

---

**SAFESEANET**

**Interface and Functionalities Control Document**

---

**SSN IFCD**

**Version: 1.1.1**

**Date: 02 December 2014**



## Table of Contents

<b>Background .....</b>	<b>6</b>
<b>Chapter 1 - Introduction.....</b>	<b>7</b>
1.1 Primary Objective.....	7
1.2 IFCD Overview.....	7
1.3 IFCD Structure.....	7
1.4 Definitions and Abbreviations.....	8
1.5 IFCD Administration .....	12
1.6 The SafeSeaNet Group.....	12
1.7 SSN Technical and Operational Documentation .....	13
1.8 Entry into Force .....	13
<b>Chapter 2 - SafeSeaNet Overview.....</b>	<b>14</b>
2.1 Introduction .....	14
2.2 Objectives .....	14
2.3 Mandatory System Functionalities .....	15
2.4 Additional system functionalities .....	16
2.5 SafeSeaNet Architecture .....	16
2.5.1 SSN Network organisation.....	16
2.5.2 Information exchange mechanisms .....	18
2.5.3 Messaging process .....	19
2.6 Cooperation with Other EU Systems .....	21
<b>Chapter 3 - Roles and Responsibilities.....</b>	<b>24</b>
3.1 General provisions.....	24
3.2 User management.....	24
3.3 Definition of roles.....	25
3.4 Maximum access rights per role .....	26
3.5 Access by users via other EU systems.....	29
3.6 Access for users outside the SSN legal framework on a pilot basis.....	29
<b>Chapter 4 - SafeSeaNet Performance .....</b>	<b>30</b>
4.1 Timeframes for Data Availability.....	30
4.2 Timeframes for Data Storage.....	30
4.3 System Availability Requirements.....	30
4.4 Backup Procedures .....	31
4.5 Additional System Performance Requirements .....	31
4.6 Data Quality .....	31
4.7 Operational Coordination.....	32
<b>Chapter 5 - Operational Services and Procedures.....</b>	<b>33</b>
5.1 Overview.....	33
5.2 Operational Services.....	33
5.2.1 System Support Services at National Level.....	33
5.2.2 Central System Support Services .....	34
5.2.3 Reference Database Management .....	35
5.2.4 Continuity of Service .....	35
5.3 Operational Procedures .....	35

---

<b>Chapter 6 - System Management and Tests .....</b>	<b>38</b>
6.1 Change Management Framework .....	38
6.1.1 Overview .....	38
6.1.2 Change Management Scope .....	38
6.2 System Commissioning .....	39
6.2.1 General Guidance .....	39
6.2.2 General Commissioning Procedure .....	39
<b>Chapter 7 - System Security .....</b>	<b>40</b>
7.1 General provisions.....	40
7.2 Security Policy .....	40
7.2.1 Organisational Aspects .....	40
7.2.2 General security measures .....	41
7.2.2.1 Access Control .....	41
7.2.2.2 Authentication .....	41
7.2.2.3 Authorisation.....	41
7.2.2.4 Traceability and accountability.....	42
7.2.2.5 Confidentiality .....	42
7.2.2.6 Integrity .....	43
7.2.2.7 Training .....	43
7.2.2.8 Audit .....	43

## Summary of Amendments

Page	Map/block text	Description of changes	Rationale	Approval date
IFCD v1.1.1:				
18	Chapter 2.5.2	Inclusion of the data distribution process	Updates regarding HLSG 11	02-12-2014
21	Chapter 2.6	Interface between SSN and CECIS		
26	Chapter 3.4	Inclusion of the data distribution process – Access rights		
29	Chapter 3.5	Interface between SSN and CECIS		
IFCD v1.1.0:				
6	Background	Updates regarding Directive 2010/65/EU	Updates regarding Directive 2010/65/EU	23-06-2014
8	Chapter 1.4	Definition of NSW and LOCODES added		
14	Chapter 2.2	Exchange of information from the notification of waste and residues and the notification of security information		
15	Chapter 2.3			
16	Chapter 2.3	Management of information on exemptions		
18	Chapter 2.5.2 and 2.5.3	Inclusion of the streaming mechanism for data distribution	Pilot project outcome	
25	Chapter 3.3	Inclusion of the “National Single Window” role and its access rights	Updates regarding Directive 2010/65/EU	
25	Chapter 3.3	Inclusion of the “Waste” and “Security” roles and their access rights		
33 35	Chapter 5.2 and 5.3	Management of information on exemptions		
33 35	Chapter 5.2 and 5.3	Coastal stations and Places of Refuge Information	Update regarding HLSG 9	
42	Chapter 7.2.2.5	Update Commercial Sensitive information with cargo residues	Updates regarding Directive 2010/65/EU	

---

## Background

---

Following the accident involving the crude oil tanker *ERIKA* off the French coast in 1999, the European Union adopted several legal instruments for improving the prevention of accidents at sea and combating marine pollution. Directive 2002/59/EC of the European Parliament and Council of 27 June 2002 as amended, establishing a Community vessel traffic monitoring and information system and repealing Council Directive 93/75/EEC, aims at establishing in the Community a vessel traffic monitoring and information system "with a view to enhancing the safety and efficiency of maritime traffic, improving the response of authorities to incidents, accidents or potentially dangerous situations at sea, including search and rescue operations, and contributing to a better prevention and detection of pollution by ships." Member States and the European Commission shall cooperate in the development of a computerised data exchange system and its necessary infrastructure.

To achieve these objectives, in 2001, the European Commission launched the development of a European network called SafeSeaNet. The main objective of SafeSeaNet is to provide a European platform for maritime data exchange between maritime administrations in the Member States to ensure the implementation of Community legislation in the area of vessel traffic monitoring. It comprises a network of national SafeSeaNet systems in Member States and a central SafeSeaNet system acting as a nodal point, which interacts with the national systems.

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 2002/6/EC enhances the role of SafeSeaNet in facilitating the reception, exchange and distribution of information between the information systems of Member States on maritime activity. In accordance with this Directive, Member States shall ensure that information received from reporting formalities provided in a legal act of the Union is made available in their national SafeSeaNet systems and shall make relevant parts of such information available to other Member States via the SafeSeaNet system. In addition it provides that to facilitate maritime transport and to reduce the administrative burdens for maritime transport, the SafeSeaNet system should be interoperable with other systems of the Union for reporting formalities.

This legal framework requires the collection and distribution of various kinds of data regarding vessel traffic monitoring, port call information, dangerous and polluting cargo details, security, waste and cargo residues, incidents and accidents reports. SafeSeaNet is established to facilitate this exchange of information in an electronic format.

Annex III of Directive 2002/59/EC (as amended) requires the Commission, in close collaboration with the Member States, to develop and maintain the SafeSeaNet Interface and Functionalities Control Document (SSN IFCD).

---

## **Chapter 1 - Introduction**

---

### **1.1 Primary Objective**

The purpose of the SafeSeaNet Interface and Functionalities Control Document (SSN IFCD) is to describe, in detail, the performance requirements and procedures applicable to the national and central elements of SafeSeaNet (SSN) in order to ensure compliance with the relevant Community legislation.

### **1.2 IFCD Overview**

The IFCD is a comprehensive document that describes:

- a) the objectives of the SSN system, the system architecture, the types of data held, the roles and responsibilities of users, the sources and recipients, the system interfaces and the relationship with existing systems,
- b) the performance requirements in terms of data handling, timing, availability and storage, the rules applicable for access rights, data transmission and exchange, and archiving at national and central level, and
- c) the procedures applicable to ensure data quality control, system management, testing and data security.

It should be noted that some technical and operational documentation related to SSN, such as standards for data exchange formats, user manuals and network security specifications, are not an integral part of the IFCD. However, these are described in the associated SSN technical and operational documentation (please refer to section 1.7), and the IFCD contains references where appropriate.

In terms of the relationship between the IFCD and SSN technical and operational documentation, the IFCD contains the high level technical and functional/operational requirements of the system, while the more detailed specifications are described in the SSN technical and operational documentation.

### **1.3 IFCD Structure**

The Interface and Functionalities Control Document (IFCD) is structured in the following manner.

- Chapter 1 - "Introduction" includes the definition of relevant terms, information on document management policy and the roles of the parties concerned.
- Chapter 2 - "SafeSeaNet Overview" provides a system overview and outlines the architecture of the information structure and technologies used. The system functionalities and features are described in this chapter.
- Chapter 3 - "Roles and Responsibilities" defines the users, their roles and the access rights applicable to data distribution.
- Chapter 4 - "SafeSeaNet Performance" describes the information flows; the services and performance rules for the messaging processes and; the information exchange systems applicable to both the national and central SSN systems.

