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

Executive Summary

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

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 Integrat-ed 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 Tech-nology. 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 Engi-neering, 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,

[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

building on the earlier Communication on establishing a European maritime transport space without barriers[4] , both point to Union Maritime In-formation 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 infor-mation 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 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.

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 notifica-tions, 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 re-porting 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 re-porting 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) progress of activities, legal records and pilot case results (like the "national

[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.

[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.

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 is 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 al-ready available (or already exchanged) in the SSN ecosystem.

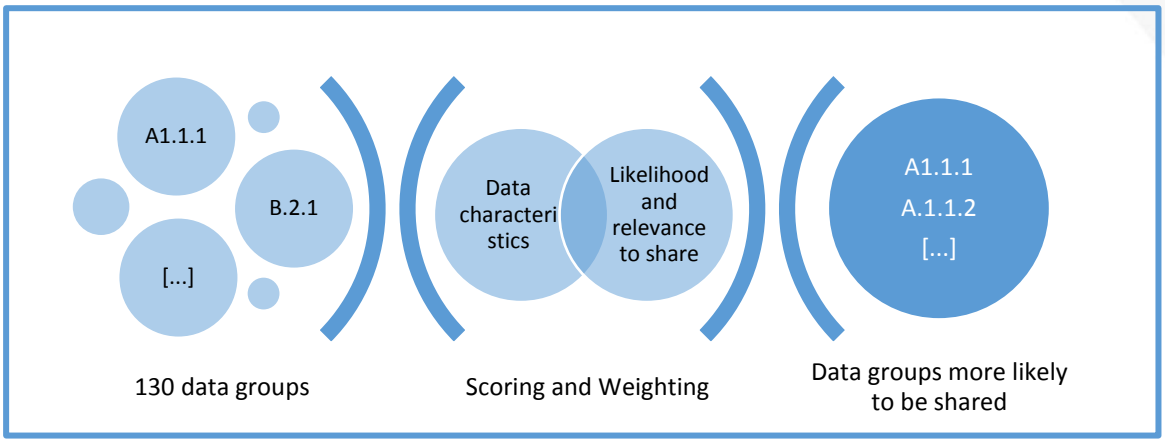
It is imperative to note that the objectives of the study did not include the identification of which "CISE data is important for each user community"[8]. Such a task is difficult given the different and varying national set ups for dealing with maritime monitoring and surveillance (no national set up 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 al-ready 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 in-formation service packages serving specific maritime surveillance purposes and attach corresponding pre-established access rights to each package*".

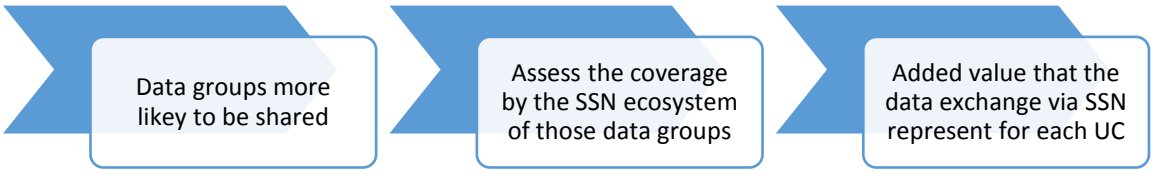
Those 130 data groups result from 113 CISE level 2 datasets and 17 CISE level 3 datasets. Despite such level of ag-aggregation, the integrity of all the CISE structure was kept, as no modification to datasets was done.

[8] 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 Environment" 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)



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.



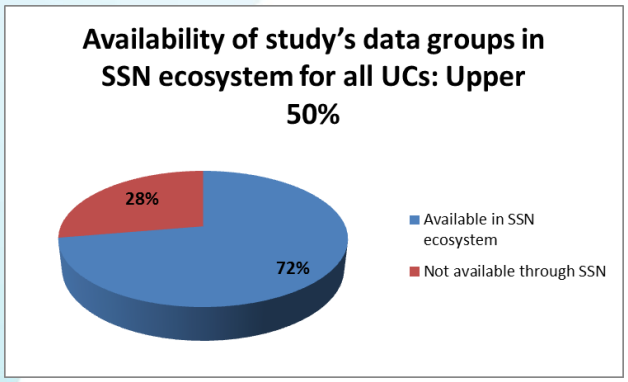
Data groups more likely to be shared (i.e. top results, corresponding to the upper 50% of the 130 data groups) for all UCs, independently on scenario considered, include:

