SAFESEANET

Interface and Functionalities Control Document

SSN IFCD

Version: 0.03

Date: 9 March 2011

Document Approval

	Name	Date	Signature
Prepared by:			
Checked by:			
Quality control by:			
Approved by:			

Distribution List

Company	Name	Function	For Info / Approval

Change Control History

Version	Date	Author	Description
0.00	12-11-2010	EMSA	Draft 'zero'
0.01	11-01-2011	IFCD WG	1st meeting review on chapter 1, 2 and 4 (partial until section 4.2)
0.02	24-02-2011	IFCD WG	2nd meeting supporting document including follow-up actions from 1st meeting on chapter 1 and 2
0.03	xx-03-2011	IFCD WG	2nd meeting review

Document information

Creation date:	
Filename:	
Location:	
Number of pages:	

Draft note: amendments to text

The proposed amendments to the text are included in track changes (insertions in blue and underline; deletions ~~in red and strikethrough~~) and identified by the author in a footnote at the bottom of the page.
Open Issues in the document are identified by text highlighted in yellow included in a footnote at the bottom of the page

Table of Contents

Summary of Amendments

Page	Map / Block text	Description of the changes	Decision Date	Rational	Context

Background [1]

Source: *ICD and Directive 2009/17/EC amending Directive 2002/59 EC VTMIS "PREAMBLE"*

Following the accident of the *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 co-operate in development of a computerised data exchange system and its necessary infrastructure.

To achieve these objectives, in 2001 the European Commission launched development of a European network - the so-called SafeSeaNet. The main objective of SafeSeaNet is to provide a European Platform for Maritime Data Exchange between maritime administrations of the Member States to ensure the implementation of Community legislation. It is composed of a network of National SafeSeaNet systems in Member States and a Central SafeSeaNet system acting as a nodal point.

Implementation of Directive 2002/59/EC (as amended) as well as other provisions from different instruments of European legislation, requires the collection and distribution of various kinds of data. These concern vessel traffic monitoring, dangerous cargo details, incidents and accidents reports, information related to ships' waste and security.
SafeSeaNet is established to facilitate this exchange of information in an electronic format.

In the future additional information might be included in SafeSeaNet according to the forthcoming legislation.

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

1 Action point 1 (IFCD#2 meeting): Send a 'clean' version of the Background [Done]

Chapter 1 - Introduction [2]

Scope: *Introduces the SSN IFCD and includes the definition of relevant terms, information on the document management policy and the roles of the parties concerned.*

Source: *ICD + amendments*
1.1 - Overview
1.6 - Definitions
1.2 – Document Objective
1.3 – Document Organization

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 designed to ensure compliance with the relevant Community legislation.

1.2 IFCD Overview

The IFCD is a comprehensive document that describes 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. It describes 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. It describes 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 SafeSeaNet, such as standards for data exchange format, users' 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 1.6), and the IFCD contains references where appropriate.

The relation between the IFCD and the SSN technical and operational documentation can be described as follows: 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.

2 Action point 2 (IFCD#2 meeting): Send a 'clean' version of chapter 1 [Done]

- Chapter 1 ”Introduction” includes the definition of relevant terms, information on the document management policy and the roles of the parties concerned;
- Chapter 2 “SafeSeaNet Overview” consists of a system overview and outlines the architecture of the information structure and technologies used. In this chapter the system functionalities and features are described;
- 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 elements of SafeSeaNet;
- Chapter 5 “Operational Services and Procedures” covers the services and operational procedures and best practices maintained by both the Central SSN system and the National SSN systems;
- Chapter 6 “System Management and Tests” describes the procedures applicable for the management of the SSN system, the testing procedures and rules, the changes to the system’s status and the procedures for performing commissioning tests;
- Chapter 7 “System Security” provides clarifications on security related terminology and defines the rules and procedures applicable to data transmission and exchange.

Each page of the document includes in its header:

- Version Number;
- Date of issue.

The detailed description of the amendments is noted with each new revision. Readers should ensure that their copy of the document includes all the revisions issued, as indicated in the Summary of Amendments on page 5.

1.4 IFCD Administration

The High-level Steering Group (HLSG) approves the IFCD and any amendments thereto. EMSA is responsible to keep the last version of the IFCD updated as approved by the HLSG and to distribute it to all NCAs in electronic format.

1.5 The SafeSeaNet Group

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

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

The National Competent Authorities (NCA) are responsible to designate their representatives to the SSN group and to notify the EMSA Secretariat of the names and functions of the members of the delegation.

EMSA chairs and is responsible to manage the SSN group.

The SSN group adopts its rules of procedure. These constitute part of the SSN technical and operational documentation.