- Chapter 5 - "Operational Services and Procedures" covers the services, operational procedures and best practices relevant to both the national SSN and central SSN systems.
- Chapter 6 - "System Management and Tests" describes the procedures applicable to the management of the SSN system; the test procedures and rules; the changes to the system's status and; the procedures for performing commissioning tests.
- Chapter 7 - "System Security" provides clarification on security related terminology and defines the rules and procedures applicable to data transmission and exchange.

Each page of the document includes the following information in its header:

- Version Number.
- Date of issue.

The list of amendments to the IFCD is recorded in the Summary of Amendments (page 5). SSN users should ensure that they use the latest version of the IFCD.

## 1.4 Definitions and Abbreviations

For IFCD purposes, the definitions in Article 3 of Directive 2002/59/EC, as amended, shall be applicable, as well as the following definitions and abbreviations:

**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.

**Accountability** – The process that ensures that the actions within the system of an entity may be traced uniquely to the entity.

**AIS Regional Server** – A server that a group of MSs agrees to maintain<sup>1</sup> in accordance with the security and reliability requirements of the SSN system and to use to relay AIS data from their national SSN systems to the central SSN system. It may include data collection, storage, backup and re-distribution, as well as monitoring the availability and quality of the data. For these functionalities, and as long as the MSs concerned request to use it as an alternative to the direct connection to the central SSN system, the AIS Regional Server will be considered to be a component of the central SSN system.

**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.

**Central SafeSeaNet system (central SSN system)** – This comprises those SSN components (both technical and procedural) which act as the central/nodal point for the exchange of information between national SSN systems. Such components are the responsibility of the Commission, in close cooperation with the MSs, and are administered by EMSA on their behalf.

---

<sup>1</sup> Under any agreement made between the MSs.



---

**Classified information** – Any information and material, an unauthorised disclosure of which could cause varying degrees of prejudice to EU interests, or to one or more of its Member States, whether such information originates within the EU or is received from Member States, third States or international organisations (in accordance with Commission Decision 2001/844/EC amending its internal Rules of Procedure by annexing Commission Provisions on Security).

**Commercial sensitive information** - Information that is likely to prejudice the commercial interest of any person (a person may be an individual, a company, the public authority or any other legal entity).

**Commissioning tests** – Tests which assess whether national SSN systems support the reliable, timely and accurate exchange of information within the SSN system (as defined in the MS Commissioning Tests Plan). The commissioning process covers all SSN messages transmitted to/from the central SSN system.

**Confidentiality** – The process that ensures that information is not made available or disclosed to unauthorized entities.

**Data provider** – An authorised SSN user who provides information required by the SSN legal framework to other MSs through the SSN system, and makes it available to end users.

**Data user** – An authorised SSN user requesting information required by the SSN legal framework from other MSs through the SSN system.

**Digital Certificate** – A digitally signed statement that certifies the binding between the owner's identity information and his/her electronic public key.

**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.

**Exchange mechanism** – Constitutes the entire electronic data interchange system, including the transmission, message flow, document format, and software used to interpret the documents.

**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 IFCD document and any amendments thereto.

**Integrity** – The process that ensures the accuracy and completeness of information.

**Local Competent Authority (LCA)** – These are authorities or organisations designated by MSs to receive and transmit information pursuant to the SSN legal framework (e.g. port authorities, coastal stations, Vessel Traffic Services, shore-based installations responsible for a mandatory ship's routing system or a mandatory ship reporting system approved by the IMO and bodies responsible for coordinating search and rescue operations).

---

**Maritime Support Services (MSS)** – The 24/7 EMSA service responsible for monitoring the EU maritime transport operational systems (in particular SSN) for the exchange between MSs (and some participating third countries) of information on ships, their voyages, their cargoes and incidents at sea (including accidents and pollution). 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.

**National Competent Authority (NCA)** – The body which assumes responsibility for a national SSN system and its management on behalf of a MS. It is responsible for the operation, verification and maintenance of the national SSN system, and for ensuring that the standards and procedures comply with the requirements described within the IFCD and with the agreed technical and operational documentation. The NCA responsibilities are defined in Annex III of Directive 2002/59/EC, as amended.

**National SafeSeaNet system (national SSN system)** – This comprises technical and procedural SSN elements which support the provision, retrieval and use of information required to implement the SSN legal framework within an MS. These elements are the responsibility of the relevant MS and can be administered either directly by the NCA, via the establishment of LCAs or by setting up other appropriate arrangements with third parties.

**National Single Window (NSW)** – It is the single window established by Member States in accordance with Directive 2010/65/EU.

**NCA 24/7** – The contact point at national level used for 24/7 operational contacts between MSs and with the EMSA MSS.

**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).

**Notification** – Required information sent by the national SSN systems to the central SSN system to inform the SSN community of an event related to a vessel or an incident at sea.

**Operational requirements** – Requirements which focus on the operational usability of SSN, and which define the information, business rules and responsibilities that should be respected during SSN system operation. Operational requirements derive from the legal framework, as interpreted by decisions taken by the HLSC or SSN groups and recorded in SSN documentation.

**Password** – A string of characters used to authenticate the identity of a user. The format of passwords used in SSN is given in the SSN Technical and Operational Documents.

**Personal Data** – Any information relating to an identified or identifiable natural living person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number.

**Request/response mechanism** – This describes the activities to be carried out when a MS requests detailed information on a notification via SSN.

**SafeSeaNet authority (SSN authority)** - These are authorities defined as NCAs, LCAs and EMSA, on behalf of the European Commission for the central SSN system. This covers both "Competent authorities" and "Port authorities" as defined in Article 3 of 2002/59/EC as amended.

**SafeSeaNet legal framework** – All requirements which relate to SSN, as defined by the following legal instruments:

- 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);
- *Directive 2010/65/EU (on reporting formalities for ships arriving in and/or departing from ports of the MSs)* and;
- Regulation (EC) No 725/2004 (on enhancing ship and port facility security);

**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 with tasks as defined in section 1.6.

**SafeSeaNet system (SSN system)** – This comprises both the national and central SSN systems.

**SafeSeaNet user (SSN user)** – This refers to **a person or persons performing the same function and position** (e.g. duty officers on shift work within a single MRCC or VTS-centre) (i.e. an SSN Web user using a browser-based web interface at central, national or local level) or **a system** (at national level the national SSN system, and at local level the LCA systems).

**Ship AIS position enriched with SSN data** – This information consists of Ship AIS position collected by fixed-based stations of Member States provided to the central SSN system enriched with a confirmation of the presence of voyage, Hazmat, Waste, Security, MRS and Incident Reports information provided by Member States.

**System Security information** - Information which requires protection as its publication or unauthorised disclosure would reveal privileged or confidential information related to persons, systems, operations and/or facilities.

**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.

**Technical requirements** – The information and communication technologies (ICT) requirements which need to be taken into account when developing, updating and operating the components that make up national and central SSN systems and their interfaces. The technical requirements support the implementation of the operational requirements.

**Traceability** – Traceability is the process to verify the history, location, or application of the information by means of documented recorded identification.

**Unclassified information** – Information that can be released to individuals without a clearance except when it is deemed personal or sensitive.

**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).

**LOCODES** – Location codes which include both UN/LOCODES and SSN Specific LOCODES as established by the NCA according to the SSN LOCODES Guidelines.

## **1.5 IFCD Administration**

The High-level Steering Group (HLSG) approves the IFCD and any amendments thereto. EMSA is responsible for keeping the latest version updated (as approved by the HLSG) and for its distribution to all NCAs in electronic format. The IFCD will also be available electronically on the EMSA website.

## **1.6 The SafeSeaNet Group**

A SafeSeaNet Group has been established. It is made up of representatives of the Member States, of the Commission and EMSA. Representatives from other organisations and industry may be invited to participate as observers.

The objective of the SSN Group is to manage the technical and operational issues related to SSN.

The NCAs are responsible for designating their representatives on the SSN Group, and for providing their names and functions to EMSA.

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.

The SSN Group consults and reports to the HLSG on any issue related to the HLSG mandate as defined in section 1.4 under "HLSG".

### **1.7 SSN Technical and Operational Documentation**

Together with the IFCD, the SSN technical and operational documentation is the reference for the implementation and operation of the national and central SSN systems.

