environment*;
- The envisioned evolutions related with *"EU system for monitoring, reporting and verifying (MRV) emissions (sulphur oxides – Sox - and nitrogen oxides – Nox) from large ships using EU ports" and "Support to the International Convention for the Control and Management of Ships' Ballast Water and Sediments (BWM)"* although already under way have a low score mainly because the changes that need to be put in place in the SSN ecosystem;
- Regarding the *"Support to the Torremolinos International Convention for the Safety of Fishing Vessels and the Cape Town Agreement"* and *"Support to the verification of International Labour Organization recommendations related to fishing activities"*, they score low in the analysis mainly because that they are still being discussed in the proper governance forums and as such the impacts and the requirements to support those new "services" are still unknown.

The importance for CISE and the sharing of information with other user communities of *Ingestion, processing and display of new data and information*, *Processing and display of new high resolution radar (SAR) and optical satellite-based imagery and data*, *Common Information Repositories* and *Exchange of FAL forms information through SSN* is straightforward:

- *New data elements* (new AIS data messages), *improved data* (high resolution SAR and optical imagery), *new information* (reports from service providers with intelligence collected from satellite imagery), and *new data types* (recorded and live video streams, aerial assets streaming/tracking information) will always be translated in more opportunities to exchange data and support the needs of CISE and other user communities;
- The *Exchange of FAL forms information through SSN* and *Common Information Repositories* are pertinent because they implement one of the key goals of CISE – the sharing and the re-use of existing information within a user community and between different user communities.

The *Creation of data ontology and semantic web services* is significant for CISE because it is the state-of-the-art technical solution to support the *Discovery of available information* and the *Discovery of available services* requirements. Semantic web services are built around standards for the interchange of semantic data – *data ontologies*[55] – which makes it easy for systems to combine data from different sources and services without losing meaning. Ontologies (and Linked Data) are the means to avoid the misinterpretation of terms by formally describing a conceptualization. Ontologies explicitly describe terms using logical expressions and guarantee that the information in any instance of communication is consistently interpreted by both involved parties and therefore facilitate semantic integration of data and information.

[55] In computer science and information science, ontology formally represents knowledge as a set of concepts within a domain, using a shared vocabulary to denote the types, properties and interrelationships of those concepts.

CHAPTER 6
CONCLUSIONS

The purpose of the current study – "*Study to assess the future evolution of SafeSeaNet to support CISE and other communities*" - as defined in the Terms of Reference (ToR) and in accordance with the Action 3.1 of the IMP Work Programme, is to assess and evaluate the potential of the Union maritime information and exchange system, SSN, to support a CISE, and to demonstrate how SSN can serve as a platform which could be of benefit to various other end- users (communities).The study aims to assess and evaluate the potentialities of EMSA's systems and to support the overall objectives of the integrated maritime surveillance initiative, especially CISE.

The SafeSeaNet ecosystem - which in the context of this study comprises all EMSA hosted maritime information systems[56] including SafeSeaNet central system, EU LRIT Cooperative Data Centre, CleanSeaNet and, THETIS in the IMDatE platform - is the European Union (EU) "ecosystem of systems" for the exchange and sharing of information between designated authorities and in electronic format, of ship positional data (AIS, Satellite AIS, LRIT, coastal radar, VMS, ship-borne AIS, VDS), ship particulars, logistic and voyage related information, the detection of potential oil spills and involved polluters and to facilitate the planning of ship inspections. The objective of the SafeSeaNet ecosystem is thus to support EU and Member States activities for the purpose of maritime safety, port and maritime security, marine environment protection and the efficiency of maritime traffic and maritime transport.

This report was created based on an exhaustive review of documentation, including CISE roadmap documents, SSN High Level Steering Group (HLSG) and CISE Technical Advisory Group (TAG) progress of activities, legal records and pilot case results. This process was conducted in conjunction with a number of EMSA staff members involved in the different pilot projects and CISE Technical Advisory Group activities. Progress was also regularly reported to the SSN High Level Steering Group as well as to the EMSA Administrative Board. In addition a review of relevant *acquis*, as it is the case for *Reporting Facilities Directive* and *Vessel Traffic Monitoring Information System (VTMIS)* was performed.

A comparative analysis supported in a Multi-criteria Analysis (MCA) to classify and weight CISE datasets was performed and the results were discussed and validated with representatives from each of the seven CISE User Communities. For that purpose the CISE 500+ data elements have been grouped and treated at an upper level – comprised of 130 data groups - while fully preserving the integrity of CISE mapping. The objective of this analysis was to identify the data groups more likely to be shared in the scope of CISE.

Data groups more likely to be shared (i.e. top results, corresponding to the up 50% of the 130 data groups) for all UCs, independently on scenario considered, include:

- "Ship position" data;
- "Ship pollution" data;
- "Resources localization for maritime interventions";
- "Maritime infrastructures" data; and
- "Legal maps" data.

After the identification of the data groups more likely to be shared, the next steps of analysis comprised:

- An assessment whether significant data groups are already covered/provided by SSN ecosystem or through its Maritime Services;

[56] Developed in full cooperation with all EU Member States to ensure the implementation of Union legislation.

- Same evaluation but excluding from the analysis the data groups that are already owned by each of the CISE User Communities.

The overarching conclusion of the assessments described above is that the SSN ecosystem has the technical capabilities to exchange data with other user communities. More specifically:

- In the "top 50%" (i.e. the highest ranked 50% of the 130 data groups used in the analysis – "top results"), 72% are available in or through the SSN ecosystem;
- In the "top 25%" (i.e. the highest ranked 25%), 88% are available and/or exchanged in the SSN ecosystem;
- Of the 58 data groups out of 130 where data is available in the SSN ecosystem:
  - 35 are native to the SSN ecosystem;
  - 23 have origin in other user communities;

In order to prioritise the different possibilities for the development of the SSN ecosystem to support CISE and further strengthen the exchange of information with other user communities, another multi-criteria analysis was performed on the different aspects of the required changes:

- Changes required by CISE Principles and Requirements not currently fulfilled or fulfilled partially by the SSN ecosystem;
- Envisioned evolutions for the SSN ecosystem at Services, Functionalities and Technical levels.