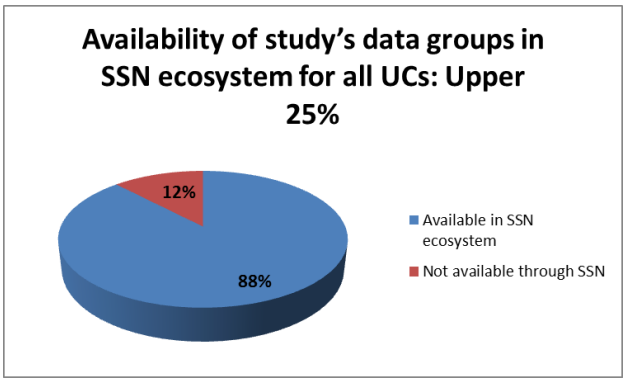
- "Ship position" data;
- "Ship pollution" data;
- "Resources localization for maritime interventions";
- "Maritime infrastructures" data; and
- "Legal maps" data.

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;

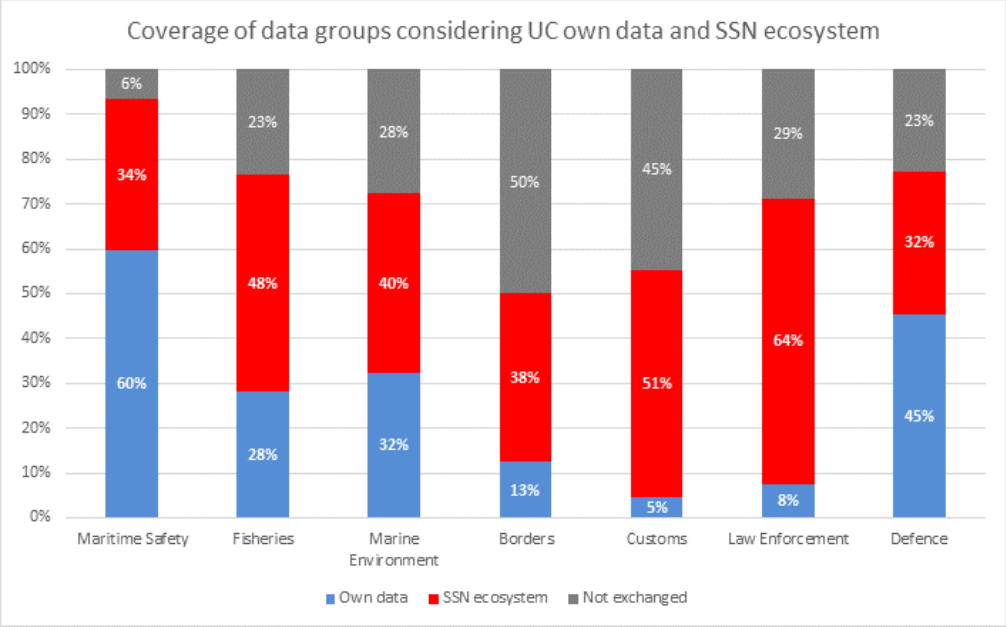
– 23 have origin in other user communities;





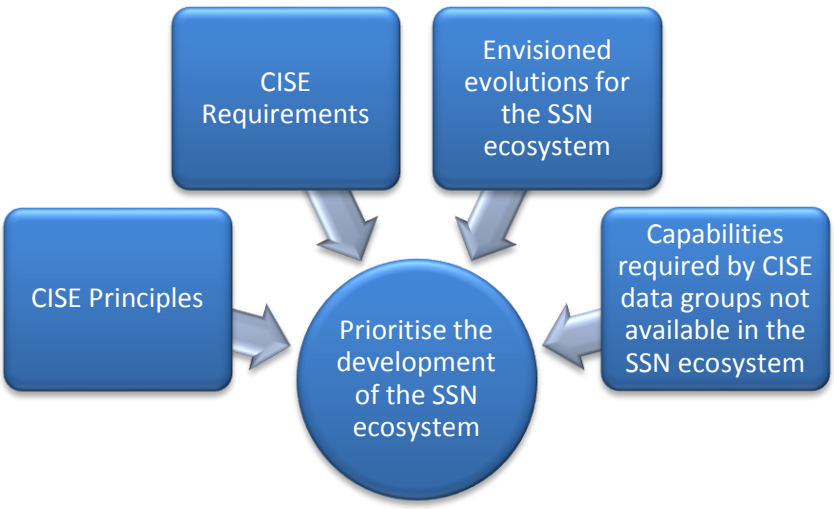
The added value that SSN ecosystem possesses for exchanging data is even clearer when it was evaluated against the data currently owned by each User Community (UC). The data groups covered by the SSN ecosystem represent a substantial value for all the UCs, catering for the coverage of at least more 32% (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[9] and doesn't fulfil 5[10]. 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.