The SSN technical and operational documentation specifies the standards, functionalities and operational guidance that are needed for the system to interact with public and private systems, including the interfaces for automatic transmission of data by electronic means to the SSN. Therefore, for the MSs to comply with the legal framework, the MSs shall follow these documents when setting up a national system.

These documents are developed and maintained by EMSA in cooperation with the SSN group. EMSA is responsible for keeping the latest version of each document updated and available in electronic format on the EMSA website. In order to maintain consistency within and between technical and operational documentation, EMSA and MSs may propose document amendments to the SSN group for approval.

In case of any dispute regarding the interpretation of the documents the IFCD will prevail over the SSN technical and operational documentation.

### **1.8 Entry into Force**

This document and any revisions to it shall enter into force 20 days after their approval by the HLSG, unless otherwise stated in the text.

---

## Chapter 2 - SafeSeaNet Overview

---

### 2.1 Introduction

SafeSeaNet is a system for the exchange of vessel and voyage related information between designated participants within EU. This chapter provides a system overview, discusses the objectives behind SSN and outlines the main flows of information and system functionalities and actors.

### 2.2 Objectives

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

The operation of SSN involves a number of entities or users at regional, national and local level. The majority of these are in the shipping industry (ships' masters, agents and operators) and national administrations (port authorities and coastal stations, port State control officers, search and rescue (SAR) centres, vessel traffic services (VTSs), ship reporting systems, pollution response bodies, etc.).

By enabling the exchange of vessel and voyage related information, the SSN system supports users at EU and MS level in:

- the **efficient and timely response to incidents or pollution at sea in progress** including search and rescue operations;
- the **monitoring of ships that pose a potential risk to the safety of shipping and the environment**, including those involved in incidents, thus allowing for earlier precautionary actions and risk mitigation at sea by **coastal states**;
- the **effective collection of information in support of the PSC inspection regime**;
- the **effective collection of the required information** on port calls, the carriage of dangerous and polluting goods, security and waste for ships calling into a port of a Member State;
- the **management of flag State responsibilities**, including the follow up of ships involved in incidents/accidents;
- the **efficiency of port calls**;
- the **facilitation of maritime transport**; and
- the **gathering and comparison of objective and reliable information on maritime safety and on pollution by ships**, thus enabling users to take the necessary steps to improve maritime safety and the prevention of ship-generated pollution, and to evaluate the effectiveness of existing measures.

SSN is a specialised system established: to enable the exchange of information in an electronic format between MSs; to provide the Commission with the relevant information in accordance with Community legislation and; to support MSs in satisfying their operational information needs.

SSN is a network of national systems in Member States which are linked to a central SSN system that acts as a nodal point. The central SSN system has different interfaces available to facilitate different means of transmission (see section 2.5.2).

## 2.3 Mandatory System Functionalities

SafeSeaNet, at the national and central levels, is built upon mandatory system functionalities which are crucial to the normal operation of the system. The mandatory SSN system functionalities are the sending, receipt, storage, retrieval and exchange of information by electronic means required by the SSN legal framework. SSN supports the exchange of the following information:

- **Port call information:** Pre-arrival information sent to ports 24 hours in advance and information on ship arrivals and departures (as per Article 4 of Directive 2002/59/EC as amended and Articles 9 and 24 of Directive 2009/16/EC). In addition, 72 hours pre-arrival information if no other national arrangement is in place.
- **Hazmat information:** Information on the carriage of dangerous and marine polluting goods (as per Articles 4, 13 and 14 of Directive 2002/59/EC as amended).
- **Incident information:** Information on accidents and incidents which have occurred at sea (as per Articles 16, 17 and 25 of Directive 2002/59/EC as amended) and information on ships which have not delivered their ship-generated waste and cargo residues (as per Articles 11.2.d and 12.3 of Directive 2000/59/EC).
- **Position information:** AIS, MRS and [LRIT]<sup>2</sup> information (as per Articles 5, 6.b, 9 and 23 of Directive 2002/59/EC as amended).
- **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.
- **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.
- **Information on exemptions** on Port call (pre-arrival 24 hours) and Hazmat (as per Article 15 of Directive 2002/59/EC), Security (as per Article 7 of Regulation (EC) 725/2004) and Waste (as per Article 9 of Directive 2000/59/EC).

---

<sup>2</sup> The technical implementation to allow for the full distribution of LRIT data to MSs through SSN is under development and will be detailed in future IFCD revisions.

The information collected and exchanged through SSN must comply with the quality and performance standards defined in this IFCD and in the relevant technical and operational documentation.

Administration of user management and locations' codes (LOCODES) are also mandatory system functionalities.

## **2.4 Additional system functionalities**

SSN provides a number of additional functionalities which are not mandatory and should they become unavailable, it would not affect the operation of the SSN system.

The additional system functionalities are related but not limited to:

- statistics;
- email warnings for giving an indication that there is Incident Report information available in SSN;
- background information display (e.g. nautical charts);
- system monitoring tools, and;
- secondary or reference data sources (e.g. SSN users contact details, ship particulars, special lists of ships).

Further functionalities may be incorporated in the SSN system, subject to approval by the SSN group.

## **2.5 SafeSeaNet Architecture**

SSN users can access the system via the Internet or the S-TESTA network.

In accordance with the Change Management Framework, SSN interfaces are subject to upgrades, amendments and technical improvements. This ensures that the system is updated, correctly implemented and able to cope with the continuous evolution in national, international or EU legislation.

### **2.5.1 SSN Network organisation**

The SSN architecture operates at two main levels:

- National SSN systems.
- The central SSN system.

Figure 1 describes the principles of the SSN system.



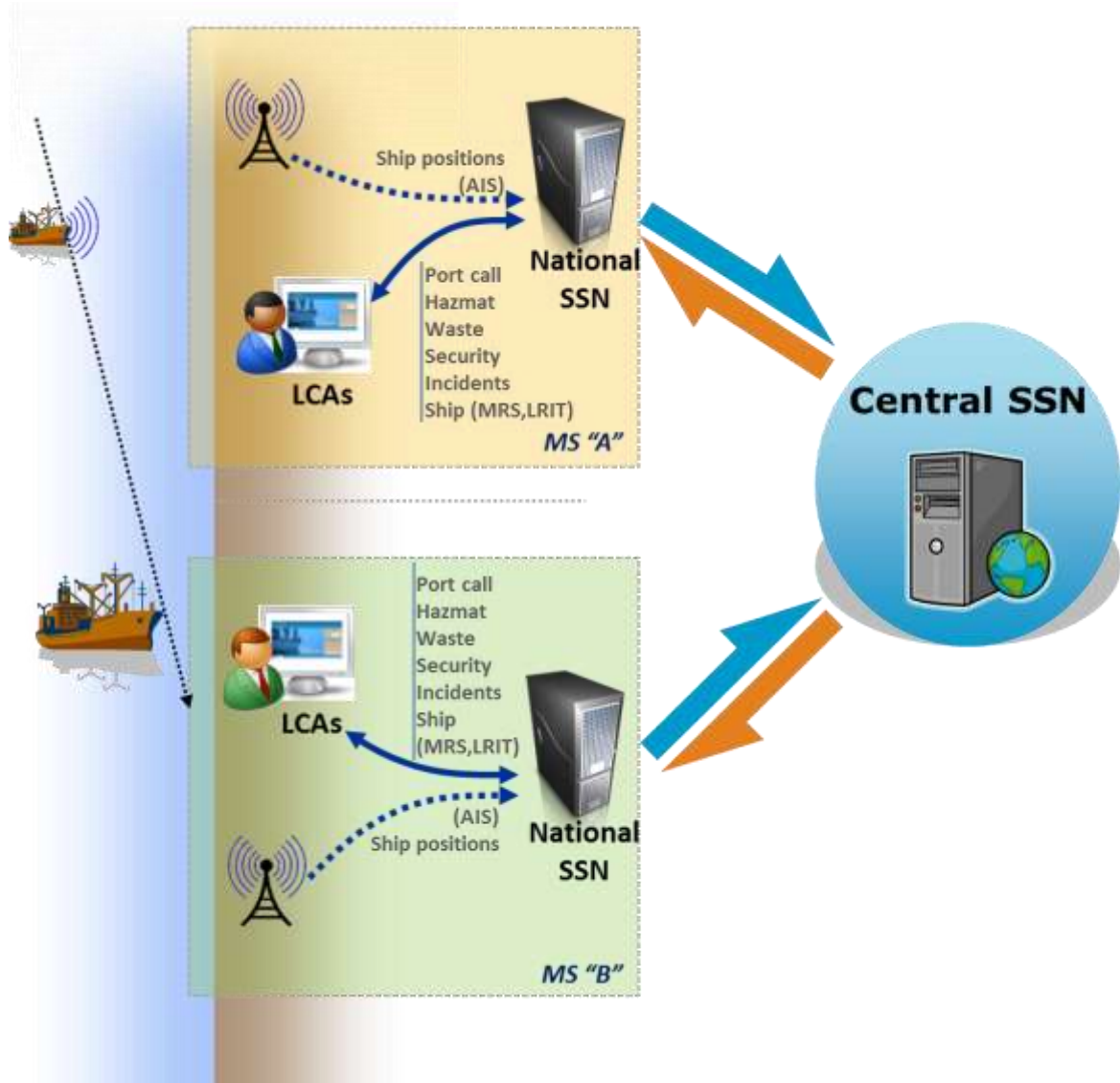


Figure 1 – SafeSeaNet system

LCAs may be data providers as well as data users at local level.