The conclusions of the analysis on the fulfilment of the CISE Principles and Requirements by the SSN ecosystem are that:

- EMSA's SSN ecosystem has the technical capabilities to fulfil 8 (out of 9) CISE's Principles. The only exception is related to the handling of "highly secure" data, a feature which is not required within EMSA's SSN ecosystem mandate (all systems being "unclassified systems" according to the Commission Decision 2001/844/EC of 29 November 2001);
- Regarding CISE Requirements, the SSN ecosystem fulfils 29 (out of 41), partly fulfils 7 and doesn't fulfil 5. The requirements which are not fulfilled (partially or completely) are:
  - Partial fulfilment:
    - *SI9 CISE must rely on a common data model for information exchanges which is as language-neutral as possible;*
    - *DI3 CISE must allow looking up what information CISE participants can provide and how they can provide that information;*
    - *DI4 CISE must allow information providers making available how their services can be used, including parameters such as the refresh rate;*
    - *IA1 CISE information exchanges must include a confidence value and must indicate who provided it. The confidence value must be a commonly agreed coded value;*
    - *IA2 CISE information requests must include a priority level reflecting the urgency of the request. The priority level must be a commonly agreed coded value;*
    - *IS5 CISE information exchanges must respect a commonly agreed information classification scheme supporting security levels from up to EU secret;*
    - *IS7 CISE must use a messaging protocol that ensures a minimum level of integrity of information exchanges between consumer and provider. The messaging protocol must also ensure higher levels of integrity depending on the classification level of the information.*

- No fulfilment*;*
  - *DI1 Member States and User Communities must provide one or more points of access that facilitate standardised discovery of the services they provide to CISE participants;*
  - *CO3 CISE must support secure audio communication;*
  - *CO4 CISE must support secure video communication;*
  - *CO5 CISE must support secure instant messaging;*
  - *CO6 CISE must support secure white-boarding.*

The analysis performed – through another Multi-criteria Analysis – in the study identified that the more significant SSN ecosystem evolutions required to address the CISE Principles and Requirements are the ones related with:

- *Discovery of available information*
- *Discovery of available services*
- *Integrity of Information exchanges*
- *Use of commonly agreed information classification scheme*
- *Confidence value for exchanged Information*
- *Priority level for urgency of requested information*

Having analysed the way to address the weaknesses of SSN ecosystem with respect to CISE Principles and Requirements, the final step of the study was to prioritize the changes and required evolutions of the SSN ecosystem. This analysis shows that the more pertinent developments are the ones related with:

- **New services** provided by the SSN ecosystem to user communities (including the Maritime Safety one): a Global SAT-AIS data coverage service, the implementation of Copernicus Maritime Surveillance Services, an upgraded service for the support of the Fisheries user community, and an upgraded service to support to FRONTEX activities;
- **New functionalities** in the SSN ecosystem services, namely the ingestion and processing of new data (e.g. High Resolution Radar and Optical satellite-based sensors for VDS and to detect "marine-based illegal/suspicious/unlawful activity"), new information (e.g. AtoN, AIS-SART, recorded and live video streams, aerial assets tracking information), the exchange of (some) FAL forms through SSN, new LOCODE and AUTHORITIES registries, and an Enhanced Ship Database;
- **Technical evolutions** that improve the sharing of information: namely, the development of "Mobile Applications for accessing the services provided by SSN ecosystem" for smartphones/tablets.

In summary, the comprehensive work performed in this study has shown that the SSN ecosystem:

- Is established and operational 24 x 7 x 365 and accessible by all EU Member States and all relevant EU/ bodies/organisations;
- Supports and feeds information exchange by/between all maritime user communities through operational services built up over time. These services are:
  - Adapted to the specific needs of each user community;
  - Standards-based;
  - With appropriate security and access management policies;
- Is largely aligned with CISE:

  - Fulfils 8 out 9 CISE Principles;
  - Fulfils 29 (out of 41) CISE Requirements, partly fulfils 7 and does not fulfil 5;
  - Around 72% of the CISE "data groups more likely to be shared" are already available in or through the SSN ecosystem;
- Possesses the technical capabilities and the flexibility to evolve in accordance with the needs of different user communities.
- At the same time the study, considering data owned by the user communities, clearly shows that the two user communities having most 'own' data are maritime safety and defence. Hence there is a gap identified in how the (relevant) information, in particular held by the defence, could be exchanged/shared with the other (civilian) communities.

CHAPTER 7
ANNEX I – EMSA IT LANDSCAPE

EMSA has available a comprehensive and state-of-the-art IT landscape supporting the SSN ecosystem.

The **basic applications** and **tools** used and available are:

- *Application Server*:
  - Oracle WebLogic 10.3.6
  - Apache Tomcat
  - JBoss
- *Database Management Server*:
  - Oracle Enterprise 11g
  - MySQL
- *ESB and SOA*:
  - Oracle SOA Suite 11g (includes OSB 11.1)
- *Operating Systems*:
  - RedHat Enterprise Desktop Linux 5 and 6
  - RedHat Enterprise Server Linux 5 and 6 (32 and 64 bits)
  - Windows Server 2008
  - Windows 7 for desktop computers
- *Virtualisation*:
  - VMWare ESXI VSphere 5
  - VMWare HA, DRS and Failover
- *GIS*:
  - ESRI ArcGIS 10
  - Jeppesen C-Map
  - GeoServer
- *Portals*:
  - Liferay Portal Enterprise Edition 5.2 and 6.1
- *Reporting, Business Intelligence and Data Warehouse*:
  - Business Objects Enterprise XI R2
  - Jasper Reports
  - Jasper BI
- *User Registries and Management*:
  - OpenLDAP 2.4
  - Oracle Access Manager 10gR3
  - Oracle Identity Management 10gR3
  - Oracle Internet Directory 11g
  - Oracle Virtual Directory 11g

The **business continuity** and **security tools** include:

- *Business continuity*:
  - VMWare HA and Failover
  - VMWare Sire Recovery Manager
  - Asynchronous data replication through Storage Array
- *Network Security*:
  - Checkpoint R75.40
- *Proxy*:
  - F5 Big IP 3600 10.2.0
- *System/Application Monitoring*:
  - Nagios
  - HP BAC SAM 9.50 with SiteScope

- *Clustering*:
  - Front-End: Oracle WebLogic 10.3.6 Active/Active
  - Back-End: Oracle RAC 11.2.0.3

The **physical components** of the SSN ecosystem include:

- *Data Links*:
  - 2 Internet circuits, each link with a 100 Mbps capacity
  - 1 sTESTA link with 2 Mbps capacity
  - 1 GEANT link with 1 Gbps
- *Hardware Servers*:
  - HP Blade and DL Series servers
- *Storage*:
  - Brocade fabric based on Sanswitch DS5300
  - EMC Clarion CX 4-240
  - NetApp FAS3240

Other technologies used are:

- *Client Tier*:
  - JavaScript
  - JQuery
  - WebGL
  - HTML 5
  - Ajax
- *Web Tier Technologies:*
  - JSP – Java Server Pages
  - JSF – Java Server Faces
  - Portlets
- *Rich Internet Application (RIA) frameworks*:
  - ExtJS
  - WebGL
  - Dojo UI
  - AdobeAir
  - AdobeFlash
  - AdobeFlex
- *Client-Server connection technologies*:
  - HTTP or HTTPS
  - Web Services
  - RMI
- *External systems integration technologies*:
  - Web Services
  - sFTP/FTP
- *Web Services technologies:*
  - AXIS 2
  - Spring Web Services
  - UDDI
- *Business Layer technologies*:
  - POJO (Plain Old Java Objects)
  - Session EJBs
  - Message Driven EJBs
- *Data Access Layer technologies:*
  - Hibernate
  - iBatis
  - Zorba XQuery
- *Spatial Data Infrastructure:*
  - Deegree 2.3
  - Oracle Locator