[9] 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.

[10] 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.

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[11] , 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 ex-change 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 ac-cessing 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.

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

SAFESEANET ECOSYSTEM

"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 – The Union Maritime Information and Exchange system, (SSN), is the European system for the exchange, in electronic format, of vessel and voyage related information as established in the VTMIS directive and other relevant Union legislation and between designated authorities within the European Union. SSN supports EU and Member States´ activities regarding maritime safety, port and maritime security, marine environment protection and the efficiency of maritime traffic and maritime transport. SSN became fully operational in 2009. It is an internet based system with distributed databases, comprising a decentralized national level and a centralised level. Currently the SSN central node is managed and operated by EMSA. The data exchanged include among other 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) hosted and managed by EMSA. It is a central application that captures, stores and distributes LRIT data to 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 tracing 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, an alert information package will be sent by the CleanSeaNet service to the pollution control authorities of potentially affected 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, hosted by EMSA which supports the Port State Control inspection regime 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, transform them in a true "ecosystem of systems" and deliver integrated maritime services, **IMDatE** was developed as an interoperable data exchange platform which brings together the existing EMSA monitoring and tracking systems that are used for maritime safety, security and protection of the marine environment with SSN at the core (the above mentioned SSN, CSN, EU LRIT CDC plus THE-TIS). IMDatE is not a new stand-alone system and it does not aim to replace any of the existing EMSA systems or national 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 wider end-users

Pertinent to the study are the **projects and operational integrated maritime services supporting other user communities, namely Blue Belt, SSN-VMS, SSN-Radar, the Anti-piracy support service for merchant fleet monitoring operations service, the Border control surveillance support service and the Fisheries monitoring service**.

SAFESEANET ECOSYSTEM

- Is a "system of operational systems" built using a Service-Oriented Architecture (SOA) and industry standards, over a number of years and updated to remain state of the art;
- Accessible i) via 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;
- Is able to exchange not only basic maritime data (e.g. ship positioning) but also processed information (e.g. ship voyages, satellite imagery, pollution reports, met-ocean information, alerts);
- Is able to ingest and process 3rd party data/information from other systems (e.g. VMS, piracy related reports);
- Provides secure and extensive "data access rights" mechanisms that be used for the definition of different ac-cess profiles. 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 – the "access rights policy". The access follows complex criteria including geo-graphic criteria or nationality of the assets involved in the information;
- Is built on top of an infrastructure in high availability and redundant configuration. Business Continuity is assured in the SSN ecosystem (along with performance and system availability principles enshrined in the systems) through the Maritime Support Services (MSS) Centre and a Business Continuity Facility (BCF). The availability of services within the SSN ecosystem is a on "twenty-four hours a day, seven days a week" basis;
- Is developed with comprehensive security measures ranging from physical access up to logical security;
- Uses an significant geographical information (GI) infrastructure that supports the geographical functionalities of the "Web Interfaces", provides Nautical Charts (ship routing systems, navigation aids, nautical background, administrative boundaries, dangerous areas, etc…) and geo-referenced basic data (geographical grip – parallel and meridian lines , countries, cities, seas, traffic separation schemes, marine infrastructures - AIS, stations- and ports).
- Has already been established as the platform through which key users from various user communities are getting maritime data on a daily basis.

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

TIS.PT, consultores em Transportes, Inovação e Sistemas, SA
AV. MARQUÊS DE TOMAR, 35, 6ºDRT, 1050-153 LISBOA
T: +351 213 504 400 | F: +351 213504401 – www.tis.pt