National SSN systems provide information to the central SSN system in the form of notifications. Authorised users within the SSN Community can retrieve information related to these notifications. The central SSN system locates and retrieves this information and provides it to the data user.

While the central SSN system stores some information which enables rapid, effective response to users' requests, detailed information may be stored at national level. When the notifiable information is changed by the data provider, a notification is provided to the central SSN system, and information is updated accordingly.

The NCA may at national level establish a centralised system where all relevant information is registered, stored and exchanged. Alternatively, the details relating to notifications may be stored in the servers of the LCAs.

### 2.5.2 Information exchange mechanisms

The central SSN system provides different alternative mechanisms to the national SSN systems in order to enable the mandatory exchange of information (in section 2.3). These are:

- I. Message-based mechanism:** A mechanism which allows individual messages to be exchanged between the national and central SSN applications. The messages (in XML format) fulfil the needs of both data users and data providers (e.g. proprietary protocol, web-services, etc.). This mechanism supports the notification, request, response and distribution functions for all types of SSN information (section 2.5.3 a).
- II. Streaming mechanism:** A mechanism which enables the constant flow of data (based on predefined criteria) between the national systems and the central SSN system (either directly or via an AIS regional server). This mechanism is available for the provision of AIS information and distributing AIS enriched information from SSN. This mechanism is an alternative to the message-based mechanism for AIS data providing (section 2.5.3 b).
- III. Central SSN Web browser-based mechanism:** This mechanism is available for requesting information, providing and distributing Incident Reports, and may be used to provide other information as a back-up solution in the case of failure of the national or local SSN systems. It is also available for system administration.

The central SSN Web browser-based mechanism offers two interfaces:

- **Textual interface:** This provides direct access to the central SSN system using a textual layout;
- **Graphical interface:** This uses geographical information system technology to provide access to ship AIS positions enriched with the SSN data in the central SSN system<sup>4</sup>, thus creating a vessel traffic image showing movements in near-real time.

For notification purposes, the message-based mechanism and the streaming mechanism are alternative ways of providing Ship AIS positions. The availability and performance standards described hereafter will be applied to the communication mechanism that each MS decides to use in order to fulfil SSN legal framework obligations.

Member States can select the mechanism which best fits their national organisation and technical framework, in order to effectively participate in the SSN Community.

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

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

**Table 1 – SSN mechanisms for information exchange**

Information will be available via all mechanisms for request purposes, regardless of the mechanism used by the national SSN system when providing information.

### 2.5.3 Messaging process

a) Message based mechanism:

- 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.

A sequence diagram describing the above mechanisms is provided in Figure 2.



**Figure 2 - Sequence diagram of notification, request and response mechanisms**

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

b) Streaming mechanism:

- Provision of AIS data
  - SSN is equipped with a streaming mechanism which enables the near-real-time exchange of ship positions obtained via the AIS network. This exists at the regional and national levels in order to enable national SSN systems to provide AIS information to regional servers and/or the central SSN system.

- Distribution for Ship AIS position enriched with SSN data
  - The streaming mechanism supports the distributing of AIS information enriched with SSN data in accordance with the access rights of the user.

## 2.6 Cooperation with Other EU Systems

In this section, the EU systems that interface with the central SSN system at the present time are described, as well as the information exchanged between these systems. A short description of each system is presented below:

- **THETIS** – The Port State Control (PSC) information system developed for the implementation of PSC Directive 2009/16/EC, as well as the New Inspection Regime applicable to the Paris MoU. The system is essential to the daily PSC activities of states operating under the Paris MoU. The entire process (port call registration, targeting, selection, reporting of inspections with corrective actions, publication of details and production of statistics), as stipulated in Directive 2009/16/EC and its implementing regulations, is facilitated by the system.
- **CleanSeaNet (CSN)** – The satellite based monitoring system for marine oil spill monitoring and vessel detection in European waters. Operating under Directive 2005/35/EC on ship sourced pollution, CSN provides a monitoring service to national maritime administrations in EU coastal Member States, EFTA countries and candidate countries in their area of interest. Upon request, CSN provides the European Commission with services in and around the waters of these participating countries. The main objectives of CSN are: the identification and tracking of oil pollution on the sea surface; the monitoring of accidental and deliberate pollution and; contributing to the identification of polluters. The system is based on the provision and analysis of Synthetic Aperture Radar (SAR) satellite images.
- **EU Long-Range Identification and Tracking Cooperative Data Centre (EU LRIT CDC)** – Following the adoption of amendments to the International Convention for the Safety of Life at Sea (SOLAS Chapter V), which introduced the long-range identification and tracking of ships, the Council of the EU (in its Resolution of 2 October 2007 and 9 December 2008) agreed to the establishment of a European LRIT Data Centre managed by the Commission through EMSA. Subject to the provisions in SOLAS Chapter V/19.1, Contracting Governments are able to receive LRIT information for security, safety and marine environment protection purposes. Search and rescue services are also entitled to receive, free of charge, LRIT information in relation to the search for, and rescue of, persons in distress. Within Directive 2002/59/EC as amended, the Council agreed to make use of SSN to facilitate the sharing of LRIT information between MSs. The EU LRIT CDC has been in operation since 4 June 2009.
- **LRIT EU Ship Database** – The EU LRIT Ship Database (EU LRIT Ship DB) is a component of the EU LRIT CDC. The purpose of the database is to allow for the registration of ships which have been instructed by their national administrations

to report to the EU LRIT CDC. It is accessible online by administrations which are responsible for registering ships, and for updating the identification details as requested by SOLAS Chapter V/19.1. An updated version of the EU LRIT Ship DB is automatically sent on a daily basis to the EU LRIT CDC.

- **Common Emergency Communication and Information System (CECIS)** – The system aims to facilitate communication between the European Emergency Response Centre and National Authorities responsible for Civil Protection and Marine Pollution. CECIS legal background lies in Article 6 of the Council Decision 2007/779. CECIS is a centralised system coordinated by the Commission (DG ECHO). In the field of marine pollution, there is an obligation to report to CECIS requests, or potential requests, for (international) assistance (e.g. requests for EMSA Pollution Response Vessels). CECIS facilitates the exchange between stakeholders by providing a tool for managing requests and offers.

Information exchanged between the central SSN system and other EU systems must respect the access rights policy defined in Chapter 3.

The cooperation between the central SSN system and the other EU systems described above can be summarised as follows. Figure 3 illustrates the process for information exchange between the systems.

- **SSN/THETIS:** The central SSN system provides to the THETIS system information received from national SSN systems on the port call (pre-arrival 24 hours, arrival, and departure), waste and security information for ships calling at EU ports and anchorages.
- **SSN/CSN:** The central SSN system provides ship positions and identifiers (transmitted by national AIS networks) to the CSN system in order to assist in the identification of vessels and possible polluters (within a limited timeframe and area).
- **SSN/EU LRIT CDC** <sup>3</sup>
- **SSN/EU LRIT Ship Database:** The EU LRIT ship database provides the central SSN system with ship information in order to validate the ship information held in the SSN system.
- **SSN/CECIS:** The central SSN system provides incident reports of type POLWARN and POLINF to CECIS.

---

<sup>3</sup> The technical implementation to allow for the full distribution of LRIT data to MSs through SSN is under development and will be detailed in future IFCD revisions.