CHAPTER 8
ANNEX II – MULTI-CRITERIA ANALYSIS SCORINGS

8.1. COMPARATIVE ANALYSIS WITH CISE DATA SETS

The scoring for the variables used in the "Comparative Analysis with CISE data sets" multi-criteria analysis is presented in the following table:

Table 8-1: "Comparative Analysis with CISE data sets" weighted scores

			Weighted Scenario	Baseline Scenario
Critical Variable	**Parameters**	**Score**	**Weighted score**	**Weighted score**
Current level of security classification	Not sensitive	4	**15,00**	14,29
	Commercial Sensitive	3	11,25	10,71
	Personnel data protection	2	7,50	7,14
	Security sensitive	1	3,75	3,57
Legal obligation to collect	EU Law	4	**15,00**	14,29
	International Conventions	3	11,25	10,71
	Other type of obligation	2	7,50	7,14
	No obligation	1	3,75	3,57
Data availability in existing information systems	Available in UC, associated systems and actively shared with other UC	4	**15,00**	14,29
	Available in UC and associated systems but not shared with other UC	3	11,25	10,71
	Available in UC but not in associated systems	2	7,50	7,14
	Not available	1	3,75	3,57
Data distribution spatial coverage	Global	5	**5,00**	14,29
	EU	4	4,00	11,43
	Regional	3	3,00	8,57
	National	2	2,00	5,71
	Local	1	1,00	2,86
Operational use of data group	Routine monitoring	4	**20,00**	14,29
	Periodic Monitoring (campaigns)	3	15,00	10,71
	Ad hoc (accidents / incidents)	2	10,00	7,14
	Support contingency planning (preparedness)	1	5,00	3,57
Data needed to fulfil operational tasks	Yes	2	**20,00**	14,29
	No	1	10,00	7,14
Cost of gathering data	Own sourced data: Free	3	**10,00**	14,29
	Sourced data: Free by agreement with data	2	6,67	9,52
	Sourced data: Licensed with payments	1	3,33	4,76

8.2. TECHNICAL ANALYSIS

The scoring for the variables used in both "Technical Analysis" MCA is presented in the following sections.

8.2.1.1. User Communities involved

The "User Communities involved" variable had the following values and scores:

Table 8-2: Values and Score – "User Communities involved"

Name	Score (%)
All User Communities	100
Border Control	15
Customs	15
Defence	15
Marine Environment	15
Fisheries Control	15
Law Enforcement	15
Maritime Safety and Security	15
Maritime Safety & Security and Marine Environment	30

8.2.1.2. Changes to Data Sets

The "Changes to Data Sets" variable had the following values and scores:

Table 8-3: Values and Score – "Changes to Data Sets"

Value	Score (%)
High	0
Low	50
Medium	25
None	100

8.2.1.3. Impact Access/Security

The "Impact Access/Security" variable had the following values and scores:

Table 8-4: Values and Score – "Impact Access/Security"

Value	Score (%)
High	0
Low	50
Medium	25
None	100

8.2.1.4. Impact Capacity

The "Impact Capacity" variable had the following values and scores:

Table 8-5: Values and Score – "Impact Capacity"

Value	Score (%)
High	0
Low	50
Medium	25
None	100

8.2.1.5. Impact Administration/Operation

The "Impact Administration/Operation" variable had the following values and scores:

Table 8-6: Values and Score – "Impact Administration/Operation"

Value	Score (%)
High	0
Low	50
Medium	25
None	100

8.2.1.6. Impact Governance

The "Impact Governance" variable had the following values and scores:

Table 8-7: Values and Score – "Impact Governance"

Value	Score (%)
High	0
Low	50
Medium	25

Value	Score (%)
None	100

8.2.1.7. Impact Legal Framework

The "Impact Legal Framework" variable had the following values and scores:

Table 8-8: Values and Score – "Impact Legal Framework"

Value	Score (%)
High	0
Low	50
Medium	25
None	100

8.2.1.8. Required system changes

The "Required system changes" variable had the following values and scores:

Table 8-9: Values and Score – "Required system changes"

Value	Score (%)
High	0
Low	50
Medium	25
None	100

8.2.1.9. Significance for CISE and other User Communities

The "Significance for CISE and other User Communities" variable had the following values and scores:

Table 8-10: Values and Score – "Significance for CISE and other User Communities"

Value	Score (%)
High	100
Low	25
Medium	50
None	0

ANNEX III – BIBLIOGRAPHY

9.1. Glossary of terms

Table 9-1: Glossary of systems

Expression	Definition
Access Control	The process that ensures that resources are only granted to those users who have a need for the information and own the proper access rights.
Access Rights	The set of privileges granted to a user allowing them to have access to certain kinds of information or services.
Application	Software designed to perform specific tasks and that exposes certain functionalities through interfaces.
Architecture	In the context of software engineering, the structure of application components, their inter-relationships and the principles and guidelines governing their design and evolution over time.
Authentication	The process of determining whether someone or something is who or what it is declared to be.
Authorisation	The process of granting access rights to a user.
Authority (or public authority)	Any organisation that has an interest in maritime surveillance information. An authority can be local, regional, national or European level.
Baltice.org	Baltice.org is a single access point to reliable and up to date information related to winter navigation in the Baltic Sea area. This site gathers information and instructions from icebreaking authorities from all the Baltic Sea countries (Denmark, Estonia, Finland, Germany, Latvia, Lithuania, Norway, Poland, Russia and Sweden). Information is available free of charge and meant for users of winter navigation information at the Baltic Sea. Daily updated ice chart of the whole Baltic Sea area is available in PDF format. Ice chart data is also viewable in Ice Map -window, where it is possible to move, zoom in and out, and measure distances and directions on the ice map. The data is viewable in different WMO styles. The website is commissioned and financed by Baltic Icebreaking Management (BIM), which has members from all Baltic Sea countries, and co-financed by the European Commission through the programme for trans-European transport network.
Bespoke system	A system that was developed specifically for the setting where it is used. The system may have been built from standard components but the applications running on it have been developed specifically.
Blue Belt	The Blue Belt Pilot Project provides ship notification reports to customs authorities of all EU Member States, with the aim of supporting customs by providing verified information about the voyages of vessels engaged in intra-EU trade. The notification reports are generated automatically by a specific module of SafeSeaNet, and delivered to the relevant customs authority two hours before a ship´s estimated arrival. The pilot project monitored 253 vessels (the "Blue Ships"), identified by the European Community Ship-owners Association (ECSA) and the World Shipping Council (WSC), which participated in the pilot project on a voluntary basis. A cross-section of vessels was chosen to be representative of the different trades most frequently seen in the European Union such as pure intra-EU movements (under the authorized regular shipping service regime - RSS - or not), feeder or main haul liner shipping vessels and bulk carriers. The pilot project took place between May 2, 2011 and November 3, 2011 and at the request of the Member States, the Blue Belt services are still provided to customs authorities.

Expression	Definition
CECIS-ProCivNet (Civil Protection and Environmental Emergencies European Network)	CECIS-ProCivNet (Civil Protection and Environmental Emergencies European Network) interconnects the Monitoring and Information Centre (MIC) of the EC Directorate General for Environment with National Authorities with responsibility to protect citizens from natural and technological hazards. It constitutes the Common Emergency Communication and Information System (CECIS) provided in the context of the Council Decision of 23 October 2001. It addresses major emergencies, i.e. natural, technological, radiological or environmental accidents occurring inside or outside the Community, including accidental or deliberate marine pollution.
CISE	The "Common Information Sharing Environment" (CISE) is "a voluntary collaborative process in the European Union seeking to further enhance and promote relevant information sharing between authorities involved in maritime surveillance. It is not replacing or duplicating but building on existing information exchange and sharing systems and platforms. Its ultimate aim is to increase the efficiency, quality, responsiveness and coordination of surveillance operations in the European maritime domain and to promote innovation, for the prosperity and security of the EU and its citizens".
CleanSeaNet (CSN)	CleanSeaNet (CSN) is a European, satellite-based oil spill and vessel detection service. It offers assistance to participating States for the identification and tracking of oil pollution on the sea´s surface, monitoring accidental pollution during emergencies and contributing to the identification of polluters. The images captured by Synthetic Aperture Radars´ (SAR) on-board satellites are transmitted to the nearest ground station, where they are processed and interpreted by designated service providers and then sent to CleanSeaNet. If an oil spill is detected, alert information will be sent by CleanSeaNet to the pollution control authorities of Member States. On top of oil spill alerts, CleanSeaNet also provides slick position and shape as well as wind and wave data. Member States can access the application via the web-based portal or via a system-to-system interface using web services. Vessels appearing in satellite images can be identified by correlating the satellite data with AIS data from SafeSeaNet. CleanSeaNet is a central system with an EU level database.
Coastnet	The Coastnet network is an Internet-based data exchange system developed under the direction of the Finnish border guard. Denmark, Estonia, Finland, Germany, Latvia, Lithuania, Norway, Poland, Russia and Sweden are part of Coastnet, enabling their border guards to exchange information about ongoing border control operations, including a joint sea surveillance system covering the whole Baltic Sea. The purpose of the forum is to prevent illegal activities in the Baltic Sea region and improve the efficiency of joint efforts of border services.
Correlation of information	A function where information from multiple sources is analysed to determine what relationships between the information exist.
Data	Facts represented in a readable language (such as numbers, characters, images or other methods of recording) on a durable medium. Data on its own carries no meaning but when given context, data becomes information.
Digital Certificate	A digitally signed statement that certifies the binding between the owner's identity information and his/her electronic public key. In more detail, a digital certificate is an attachment to an electronic message used for security purposes. The most common use of a digital certificate is to verify that a user sending a message is who he or she claims to be, and to provide the receiver with the means to encode a reply. An individual wishing to send an encrypted message obtains a digital certificate from a Certificate Authority (CA). The CA issues an encrypted digital certificate containing the applicant's public key and a variety of other identification information. The CA makes its own public key readily available through print publicity or on the Internet. The recipient of an encrypted message uses the CA's public key to decode the digital certificate attached to the message, verifies it as issued by the CA and then obtains the sender's public key and identification information held within the certificate. With this information, the recipient can send an encrypted reply.

Expression	Definition
e-Customs	The electronic customs project (also known as "e-Customs") initiated by the European Commission aims to replace paper format customs procedures with EU wide electronic ones, thus creating a more efficient and modern customs environment. The project's dual objective is to enhance security at the EU's external borders and to facilitate trade. The first step to the EU-wide electronic exchange of customs declarations was established with New Computerised Transit System started in 1997. As a contribution to the "e-government" programme, in July 2003, the Commission published its communication on a paperless environment for customs and trade (COM/2003/452 of 24/07/2003) which provided a vision of a modern customs service communicating electronically with trade. This vision was endorsed by the Council Resolution of December 5, 2003 which called for a Multi-Annual Strategic Plan for the creation of a European electronic environment, consistent with the operational and legislative projects and developments already scheduled or underway in the areas of customs and indirect taxation.
ECDIS	ECDIS (as defined by IHO Publications S-52 and S-57) is an approved marine navigational chart and information system, which is accepted as complying with the conventional paper charts required by Regulation V/19 of the 1974 IMO SOLAS Convention.
EMODNet	The European Marine Observation and Data Network (EMODNet) has the goal of creating a network where maritime observation data can be shared openly. In EMODNet the maritime observation data is split into 6 datasets, each having its own pilot web portal. The two main capabilities offered by the EMODNet portals are the queries it provides into the databases of the Member States and the Data Products correlating the available data into a combined picture. Data can also be exchanged between the portals using web services. EMODNet is managed by DG MARE.
Encryption	The Cryptographic transformation of data into a form that conceals the data's original meaning to prevent it from being known or used by unauthorized entities. Encryption is the most effective way to achieve data security. To read an encrypted file, one must have access to a secret key or password that enables to decrypt it. Unencrypted data is called plain text; encrypted data is referred to as cipher text. There are two main types of encryption: asymmetric encryption (also called public-key encryption) and symmetric encryption.
EU maritime domain	The EU maritime domain encompasses the EU Member States' Territorial waters, Exclusive Economic Zones and Continental Platforms as defined by the 1982 United Nations Convention on Law of the Sea as well as all maritime-related activities carried out therein, on the seabed, subsurface, surface and above the sea such as installations, cargo, small boats and vessels flagged, owned, managed by or bound to the EU. Beyond the above, it also comprises any Search and Rescue Area and any Area of Operations that has been designated for an EU Maritime Operation under civil or military authority. While all of the areas included in the 'EU Maritime Domain' have a direct or indirect impact on EU policy and interests, not all of them are subject to EU competence.
Europol Information System (EIS)	In addition to SIENA, Europol also provides the Europol Information System (EIS), which is a database for sharing information. Each member state, non-member states with a cooperation agreement and Europol can insert and query data. Hence, information deposited therein is made available to other EU investigators. Furthermore, data is automatically compared with information deposited by other member states. The purpose of this is to look for matches with a view to enhancing intelligence and providing new leads for further investigation. The Europol national units have direct access in order to run queries and to insert and maintain data in it. Member states' liaison officers at Europol and duly empowered Europol officials also have direct access to perform these actions. In specific situations as described in the Europol Council Decision, third parties may also have indirect access to the information through Europol. They may also contribute data to the system.