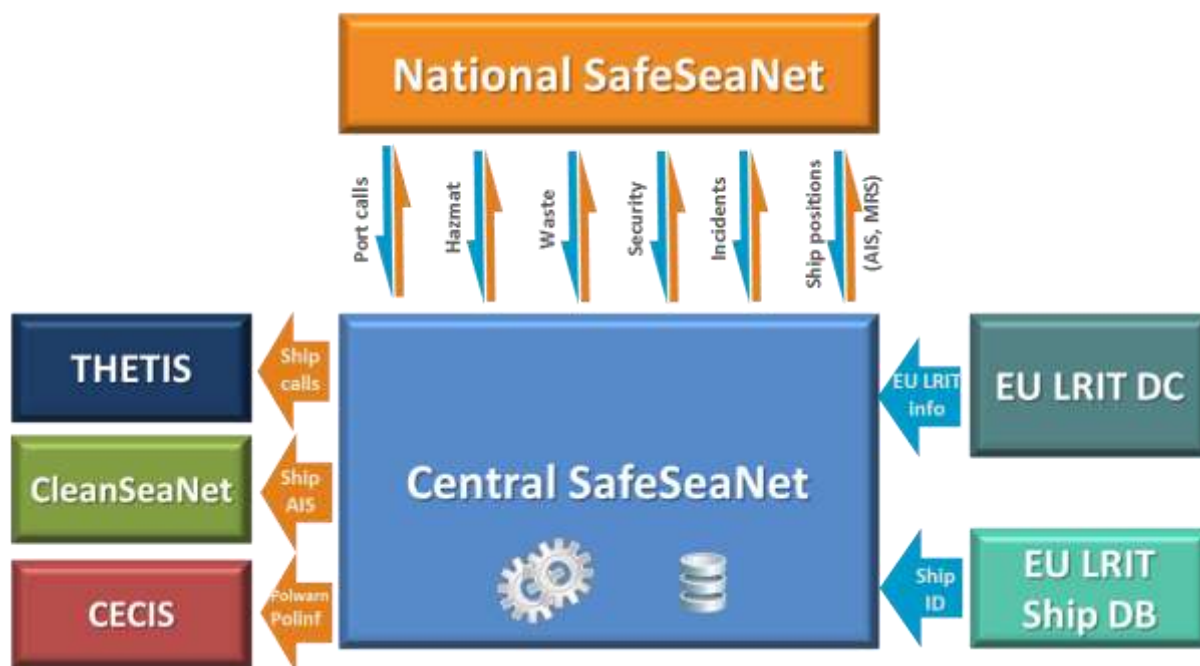


Figure 3 – Interfaces of the central SSN system with other EU systems



---

## Chapter 3 - Roles and Responsibilities<sup>4</sup>

---

### 3.1 General provisions

The EU Commission is responsible for the management and development at policy level of the central SSN system and for the oversight of the SSN system in cooperation with Member States. EMSA assumes operational responsibility for, and is the administrator of, the central SSN system.

With respect to access rights, NCAs and EMSA shall comply with the requirements of the SSN legal framework when managing access to the system.

Access rights should support the performance of the objectives and functions identified in the legal framework or necessary for the operation and administration of the SSN system.

The “competent authorities” (otherwise known as “SSN authorities”) designated to perform the above functions or “roles” should have the appropriate access to perform their responsibilities within the SSN system in accordance with the SSN legal framework.

Within each SSN authority, individual persons, persons with the same function and position or systems may be identified as SSN users.

Hereunder are defined: the general rules for user management; the possible roles for SSN authorities and users, and maximum access rights that should be respected in the implementation and operation of the SSN system.

### 3.2 User management

The NCA within each Member State is responsible for identifying its own SSN authorities and users at national or local level, and for assigning their roles and access rights.

With the support of EMSA, the Commission is responsible for the management of the roles and access rights for the following types of SSN authorities and their users:

- EMSA and the European Commission for SSN administration and management at central level.
- NCAs for SSN administration and management at national level.
- Other types of authorities and users, within the conditions decided by the SSN HLSG (e.g. access to other EU Institutions).

The above mentioned SSN administrators are only entitled to assign access rights within the allowed maximum boundaries defined per role (see section 3.4).

They have the right to manage their own SSN authorities and users through a web based application within the central SSN system (“the web management console”). The user

---

<sup>4</sup> The technical implementation to allow for the full distribution of LRIT data to MSs through SSN is under development and will be detailed in future IFCD revisions.



management process includes adding, editing and removing users, as well as setting their roles and access rights.

SSN users only have access to the information they have been authorised to use in accordance with the roles and access rights assigned by the SSN administrators at national or EU levels.

Access to the SSN system is controlled via a formal user registration process. Each user is identified in SSN by a unique user ID, so that they can be monitored and held accountable for their actions.

The management of users within national applications is the responsibility of NCAs, but the methods used should reflect the principles of the central SSN system.

### 3.3 Definition of roles

SSN administrators assign to SSN authorities one or more of the following functional roles within the system. Each role relates to certain specific SSN system responsibilities in accordance with the SSN legal framework (see section 3.4). The assigned roles should correspond to effective operational functions within the organisation concerned. The possible roles are:

- **National Competent Authority role (NCA):** for the competent authority or body designated by a Member State at national level as data provider and/or data user (as per the SSN legal framework).
- **National Competent Authority Administrator role (NCA ADMIN):** including the management responsibility for the national SSN system at national and local level.
- **National Single Window Authority role (SINGLE WINDOW):** the competent authority designated by a Member State to implement the provisions of Directive 2010/65/EU, in particular, with the responsibility for overseeing the setting up and operation of the NSW as envisaged for the purposes of this Directive.
- **Coastal Station role (CST):** with the responsibilities identified by NCAs as data providers and/or data users for vessel traffic services, shore-based installations, bodies responsible for search and rescue and/or pollution response centres (as per the SSN legal framework).
- **Port Authority role (POR):** for the competent authority or body designated by NCAs to receive and pass information to SSN for each port (in accordance with the SSN legal framework).
- **Port State Control role (PSC):** Fulfilling the SSN-related responsibilities of the maritime authority in charge of port State control (in accordance with Directive 2009/16/EC).
- **Waste Authority role (WASTE):** The “appropriate authorities or bodies for performing functions” under Directive 2000/59/EC, as mentioned in Articles 6.1 and 12.b. Their areas of responsibility might be of national scope or limited to one or several ports.

- **Security Authority role (SECURITY):** the “Competent Authority for maritime security”, as defined in Article 2.7 of Regulation (EC) No 725/2004. Its area of responsibility might be of national scope or limited to one or several ports.
- **Other Users role within Directive 2002/59/EC (VTMIS OTHER):** Fulfilling any other responsibility assigned to a Local Competent Authority (LCA) in accordance with Directive 2002/59/EC and not covered by the above roles.
- **European Commission and EMSA role (EMSA\_EC):** EU Commission and EMSA users with responsibilities at EU level.
- **Central SSN Administrator role (SSN\_ADMIN):** Fulfilling SSN administrator responsibilities at EU level.

National and local systems may have their own sets of roles relating to system functions. These should be constructed to balance the need for access to relevant data with the requirements necessary to maintain confidentiality.

### 3.4 Maximum access rights per role

The **access rights** assigned to each role are defined in the matrix in Table 2, which indicates the default and maximum access rights assigned to each SSN role. Whenever an SSN Authority is allocated less than the maximum access rights for its role, SSN users under that authority will be limited to the same reduced access rights.

Certain cells in the access rights table include **location/condition restrictions**, which limit the access rights of a specific role to a defined area or condition. There are three levels of restrictions:

- Country – limits the access rights to the country where the LCA user is situated (identified in SSN through LOCODES).
- Port – limits the access rights to the port location of the LCA user (identified in SSN through LOCODES). For example, port authorities may only receive port call, Hazmat, waste, security and ship position (MRS) information from SSN if the requested information concerns their port or ports under their responsibility (i.e. information on ships leaving, or en route to, their ports).
- Geographical area - limits the access rights to the information related to ships in a predefined area:
  - MRS - National authorities may only provide MRS information for MRSs’ under their responsibility as per dedicated IMO resolution (unless specific agreement between MSs is in place to report MRS information to SSN);
  - AIS positions enriched with SSN data - National authorities may only receive streamed data of Ship AIS positions enriched with SSN information for their area of interest justified by operational needs (i.e. search and rescue region/exclusive economic zone or equivalent).

The restriction level is indicated in square parenthesis [] in the table below.  
An SSN Authority may have one or several roles.