Expression	Definition
EU LRIT Cooperative Data Centre (EU LRIT CDC)	The Long-Range Identification and Tracking (LRIT) of all EU flagged vessels is performed worldwide by the EU LRIT Cooperative Data Centre (CDC). The EU LRIT CDC is hosted and managed by EMSA. The EU LRIT CDC is a central application taking care of capturing, storing and distribution of LRIT data with other international LRIT data centres globally. Equipment on board vessels automatically submits ship identification and position data via satellite to the EU LRIT CDC from where it can be accessed by Member States.
EUROSUR	The European Border Surveillance System (EUROSUR) provides a platform to cooperate and to share operational information in the form of structured messages about external border events (e.g. illegal immigration, organised crime, drug trafficking, customs fraud, etc.) that are of common interest. EUROSUR is a decentralised network of identical national nodes located in the National Coordination Centres (NCCs). Each NCC collates information from various border control and law enforcement bodies to create a coherent national picture. NCCs are connected to each other and FRONTEX over a secured internet connection (VPN). EUROSUR itself does not process raw data. EUROSUR is managed by FRONTEX.
Feasibility study	Viability study of an integrated solution and associated services.
FIDES	FIDES is a one-stop shop which automates the management of fishery data using Internet technologies, accessible by national administrations in the EU Member States and the European Commission. It offers a wide range of alternatives such as web, e-mail and file transfer. Overall, FIDES aims to improve the operation of the Community's Common Fishery Policy through a technology enhanced communications infrastructure linking DG Maritime Affairs and Fisheries and corresponding administrations in the EU Member States.
Fusion of information	A function where information from multiple sources is combined to form a single unified response.
GEANT or GÉANT	GÉANT is the high bandwidth pan-European research and education backbone that interconnects National Research and Education Networks (NRENs) across Europe and provides worldwide connectivity through links with other regional networks.
High Level Steering Group on SafeSeaNet (HLSG)	The group defined in Annex III of Directive 2002/59/EC (as amended), which comprises MS and Commission representatives, and which has the tasks defined in Commission decision 2009/584/EC of 31 July 2009. The HLSG shall: • make recommendations to improve the effectiveness and security of SafeSeaNet; • provide appropriate guidance for the development of SafeSeaNet; • assist the Commission in reviewing the performance of SafeSeaNet, and; • – approve the Interface and Functionalities Control Document (IFCD) and any amendments thereto.
ICONET	ICONET is the secure web-based Information and Coordination Network for Member States' Migration Management Services. The network enables Member States to transmit confidentially early warning messages relating to illegal immigration, in particular, to first indications of illegal immigration and facilitator networks, perceptible changes in routes and methods or other events and incidents which herald new developments. The network can also be a useful tool for enhancing co-operation among immigration liaison officers posted abroad by the Member States by providing for easy access to all relevant information with regard to their activities.
IMDatE	The IMDatE platform was developed as an interoperable data exchange platform which brings together the existing EMSA monitoring and tracking systems (SSN Central System, CleanSeaNet, THETIS and EU LRIT CDC) that are used for maritime safety, security and protection of the marine environment. IMDatE should not be viewed as a new, stand-alone system developed as an additional pillar of the EMSA portfolio of services and it does not aim to replace any of the existing EMSA systems. IMDatE is thus the technical framework that enhances existing capabilities and brings new ones to the maritime surveillance portfolio, allowing also the delivery of services to new user communities.

Expression	Definition
Information	Contextual meaning associated with, or derived from, data.
Integrated maritime awareness picture	Within the scope of CISE, "integrated maritime awareness picture" is defined as a "picture" produced by means of collection, analysis, interpretation and visualisation – when appropriate through a graphical interface – of data and information received from and shared with different authorities, platforms and other sources in order to achieve maritime awareness and to support the re-action capability at sea.
INSPIRE	Directive 2007/2/EC of the European Parliament and of the Council of 14 March 2007 establishing an Infrastructure for Spatial Information in the Euro-pean Community (INSPIRE) was published in the official Journal on the 25th April 2007 and entered into force on the 15th May 2007. The directive ensures that the spatial data infrastructures of the Member States are compatible and usable in a Community and transboundary context, by requiring that common Implementing Rules (IR) are adopted in a number of specific areas (Metadata, Data Specifications, Network Services, Data and Service Sharing and Monitoring and Reporting). These IRs are adopted as Commission Decisions or Regulations, and are binding in their entirety. The Commission is assisted in the process of adopting such rules by a regulatory committee composed of representatives of the Member States and chaired by a representative of the Commission (this is known as the Comitology proce-dure).
Interoperability	The European Interoperability Framework 2.0 (EIF) defines interoperability as *'the ability of disparate and diverse organisations to interact towards mutually beneficial and agreed common goals, involving the sharing of information and knowledge between the organisations, through the business processes they support, by means of the exchange of data between their respective ICT sys-tems.'* The EIF defines four levels of interoperability: • Legal • Organisational • Semantic • Technical
Maritime surveillance	*Maritime surveillance* is the effective real time and historical understanding of all manmade and natural occurrences at sea.
LOCODE or UN/LOCODE	The United Nations Code for Trade and Transport Locations (UN/LOCODE) is an international, geographical coding scheme which has been developed and maintained by the United Nations Economic Commission for Europe (UNECE).
MARSUR	The aim of this initiative is to improve the maritime picture by linking existing military networks and systems to foster information exchange between all voluntary participants. MARSUR is a decentralised network, whereby existing national systems are connected to a national node (MEXS) through an API in-terface over a secured internet connection (VPN). The MEXS provides common services/capabilities to enable data exchange, such as chat, notification, email, track exchange, white boarding, file sharing, etc. Services can be both distributed and central. The exact data shared can differ from Member State to Member State and from case to case, based on the bilateral and multilat-eral agreements between the Member States. MARSUR is managed by the Eu-ropean Defence Agency (EDA).
Mercury	Mercury is originally a multi-layer security software from Lockheed Martin de-veloped in the framework of CentrixS net-centric warfare development for US and NATO defence forces. It has been used to implement a specific secure in-formation exchange network to support the ATALANTA anti-piracy activities. Access to this "chat" network managed from Northwood (UK) can be granted to other countries and institutions involved as well in anti-piracy actions. It provides in particular instant messaging and chat, near-real time broadcast of piracy alerts, and attack reports. Building and exchanging a Common Opera-tional Picture through Mercury has been discussed at the SHADE information exchange forum on Piracy.

Expression	Definition
Maritime Support Services (MSS)	The 24/7 EMSA service responsible for monitoring the EU maritime transport operational systems (in particular SSN ecosystem). The MSS is permanently monitoring the data quality in, and the performance and continuity of, the operational systems. It also provides a helpdesk facility to the SSN Community and supports the prompt mobilisation of EMSA's contracted oil pollution response vessels following a MS request.
MSSIS (Maritime Safety and Security Information System)	MSSIS (Maritime Safety and Security Information System) provides the unclassified ("white" picture of the maritime traffic from the AIS data of the members of the network). Managed by the US Department of Transportation (DOT), it is aiming for global coverage and aggregates AIS data from 66 Nations on a willing to share basis including many third countries e.g. in South and East Mediterranean Sea. It is not comparable to systems based upon EU legislation. The Defence Community has, for a majority of Member States, access to the NATO maritime surveillance data exchange network: MSSIS data (cf. above) are fed into NATO's MCCIS (Maritime Command and Control Information System), which is classified and includes also intelligence and classified surveillance data. NATO has two Maritime Component Commands (MCCs): The MCC Naples (Italy) is responsible for the Mediterranean Sea, while the MCC Northwood (UK) covers the North Atlantic. In addition, a single Shipping Centre is located at Northwood to maintain a global commercial shipping picture. Each MCC has an MSSIS.
National Single Window (NSW)	System that has B2G (Business to Government) character and provides national level information related to vessel and cargo procedures in ports. Usually consists of a system for interchanging EDI messages, between private and public actors.
Non-repudiation	The process that ensures that the entities involved in a communication cannot deny having participated (e.g. sending entity cannot deny having sent a message).
Port Community System (PCS)	A tool that has B2B (Business to Business) character and supports the exchange of messages in a port environment, having a commercial and logistic nature.
Port Single Window (PSW)	System that has B2G (Business to Government) character and provides local/port level information related to vessel and cargo procedures in the ports. Usually consists of a system for interchanging EDI messages, between private and public actors.
Product	A sellable good such as equipment, subsystem, system or service offered by the supplier to the user and required by the user in order to implement their application.
Protocol	In software engineering, a set of well-known procedures for information exchange that the systems use to send messages back and forth.
Regional Fishery Monitoring Organisations (RFMOs)	Regional Fishery Monitoring Organisations (RFMOs) are international organisations formed by countries with fishing interests in an area. Some of them manage all the fish stocks found in a specific area, while others focus on particular highly-migratory species, notably tuna, throughout vast geographical areas. The organisations are open both to countries in the region ("coastal states") and countries with interests in the fisheries concerned. While some RFMOs have a purely advisory role, most have management powers to set catch and fishing effort limits, technical measures, and control obligations. The EU, represented by the Commission, plays an active role in six tuna organisations and 11 non-tuna organisation. The RFMOs are generally supported by information sharing networks aiming in particular at fighting IUU fishing.

Expression	Definition
SafeSeaNet (SSN)	SafeSeaNet (SSN) is the overall, generic information system including SSN Central System, EU LRIT Cooperative Data Centre (EU LRIT CDC), CleanSeaNet and IMDatE. As such, SSN is the European Union (EU) "ecosystem of systems" for the exchange between designated authorities and in electronic format, of ship positional data, ship particulars, logistic and voyage related information, the detection of potential oil spills and involved polluters and to facilitate the planning of ship inspections. The objective of SafeSeaNet is to support EU and Member States activities for the purpose of maritime safety, port and maritime security, marine environment protection and the safety and efficiency of maritime traffic. The EU Commission is responsible for the management and development at policy level of the SafeSeaNet, CleanSeaNet and IMDatE platforms and for the oversight of those systems in cooperation with Member States. The EU LRIT CDC follows the policies established at IMO and THETIS the policies established by the Paris MoU agreement. EMSA assumes operational responsibility for and is the administrator of all SSN systems.
SafeSeaNet Central System	SafeSeaNet Central System is the EU system for the exchange, in electronic format, of vessel and voyage related information between designated authorities within the European Union. The objective of SSN is to support EU and Member States activities for the purpose of maritime safety, port and maritime security, marine environment protection and the safety and efficiency of maritime traffic. SSN was initiated in October 2004 and became fully operational in 2009. Currently, SSN is managed and operated by EMSA. It is an internet based system with distributed databases. The data exchanged include Automatic Identification System (AIS) data, ship notifications, incident reports, port notifications and hazmat notifications.
SafeSeaNet Group (SSN Group)	The working group, which comprises representatives from MSs, the Commission and EMSA with responsibility for managing technical and operational issues relating to SSN. EMSA chairs and is responsible for managing the SSN group. The SSN group adopts its own rules of procedure, and these constitute part of the SSN technical and operational documentation. The SSN group aims to: a) regularly report to MSs, European Commission (COM) and the HLSG on SSN activities (both central and national systems); b) define user requirements, monitor the system and support its adaptation to users' requirements; c) define the necessary modification and adaptation of the system in order that it complies with the latest regulations; d) coordinate the network of SSN users; e) define new system functionalities and user interfaces as requested by the HLSG; f) develop and update SSN technical and operational documentation, and; g) Propose amendments to the IFCD. The SSN group may decide to create working groups to examine specific issues related to SSN. The general objectives and tasks given to such entities are defined in the terms of reference determined by the SSN group. The working groups shall be dissolved as soon as their mandates are fulfilled.

Expression	Definition
Sea Horse Network	The Sea Horse Network is a dedicated secure satellite communication network developed by the European Union (EU) and Spain to monitor migratory flows between sub-Saharan Africa and Spain. The "Sea Horse Network is already in place between Spain, Portugal, Morocco, Senegal, Gambia, Guinea Bissau, Mauritania and Cape Verde. All this information is processed in the central platform installed in the Canary Island. The major advantage of the Sea Horse system is that increases the cooperation of authorities from Spain, Portugal, North and West African countries. It might be extended to other EU and non-EU states. Based upon a SatCom VPN, it allows sharing sensitive information such as intelligence.
Sea Surveillance Co-operation Finland Sweden (SUCFIS) and SUCBAS	In the early 2000's, Finland and Sweden initiated the Sea Surveillance Co-operation Finland Sweden (SUCFIS) Project. The aim was to merge two independent national sea surveillance systems electronically. In addition to the automatized exchange of information, another significant step was the adoption of common practices and establishing points of contact between the sea surveillance centres. SUCFIS has been operational since the summer of 2006. SUCFIS is established through a specific secure network between the two countries. SUCBAS is an initiative at the scale of the entire region, including Norway, based on the principle that each state decides for itself what parts of its recognised maritime picture (RMP) it wants to share with other states. The exchange of information between the contracting parties' (Finland, Estonia, Lithuania, Sweden, Denmark, Germany, Latvia and Poland) sea surveillance operators is effective from 2 April 2009.
SEIS (Shared Environmental Information System)	SEIS (Shared Environmental Information System) provide decision-makers at all levels (local to European) with real-time environmental data, thus allowing them to make immediate and life-saving decisions. It aims into improving collaboration between organisations and facilitating interaction with civil society at large. It implements the INSPIRE principles.
Service	In generic terms, an intangible good provided to make available and support a specific application in the user environment. In software engineering, a unit of functionality that an application provides or exposes to other applications.
Service Provider	A service provider is an information system that makes available a service to others. When exposing a service, the service provider defines how the service must be used by others (called service consumers). The user of the service only needs to comply with these definitions; the internal workings of the service (e.g. how information is stored, processed or where it originates) are hidden from the user.
SOA	SOA (Service Oriented Architecture) is a type of software architecture that results from applying Service-orientation, understood as a software design pattern where system functionalities are built as "services" that can be reused for different purposes. These "services" are also loosely coupled with the operating systems and technologies that underlie them.
SIENA	Europol has established SIENA to support the Law Enforcement Communities, as an information exchange network. SIENA cannot be seen as a database, but as an application for secure exchange of information within the law enforcement communities. The Europol National Units in the Member States as well as the Liaison Officers at Europol are connected directly to SIENA. Additionally it is possible to connect other competent authorities in the Member States directly to SIENA. Competent Law Enforcement Authorities not connected to SIENA can be reached through the Europol National Unit. Additionally, organisations and non EU Member States, with whom Europol has a co-operation Agreement can be connected directly to SIENA, which is already the case for a number of Member States.