Table 2 –The maximum access rights per role defined in the SSN system (national and central SSN systems)

ROLES ACCESS RIGHTS		NCA	NCA_ADMIN	SINGLE WINDOW	CST	POR	PSC	Waste Option: [port]	Security Option: [port]	OTH	SSN_ADMIN	EMSA_EC
Data Providing	Port call	X [country]	X [country]	X [country]	X [country]	X [port]	X [country]			X [country]		
	Hazmat	X	X	X								
	Waste	X	X	X								
	Security	X	X	X								
	MRS position	X [area]	X [area]		X [area]					X [area]		
	AIS position	X	X		X							
	Incident	X	X		X	X	X			X		
	Exemptions	X	X							X		
Data Requesting	Port call	X	X	X	X	X [port]	X	X	X	X	X	X
	Hazmat	X	X	X	X	X [port]	X	X	X	X	X	X
	Waste	X	X	X	X	X [port]	X	X	X	X	X	X
	Security	X	X	X	X		X		X	X	X	X
	MRS position	X	X	X	X	X [port]	X	X	X	X	X	X
	AIS position	X	X	X	X	X	X	X	X	X	X	X
	Incident	X	X	X	X	X	X	X	X	X	X	X
	Ship IDs	X	X	X	X	X	X	X	X	X	X	X

ACCESS RIGHTS \ ROLES		NCA	NCA_ADMIN	SINGLE WINDOW	CST	POR	PSC	Waste Option: [port]	Security Option: [port]	OTH	SSN_ADMIN	EMSA_EC
Data Distribution	Incident	X	X	X	X	X	X	X	X	X	X	X
	AIS positions enriched with SSN data	X [area]	X [area]	X [area]	X [area]	X [port]	X [area]	X [area]	X [area]	X [area]	X	X
Other functionalities	Access to banned vessels list	X	X	X	X	X	X	X	X	X	X	X
	Access to SHT vessels list	X	X	X	X	X	X	X	X	X	X	X
	Access to locations list	X	X	X	X	X	X	X	X	X	X	X
	Send email	X	X	X	X		X	X	X	X	X	X
	Search logs	X	X								X	X
	Access to statistic information	X	X		X		X	X	X	X	X	X
	Ship activity tracking	X	X		X	X	X	X	X	X	X	X
	Access rights management		X [country]								X	
	Location manager		X [country]								X	X
	Vessel manager										X	X
	Banned vessel manager										X	X
	Management functions										X	

### 3.5 Access by users via other EU systems

Access to SSN information by users of other EU systems that are connected to SSN (defined in section 2.6) is granted only for the information relevant to their operation (as defined in their legal mandate and respecting the above mentioned maximum access rights per role).

User access to SSN information via other EU systems is limited to the following:

- **THETIS users:** Port call information (pre-arrival, arrival and departure) for any ship calling at an EU port or anchorage (in accordance with Article 24 of Directive 2009/16/EC).
- **CleanSeaNet (CSN) users:** Ship AIS positions and identifiers within a limited timeframe and area (to fulfil mandate of Article 10 of Directive 2005/35/EC).
- **CECIS users:** Incident reports of type POLWARN and POLINF.

### 3.6 Access for users outside the SSN legal framework on a pilot basis

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

In each case, access will be granted only to information relevant to their mandate. The access rights for each user profile shall be determined by a decision of the HLSC for the specific agreed purpose.

Requests for access should be transmitted by the NCA to EMSA, and should provide a precise description of the access requirements, and of the reasons that the information is needed. EMSA, will examine the request in consultation with the Commission, and if appropriate, it will be approved by the HLSC and, if necessary, by the appropriate European Council body.

Subject to the paragraph above, access may be granted to users involved in pilot projects under the following conditions:

- for a limited period up to one (1) year with possibility of renewal.
- through the web interface only.
- for a specific agreed purpose.
- for a limited number of individual users.

EMSA is responsible to inform the HLSC and the NCAs on any access rights given to users outside the SSN legal framework.

At the end of the pilot project the HLSC or appropriate Council body will review the conduct of the user. Access can then be granted on an on-going basis subject to the signature of a Memorandum of Understanding (MoU) and annual renewal by the HLSC or appropriate Council body.

---

## Chapter 4 - SafeSeaNet Performance

---

The following performance requirements apply to the processing of messages and system information.

Member State authorities may assign more specific performance standards in accordance with their national requirements.

### 4.1 Timeframes for Data Availability

The national SSN systems connected to the central SSN system should be supported by data communication links and networks that allow them to transfer information between the two systems within 1 minute. This timeframe should be respected for 95% of the information exchange over a 24h period, and for 99% of the cases over a one year period.

SSN data users should receive the desired information from SSN within an average of 30 seconds (central SSN system will not process responses received after 4 minutes) of making a request. Member States should aim at an average response time much lower than this maximum to meet the operational needs. In the case of phone, fax or email, they should receive the requested information within 60 minutes. This is not applicable to archived information (see Chapter 4.2).

### 4.2 Timeframes for Data Storage

The data shall be directly available in the **SSN system** for:

- a) a minimum of 5 years for information related to incidents and accidents, and;
- b) a minimum of 2 months from the departure of the ship for information related to port calls, hazmat, security, waste and cargo residues; and from the reporting date for ship position information.

In any case, the data should be **archived** for at least 5 years, down-sampled when necessary. The archived data should be made available when requested by NCAs or EMSA, on the basis that the requester must provide a justification for why the information is required. Among other things, archived data may be used for purposes such as: obtaining historical positions of ships involved in illegal activities; statistical analysis or; studies on traffic flows.

NCAs should respond to requests for archived data within 5 working days. The exchange of archived data is done through alternative communication means (see as per point 4.7).

### 4.3 System Availability Requirements

This section refers to the availability of the hardware and software necessary for the performance of the mandatory functionalities of the SSN system (see Chapter 2 - SafeSeaNet Overview).

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

The availability of the SSN 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.

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

#### **4.4 Backup Procedures**

Backup procedures should be in place for each SSN system component, and should be implemented in the event of a failure or a scheduled interruption (as described in the SSN Technical and operational documentation).

In the event of a failure or a scheduled interruption, NCAs shall ensure that SSN messages are stored and then transmitted to the central SSN system when communications and/or systems have recovered. The national and central SSN systems should be able to re-send messages for up to 2 weeks (ship position information may be down-sampled for this purpose).

The body responsible for the affected SSN system component must inform the other SSN system participants according to the operational procedures whenever a failure or scheduled interruption occurs.

#### **4.5 Additional System Performance Requirements**

Invalid messages will be rejected by the central SSN system, and an error message will be sent back to the national SSN system. In cases where the central SSN system transmits an invalid message, the national SSN system should inform the MSS of the reasons for the invalid message as soon as possible.

Invalid messages (those not compliant with the standards set in the SSN Technical and operational documentation) should be less than 0.1% of the total number of messages sent.

All participants should aim to prevent invalid messages from being sent.

#### **4.6 Data Quality**

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

Missing information (provided in accordance with chapter 2.3) should be less than 0.1% per type.

In liaison with EMSA, MSs should set in place appropriate control mechanisms to investigate data quality issues that affect more than 0.1% of the reports per country and type (see Chapter 2.3) per month.

#### **4.7 Operational Coordination**

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

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

The monitoring and operational communication procedures to be used for interaction between the NCA 24/7 contact points and the MSS are agreed at the level of the SSN group (within the framework of Chapter 5).



---

## Chapter 5 - Operational Services and Procedures

---

### 5.1 Overview

This chapter provides a framework for the operational services and procedures to be maintained by both national and central SSN systems to ensure the correct operation of the system.

For this chapter operational services and procedures are understood as services and procedures that require human intervention.

MSs and EMSA should take necessary steps to ensure that operators of the national and central SSN systems are appropriately trained to perform their duties.

### 5.2 Operational Services

#### 5.2.1 System Support Services at National Level

Member States shall ensure that effective exchange of the information referred to in the SSN legal framework takes place at national level.