Expression	Definition
Single Window in European Union Member States	Following the approval of the *Directive 2010/65/EU of the European Parliament and of the Council of 20 October 2010 on reporting formalities for ships arriving in and/or departing from ports of the European Union Member States*, the electronic submission of the reporting formalities in electronic format via a "single window" will enter into force by 1 June 2015. The Single Window (SW) is an environment for collection, dissemination and exchange of vessel reporting information with a structured and commonly defined data structure and rules and rights management of information, which are in accordance with relevant international, national and local legal requirements. The goal of the SW is to simplify and harmonise the administrative procedures applied to maritime transport by making the electronic transmission of information standardized and by rationalising reporting formalities.
sTesta or S-TESTA	A private network that gives public administrations access to modern telecommunications services for daily dealings with other public sector bodies across Europe. Its purpose is to provide European institutions and agencies, as well as administrations in the MSs, with network infrastructure that ensures the easy, reliable exchange of data.
System	A functionally self-contained and integrated combination of hardware and/or software products which represent the technological building blocks required to provide a service. The system, in turn, can consist of a number of subsystems and equipment, representing a further breakdown of the technological platform.
SWOT Analysis	This is a tool for establishing the general, strategic circumstances of a business and its environmental position by means of analysing of the Strengths, Weaknesses, Opportunities and Threats.
TAG	The Technical Advisory Group (TAG) is defined in COM(2010) 584 final as a group composed of representatives of each User Community, a representative from BLUEMASSMED and MARSUNO as well as the pertinent EU Agencies and initiatives.
THETIS	THETIS is a central, web-based system hosted by EMSA, which supports the Port State Control inspection regime by facilitating the planning, logging and publishing of vessel inspections. Member States access the system via a web portal. Data regarding the results of inspections are stored in a central database located in EMSA's Data Centre in Portugal. To facilitate the planning of ship inspections, THETIS is linked to SafeSeaNet for vessel traffic information and to AROS to get updates on required vessel certificates.
User	Person or an organization for which the product is designed and which exploits at least one of its functions at any time during its life cycle.
User Community	A user community is composed of a set of public authorities which are bound together by their function, e.g. customs, marine environment, maritime safety and security, defence, fisheries control, border control.
V-RMTC (Virtual Regional Maritime Traffic Centre)	V-RMTC (Virtual Regional Maritime Traffic Centre) is an internet –based ship positions exchange network (mainly AIS) in the form of a plain and unclassified Maritime Picture. V-RMTC was initialised in the Mediterranean and Black Sea (5+5 group) but possibly extended to any nation/region and handles ever-increased ship positions. Compared to SSN, V-RMTC assembles in a centralised way the data from a "coalition of the willing" well beyond EU borders instead of being related to mandatory EU reporting. V-RMTC also provides unclassified Chat-Rooms and Forums within the communities for message exchange. Based on V-RMTC Italy is currently developing the System for Interagency Integrated Maritime Security (DIIMS) with additional sensor data from satellite, radar, Vessel Traffic Systems and other sources, making the data and information exchange available to the Italian authorities (Carabinieri, Coast Guard, State Police, Custom Police and Customs).
Web Service	W3C defines a web service as 'a software system designed to support interoperable machine-to-machine interaction over a network'. It exists as a physically independent software program, comprising a set of capabilities, made available to other software programs.

9.2. Reference Documents

The following documents, although not part of this document, amplify or clarify its contents. Reference documents are those not applicable and referenced within this document. They are referenced in this document in the form [RD.X]:

Table 9-2: Reference Documents

Ref.	Title	Code	Ver.	Date
[RD. 1]	Invitation to Tender nº EMSA/OP/07/09/Lot2/RFP 5 for the "Study to assess the future evolution of SSN to support CISE and other communities"	EMSA/OP/07/09/Lot2/RFP 5	1	
[RD. 2]	Study to assess the future evolution of SSN to support CISE and other communities : Task 1 Interim Report	EMSA.FWC.L2.R5.RES.DD.D1.1	1.5	2013/12/05
[RD. 3]	Study to assess the future evolution of SSN to support CISE and other communities : Task 2 Interim Report	EMSA.FWC.L2.R5.RES.DD.D2.1	1.5	2013/12/03
[RD. 4]	CISE Architecture Visions Document [non paper]		2.01	25/02/2013
[RD. 5]	Directive 2010/65/EU of the European Parliament and of the Council of 20 October 2010 on reporting formalities for ships arriving in and/or departing from ports of the Member States and repealing Directive 2001/6/EC	Directive 2010/65/EU		20 October 2010
[RD. 6]	COMMISSION IMPLEMENTING DECISION of 12.3.2012 concerning the adoption of the Integrated Maritime Policy work programme for 2011 and 2012			12.3.2012
[RD. 7]	OASIS reference Model for Service Oriented Architecture 1.0			12 October 2006
[RD. 8]	ICT Architecture – System and Application Technical Landscape		20	29/01/2013
[RD. 9]	COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS "Towards interoperability for European public services"	COM(2010) 744 final		16.12.2010
[RD.10]	DIRECTIVE 2003/98/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 November 2003 on the re-use of public sector information			17 November 2003
[RD.11]	European Commission Decision 2001/844/EC			29 November 2001
[RD.12]	EU Regulation (EC) 725/2004			
[RD.13]	Directive 2010/65/EC			
[RD.14]	Directive 2000/59/EC			
[RD.15]	Directive 2009/16/EC on Port State Control			
[RD.16]	Directive 99/35/EC on ro-ro ferries and high-speed passenger crafts			
[RD.17]	Directive 2009/17/EC on vessel traffic monitoring			
[RD.18]	Directive 2009/15/EC on Recognised Organisations and the related Regulation			