This information exchange may be executed by means of the designated **24/7 NCA** services, which could include the following elements (on a 24/7 basis):

- Respond to direct requests for information from a SSN user by phone, fax or e-mail: MSs are obliged to respond to SSN requests in accordance with the agreed response times mentioned in Chapter 4.1.
- Respond to requests for information from a MS NCA 24/7 or MSS by phone, fax or e-mail, during a Business Continuity event (in accordance with section 5.2.4).
- Provide an SSN Incident Report distribution service at national level: Incident Reports received from another MS via SSN should be distributed among the relevant LCAs within the country.
- Monitor the performance of the communication system within its service area in order to assess any degradation in its operational capability.
- Monitor data providers' communication links.
- Monitor the NCA's own operations in order to ensure availability and to avoid the distribution of unreliable or corrupted messages.
- Immediately notify the MSS should the national system be unavailable to receive, process or transmit data in accordance with the IFCD specifications.
- Receive information on reported technical failures from the MSS and distribute to national users whenever required (e.g. failures in another MS or in the SSN application/hardware/network).
- Provide support to users at national level.

The NCA should also ensure that additional SSN related services, such as the following, are carried out (not on a 24/7 basis):

- Managing reference databases at national level (see chapter 5.2.3).
- Administrating users' access at national level.
- System assessment relating to the quality of the information provided by the national SSN system.
- Providing feedback to the SSN development teams.
- Providing archived data following requests from NCAs or EMSA.
- Ensure that the company, who has been given an exemption in accordance with Article 15 of the Directive 2002/59/EC as amended, has established an internal system that makes it possible for the NCA to receive the due information.
- Designation of the list of competent bodies according to Article 20.a.3 and Article 22 of Directive 2002/59/EC.
- Report to the central SSN system the information on granted exemptions regarding:
  - Pre-Arrival 24 hours and Hazmat (in accordance with Article 15 of the Directive 2002/59/EC as amended)
  - Security (in accordance with Article 7 of Regulation (EC) 725/2004)
  - Waste (in accordance with Article 9 of Directive 2000/59/EC as amended)

### 5.2.2 Central System Support Services

In accordance with the definition provided in Chapter 1, EMSA is responsible, on behalf of the European Commission, for the management of the central SSN system. This includes: monitoring the continuity of service at the centre; connections with Member States; monitoring and reporting on data quality and availability; IT and engineering support restricted to the user interfaces and; communication interfaces within SafeSeaNet.

EMSA provides these services via its 24/7 **Maritime Support Services (MSS)** operations centre. The services provided on a 24/7 basis are as follows:

- Monitoring the availability and performance of the central SSN system.
- Support Member States in the monitoring of the national SSN systems in terms of availability and data quality of the information exchanged (i.e. the availability of notifications, rejected messages, details in ship positions, Hazmat and incident information).
- Provision of an operational and IT helpdesk for central SSN users (e.g. NCAs).

The MSS also provides the following SSN support services:

- Management and validation of the reference databases in the central system.
- Administration of user accounts within the central system, and in particular, managing the list of NCA contacts to be used for communication purposes.

- Provision of statistics on SSN activity by Member State and type of message.
- Testing of new versions and provision of feedback to development teams.

### 5.2.3 Reference Database Management

Reference databases are those used at the central, national and local levels to support reporting obligations. A non-exhaustive list of the potential databases includes: the location codes database (LOCODES), the ship database, the users database and the dangerous and polluting goods database.

Data exchanged within the SSN system should be coherent and of the best possible quality. Therefore, where practical, the reference databases should be the same for all NCAs and their systems. These may be developed and managed centrally by EMSA in order to harmonise the data and to avoid inconsistencies that may occur as a result of using too many different databases. These central databases should be agreed by the SSN group, and should be made available to all users to improve the quality of the information in the system.

### 5.2.4 Continuity of Service

To cover unforeseen crises, disasters and/or general disruptions to normal system operations, business continuity measures should be in place in order to ensure continuity of service at both the national and central levels. These should be able to guarantee that the SSN system remains able to perform its mandatory functionalities (listed in Chapter 2.3) to the fullest extent possible. These measures are separate from those required to meet the performance standards in sections 4.1 and 4.3 under 'normal' conditions.

The business continuity measures should be defined at national and central level and aim at:

- Ensuring, by means of the alternative solutions, that the mandatory information required by the SSN legal framework can still be available on request, and;
- Ensuring that information is recoverable to the fullest extent possible after a down-time period/disaster/failure.

## 5.3 Operational Procedures

Operational procedures should be defined at both the national and central levels in order to support the operational services defined in Chapter 5.2. These procedures should be described and documented in local manuals and/or in the SSN technical and operational documentation.

The operational procedures should be available to all system support services staff in electronic and/or printed form, and they should be an integral part of regular training activities.

Updating the procedures should be a continuous process, and NCAs should ensure that updates are also made available to all systems support services staff. This should ensure

that they are made aware of all relevant changes, and that new procedures are understood and properly implemented.

Operational procedures which only affect national SSN systems should be defined at national level and are not covered by the IFCD.

The main non-exhaustive list of general operational procedures which affect the different types of SSN users in different MSs is as follows:

**a. Reporting technical failures or planned interventions**

The purpose of this procedure is to ensure that data providers and users receive appropriate information on technical failures or planned interventions in the SSN system.

**b. Providing information during system failures or planned interventions**

The purpose of this procedure is to ensure that, during short periods of system failure or planned interventions, MSs are still able to request information stored at national level using alternative communication means. This back-up procedure only applies to limited requests during maritime emergencies.

**c. Distributing Incident Report notifications to other MSs**

The purpose of this procedure is to harmonise the process of distributing and storing information on Incident Reports.

**d. Reception of distributed Incident Reports**

The purpose of this procedure is to ensure the proper information flow for the distribution of incident reports.

**e. LOCODES management**

The purpose of this procedure is to manage the reference list of LOCODES in the SSN system.

**f. Updating the list of NCA and LCA details**

The purpose of this procedure is to maintain an updated list of NCA and LCA details, including the NCA 24/7 contact and others related to the management of SSN system. The list should be communicated to the MSS.

**g. Missing or mismatched information in SSN**

The purpose of this procedure is to investigate and correct any detected inconsistency in the information provided to the SSN system, including ship details (IMO, MMSI, Call sign and name).

**h. Requesting and providing historical data**

The purpose of this procedure is to harmonise the way that archived data can be requested from any data provider (see Chapter 4.2).

**i. SHT early warning**

The purpose of this procedure is for the MSS to inform MSs is so agreed each time that a single hull tanker (SHT) has been identified in their notifications.

**j. Communication procedure**

The purpose of this procedure is to establish an identification method for data exchanged between two different MSs using communication means such as phone

or email. In such cases, the communication should be re-directed through the NCAs to allow for proper identification (based on the most recently updated SSN contacts list in the system).

**k. Exemption procedure**

The purpose of this procedure is to harmonise the process for recording information on exemptions through the central SSN system. It also clarifies how to retrieve information on exemptions.

**l. Communication of the list of competent bodies**

The purpose of this procedure is to establish the process whereby MSs provide and update information on their coastal stations and places of refuges related information to the Commission, as required by Article 20.a.3 and Article 22 of Directive 2002/59/EC.

---

## Chapter 6 - System Management and Tests

---

### 6.1 Change Management Framework

#### 6.1.1 Overview

The SSN group is responsible for the technical and operational management of the SSN system, including the integration of added value functionalities when approved by the HLSG, and also requirements arising from new or revised legislation. The implementation of new requirements at the national and central levels requires close coordination between MSs and EMSA.

The SSN Change Management Framework (CMF) document, which is part of the SSN technical and operational documentation, describes the procedure/process by which changes to the SSN system are decided upon, introduced and managed. This framework applies to all parties in the SSN system, including the participating MSs and EMSA. The objective of the CMF is to:

- establish a formalised and binding Change Management Process (CMP) via which changes to the SSN system are introduced, coordinated and evaluated;
- identify the actors involved in the CMP, along with each actor's roles and responsibilities;
- determine methods for classifying and prioritising change proposals;
- establish documentation and reporting standards in order to provide an appropriate measure of accountability for changes made using the CMP, and;
- manage modifications to the CMP.

Changes to the CMF will be proposed to the SSN group by participating MSs or EMSA.

#### 6.1.2 Change Management Scope

The CMF will be invoked for all proposed changes to SSN system.

The first stage will be the evaluation of the impact of any requested change. Should the evaluation determine that the change request will have an impact on SSN (at the central and/or national levels), further steps in the change management procedure/process will be applied. The decision making process will reflect the type and extent of any impact on the SSN documentation and its specifications:

- a) When there is an impact on the IFCD, a decision of the HLSG is needed.
- b) Changes affecting mandatory SSN documentation require a decision of the SSN group.
- c) In other cases, a decision by EMSA is sufficient, subject to preliminary consultation with the SSN group.

The CMF is the framework for managing changes which result from EU directives or legal obligations, but it cannot be used to block such changes.