Ref.	Title	Code	Ver.	Date
[RD.19]	Regulation (EC) No 319/2009			
[RD.20]	Directive 2009/20/EC on insurance for maritime claims			
[RD.21]	Regulation (EC) No 392/2009 on liability for the carriage of passengers			
[RD.22]	*"Mapping of Data Sets and Gap Analysis"*, TAG, Step 2 of the CISE Roadmap			
[RD.23]	Study to assess the future evolution of SSN to support CISE and other communities : Task 3 Comparative Analysis of CISE datasets	EMSA.FWC.L2.R5.RES.DD.D3.2	1.1	2013/12/23
[RD.24]	Study to assess the future evolution of SSN to support CISE and other communities : Task 3 Interim Report	EMSA.FWC.L2.R5.RES.DD.D3.1	2.0	2013/11/27
[RD.25]	Study to assess the future evolution of SSN to support CISE and other communities : Task 4 Interim Report	EMSA.FWC.L2.R5.RES.DD.D4.1	1.0	2013/12/20
[RD.26]	Torremolinos International Convention for the Safety of Fishing Vessels and the Cape Town Agreement	http://www.imo.org/About/Conventions/ListOfConventions/Pages/The-Torremolinos-International-Convention-for-the-Safety-of-Fishing-Vessels.aspx		
[RD.27]	ILO convention concerning work in the fishing sector	http://www.ilo.org/dyn/normlex/en/f?p=NORMLEXPUB:12100:0::NO::P12100_ILO_CODE:C188		
[RD.28]	e-Navigation Strategy	http://www.imo.org/OurWork/Safety/Navigation/Pages/eNavigation.aspx		
[RD.29]	COM (2013) 510 final: "COMMUNICATION FROM THE COMMISSION - Blue Belt, a Single Transport Area for shipping"			08/07/2013
[RD.30]	Study to assess the future evolution of SSN to support CISE and other communities : Task 3 Interim Report	EMSA.FWC.L2.R5.RES.DD.D3.1	2.1	2014/03/05
[RD.31]	Study to assess the future evolution of SSN to support CISE and other communities : Task 3 Comparative Analysis	EMSA.FWC.L2.R5.RES.DD.D3.2	1.5	2014/02/26
[RD.32]	Study to assess the future evolution of SSN to support CISE and other communities : Task 4 Interim Report	EMSA.FWC.L2.R5.RES.DD.D4.1	1.6	2014/03/07
[RD.33]	Proposal for a Regulation of the European Parliament and of the Council establishing the Copernicus Programme and repealing Regulation (EU) No 911/2010			

9.3. Acronyms

The following acronyms are used in this document:

Table 9-3: Acronyms

Acronym	Definition
AG	Advisory Group
AIS	Automatic Identification System
ASP	Application Service Provider
CAMSS	Common Assessment Method for Standards and Specifications
CISE	Common Information Sharing Environment
CDF	Computable Document Format
CG	Correspondence Group
CSN	CleanSeaNet
CST	Coastal Station
CAP	Common Alert Protocol
CSW	Catalogue Service for the Web
CFP	Common Fisheries Policy
DC	Data Centre
DDP	Data Distribution Plan
DNID	Data Network IDentity
EDA	European Defence Agency
EDRM	Enterprise Digital Rights Management
EEA	European Environment Agency
EMSA	European Maritime Safety Agency
ERS	Electronic Reporting System
ESA	European Space Agency
EU	European Union
EC	European Commission
ECSA	European Community Ship-owners Association
EPN	European Patrol Network
ETD	Estimated Time of Departure
ETA	Estimated Time of Arrival
EUNAVFOR	EU Naval Force
EU LRIT CDC	European Union Long-Range Identification and Tracking Cooperative Data Centre
EUROPOL	European Police Office
EUROSUR	European Border Surveillance System
EFCA	European Fisheries Control Agency
FAL	Convention on Facilitation of International Maritime Traffic
FMC	Fishing Monitoring Centre
FRONTEX	Frontières Extérieures (External Borders) the European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union
GNSS	Global Navigation Satellite System
GMT	Greenwich Mean Time
IDABC	Interoperable Delivery of European eGovernment Services to public Administrations, Businesses and Citizens
IDE	International Data Exchange
IDF	Intermediate Distribution Frame
IEC	International Electrotechnical Commission
IHO	International Hydrographic Organization
IMDatE	Integrated Maritime Data Environment
IMO	International Maritime Organization
ITS	Integrated Track Service
INSPIRE	Infrastructure for Spatial Information in the European Community (Directive)
ISM	International Safety Management Code
ISPS	International Ship and Port Security
IPS	Integrated Position Service
IALA	International Association of Lighthouse Authorities
IVEF	Inter-VTS Exchange Format
JRC	Joint Research Centre (EC Directorate-General)
JDP	Joint Deployment Plan

Acronym	Definition
LRIT	Long-Range Identification and Tracking of ships
LAN	Local Area Network
LCA	Local Competent Authority
LOCODE	United Nations Code for Trade and Transport Locations
LTM	Local Traffic Manager
MRS	Message Relay Service
MMSI	Maritime Mobile Service Identity
MSS	EMSA Maritime Support Services
NAF	The North Atlantic Format (Fisheries Standard for Electronic Data Transmission)
NCA	National Competent Authority
NCC	National Coordination Centre (of EUROSUR)
OGC	Open Geospatial Consortium
OWASP	Open Web Application Security Project
PSC	Port State Control
RSS	Regular Shipping Service
SAR	Synthetic Aperture Radars
SAR	Search and Rescue
SSN	SafeSeaNet
SSO	Single Sign On
SQL	Structured Query Language
SSL	Secure Sockets Layer
SOLAS	International Convention for the Safety of Life at Sea
SMS	Short Message Service
SURPIC	SURface PICture
S-AIS or SAT-AIS	Satellite AIS
RVD	Reference Vessel Database
TAG	Technical Advisory Group of CISE
TCO	Total Cost of Ownership
THETIS	Information system hosted at EMSA that supports the new Port State Control inspection regime
UC	User Community
UMA	User Management
UWI	User Web Interface
VLAN	Virtual Local Area Network
VMS	Vessel Monitoring System
VDS	Vessel Detection System
VPN	Virtual Private Network
WSC	World Shipping Council
VTMIS	Vessel Traffic Monitoring & Information Systems -Directive 2002/59/EC…..
VTS	Vessel Traffic Service
WSDL	Web Services Description Language
WMS	Web Map Service
WFS	Web Feature Service
WCS	Web Coverage Service
XML	Extensible Markup Language

DISCLAIMER

The information and views set out in this report are those of the authors and do not necessarily reflect the official opinion of the Commission.

Neither the Commission nor any person acting on the Commission's behalf may be held responsible for the use which may be made of the information contained therein.

[End of Document]