## **6.2 System Commissioning**

### **6.2.1 General Guidance**

Before connecting with the production site of the central SSN system, an NCA shall perform commissioning tests on the national SSN system and provide the data specified in the "MS Commissioning Test Plan" document, which is part of the SSN technical and operational documentation, to the SSN system manager (EMSA). The commissioning tests verify that the system developed by a MS is able to exchange messages in accordance with the system specification.

The commissioning process is required to ensure that national SSN systems can support the reliable, timely and accurate exchange of data and system information within the overall SSN system. The commissioning process is also required whenever there are major changes to SSN system interfaces.

The commissioning process is defined in the "MS Commissioning Tests Plan" document, and it covers all system functionalities and information exchange mechanisms adopted by national SSN systems.

### **6.2.2 General Commissioning Procedure**

Commissioning tests are performed at the request of MSs, and the results shall be documented in a test report. The test report, and the associated data files (if any), are to be submitted to EMSA for assessment.

EMSA shall analyse and evaluate the test report and, if the test results comply with the SSN requirements, EMSA shall aim to validate the results within 2 weeks. Once the results have been validated, EMSA issues a test acceptance form and updates the status of operation of the MS concerned. Via this process, the MS becomes an officially recognised participant in the SSN network for the designated functionality.

The acceptance is then communicated to the SSN group.

MSs may perform tests for a part, or parts, of the system and gain approval only for the designated parts. In cases where MSs choose this option, they must still undergo tests for the remaining part(s) of the system requirements before they can use them in production.

---

## Chapter 7 - System Security

---

### 7.1 General provisions

The following chapter describes the security policy that applies to the processing of messages and system information at central SSN system level.

The baseline security requirements hereunder should be mandatory for the central system and its interface with the National SSN systems and be referred to as optional at national/local level.

Further details about the requirements of this chapter can be found in the SSN Technical and Operational Documentation which includes the SSN security vocabulary.

The SSN authorities may assign higher security measures on the system components they manage due to their specific needs and policies as long as these additional measures do not limit the ability of duly authorised SSN users to access relevant information.

### 7.2 Security Policy

#### 7.2.1 Organisational Aspects

SSN Authorities implementing the SSN system in form of hardware and software and/or with responsibilities in terms of provision of access rights to the SSN system should clearly assign to specific responsible individuals the following minimum security related functions:

- a. Functions related to security management:
  - Evaluation of requests to become a SSN user, against the user management rules in Chapter 3 and any other specific rule on access rights;
  - Association of user roles and sets of user access rights;
  - Ensuring, facilitating and carrying regular system security audits;
  - Carrying out of training courses on security matters;
  - Proposing review and update of the security policy of the authority; and of the security requirements deriving from the IFCD and the SSN documentation to the SSN group.
- b. Functions related to security implementation:
  - Technical implementation and monitoring of the security measures deriving from the IFCD and the SSN documentation;
  - Technical implementation and monitoring of the security policy of the authority.

The above functions shall be adjusted to the needs and the organisation of each Member State.



## **7.2.2 General security measures**

### **7.2.2.1 Access Control**

- a. SSN Authorities implementing the SSN system in form of hardware and software should keep record of individuals gaining physical access to it.
- b. Tailoring of privileges granted to a SSN user by the NCA administrator shall be performed as per access rights policy defined in Chapter 3.

### **7.2.2.2 Authentication**

- c. A reliable authentication mechanism shall be implemented to uniquely identify the SSN users.
- d. Passwords should be compliant with the SSN password policy detailed in the SSN Technical and Operational Documentation.
- e. The creation of User IDs should follow the naming convention defined within the SSN Technical and Operational Documentation.
- f. SSN Authorities implementing a web interface shall guarantee the authenticity of that web interface by appropriate means based on industrial best practices. For the central SSN web interface 1-way SSL will be implemented.
- g. SSN authorities implementing a machine-to-machine interface shall guarantee the authenticity by appropriate means based on industrial best practices. For interfaces with the central SSN system 2-way SSL will be implemented.
- h. A user ID should only be used by the appointed SSN user or users. Authorities in charge of providing access to the SSN system should keep a record of all accesses per user ID at their system level.
- i. A review of the credentials (e.g. password modification, user account revocation) used to access the SSN system should be performed at each system level regularly (at least each year) or whenever there is an upgrade of the SSN security policy affecting the authentication mechanism (e.g. SSN password policy).

### **7.2.2.3 Authorisation**

- j. Authorisation of the NCA by EMSA, or of the LCA (implementing a local system) by the NCA should be subject to the identification of the individuals in their organization responsible for the security management and security implementation.
- k. SSN Authorities should grant access only to users in accordance with the rules in Chapter 3.
- l. A review of the authorisation/access rights) should be performed at each system level at least each year or whenever there is an upgrade of the SSN security policy affecting the authorisation protocol (e.g. change in the access right policy).

---

#### 7.2.2.4 Traceability and accountability

- m. Central SSN system allows the verification of the history, location, or application of the information from the mandatory system functionalities (as per chapter 2.3) by means of documented recorded identification. NCAs are responsible for collecting this security data at national level.
- n. The following actions shall be traced and the records shall be available to the data provider of the information upon request:
  - Receipt of the information.
  - Modification of the information.
  - Requests for the information.
- o. The information recorded shall be as follows:
  - User identification<sup>5</sup>.
  - Time stamp.
  - Description of action.
- p. Each SSN system (national and central) shall ensure the non-repudiation and traceability of actions performed by SSN users accessing the system by means of both automated systems (message based and streaming mechanism) or the web interface (web-browser based mechanism). An administration providing the information can request the identity of the data requestor, without delaying the response.

#### 7.2.2.5 Confidentiality

- q. SSN Authorities implementing the SafeSeaNet system in form of hardware and software and/or with responsibilities in terms of provision of access rights shall ensure that the confidentiality of the data stored within or exchanged by those system components they are responsible for is not compromised. Data protection procedures shall be put in place. The protection procedures for the data exchange are specified in the SSN Technical and Operational Documentation.
- r. The SSN system shall manage data according to their confidentiality level for both data exchanged and data stored. According to Commission Decision 2001/844/EC amending its internal Rules of Procedure by annexing Commission Provisions on Security, the SSN system is classified as an "unclassified system". SSN nevertheless includes some commercial sensitive data, system security related information and personal data as follows:
  - "Commercial Sensitive" : all Hazmat, incidents, cargo residues and port call information;
  - "System Security related" : user authentication password, security tokens and certificates;
  - "Personal data": users' credentials, names and contact details of persons.

---

<sup>5</sup> In case a user account is shared by a group of people sharing the same functions, the identity of all the persons that make use of the account shall be available.

- 
- s. Data storage shall be performed in accordance with the following rules:
    - System Security Related data shall be stored encrypted;
    - Commercial Sensitive data shall be protected according to the access rights policy.
    - Personal data should be stored in accordance with point (w) below.
  - t. Users shall not provide information to any unauthorised persons or systems.
  - u. Users shall not disclose their login credentials to unauthorised persons.
  - v. Users shall not provide to the SSN system classified information as defined by Commission Decision 2001/844/EC.
  - w. The principles of personal data protection as defined in Directive 95/46/EC shall be applicable to any information concerning an identified or identifiable person exchanged through SSN system. In addition, the central SSN system shall comply with Regulation (EC) 45/2001 on protection of data by the Community Institutions and bodies and in accordance with Directive 2001/45/EC for EMSA.

#### **7.2.2.6 Integrity**

- x. SSN shall ensure that the information is authentic and complete. The information transmitted via the central SSN system shall only be modified by:
  - the data provider;
  - the NCA covering the data provider, or;
  - the central SSN system (in accordance with the rules/procedures defined in the SSN documentation).
- y. The management of data provision shall ensure all reasonable steps have been taken to prevent denial of service attacks, the introduction of 'malware', or other malicious events with the potential of compromising SSN functionalities.
- z. The list of hardware and software, used to implement the SSN system or used within the authority to interface with it, should be recorded in a register. This register should be maintained during the whole system lifecycle.

#### **7.2.2.7 Training**

- aa. 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.

#### **7.2.2.8 Audit**

- bb. Security audits on the SSN system implementation and usage should be carried out on a regular basis or in case of events defined within the SSN Technical and Operational Documentation. Whenever possible existing audit arrangement will be accepted as the fulfilment of this requirement
- cc. Following a security breach there should be an investigation to identify the cause and any remedial actions required.