The SSN Group aims to:

a) regularly report on the SafeSeaNet activities (both Central and National systems) to MS, COM and HLSG;
b) define user requirements, monitor and support adaptation of the system to users' requirements;
c) define the modification and adaptation of the system needed for compliance with the latest regulations and technical evolutions;
d) coordinate the network of SSN users;
e) define new system functionalities;
f) elaborate the SSN technical and operational documentation; and
g) propose amendments to the IFCD.

The SSN group may decide to create sub-working groups to examine specific issues related to SSN. The tasks and frames given to such groups are defined through the Terms of Reference decided by the SSN group. The sub-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.

1.6 SSN Technical and Operational Documentation [3]

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 validation of these documents is made by the SSN Group.

The IFCD prevails over the SSN technical and operational documentation.

EMSA is responsible to keep the last version of each document updated and available in electronic format. In the purpose of maintaining consistency over the whole technical and operational documentation, EMSA can suggest changes to documents to the SSN group.

The SSN technical and operational documentation is the following:

SSN Interface Reference Guide (requirements for the communication mechanisms chosen by the NCA) defines all the communication mechanisms and standards to interface SafeSeaNet, it includes the following documents:

The document details:

3 Action point 3 (IFCD#2 meeting): Evaluate if the section 1.6 'SSN technical and Operational Documentation' should be included as an annex to allow revision by SSN group [All]

- the SafeSeaNet system, including the architecture, scope, tools for sending and receiving data, administration of servers and databases, constraints, stakeholders, data quality guidelines, data encoding, network and security requirements.
- the functional services, including administrative, operational, reporting, security, and transactional services, and processes detailing how to send and request information (communications).
- the messaging framework, including the messages overview, detailed content and the business rules to apply. This is an essential part regulating the interfaces between National and Central SSN systems.

Network and Security Reference Guide (requirement) defines SafeSeaNet network and information exchange/ data security policies and relevant functional/ non-functional specifications.

SafeSeaNet Handbook (for guidance) is the reference document to support MS through preparatory and development phases up to the regular operations within the system. It aims at linking procedures described in existing SSN documents and presenting them together in a set of control lists. The SSN Handbook does not supersede or replace any of the existing SSN documentation.

SSN Web interface User Manual (for guidance) presents the SafeSeaNet Web application user with the information necessary to use the application efficiently and effectively (including SSN GI).

Change Management Framework (requirement) presents the procedures to define and control the process by which changes to SSN are introduced, coordinated and decided.

Member States Commissioning Test Plan (requirement) presents the test cases and test scenarios that should be used by Member States in order to support the Commissioning process.

Messages Guidelines (for guidance) provides information and advice to SSN Users on how to apply different Reports. The guidelines clarify the procedures for exchanging information, including what information needs to be shared.

SSN Group Rules of Procedure (requirement) gathers the rules of procedure adopted by the SSN Group members to regulate their communication and decision process.

1.7 Definitions

For IFCD purposes, the definitions in Article 3 of the Directive shall be applicable, as well as the following definitions:

Central SafeSeaNet system is made up of those components, both technical and procedural, of SafeSeaNet that act as the nodal point to allow the exchange between National SafeSeaNet systems of information required by Member States to implement the

SSN legal framework. Such components are the responsibility of the Commission, in cooperation with the Member States, and are administered on their behalf by EMSA.

Commissioning tests - Tests required to ensure that the NCAs provide for reliable, timely and accurate exchange of data and system information within the SSN system (as defined in the MS Commissioning Tests Plan). The commissioning process covers all the SSN messages transmitted to/from the Central SSN system.

High Level Steering Group on SafeSeaNet (HLSG) – Group defined in the Annex III of the Directive and composed of representatives of the Member States and of the Commission with tasks as defined in the 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;
- approve the IFCD document and any amendments thereto.

SSN Legal framework – All the requirements related to SSN defined by the following legal instruments: Directive 2002/59/EC as amended (establishing a Community vessel traffic monitoring and information system) and Directive 2009/16/EC (on Port State control).

Local Competent Authority (LCA) - The authorities or organisations designated by Member States to receive and transmit information pursuant to the Directive (e.g. port authorities, coastal stations, Vessel Traffic Services, shore-based installations responsible for a mandatory ship's routeing system or a mandatory ship reporting system approved by the IMO or bodies responsible for coordinating search and rescue operations).

Maritime Support Services (MSS) – The 24/7 EMSA service responsible for monitoring the main EU maritime operational systems (in particular SafeSeaNet) for the exchange between EU MS (and some third countries participating) of maritime information about ships, their voyage, their cargoes and any incidents at sea, including accidents and pollution. The MSS is permanently monitoring the data quality in those EU maritime information systems, their performance and continuity, providing helpdesk and supporting the prompt mobilisation of the EU Pollution Response in case of MS request.

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.

National Competent Authority (NCA) – The body that assumes the responsibility for the National SafeSeaNet system, and its management, on behalf of a Member State. It is responsible for the operation, verification and maintenance of the National SafeSeaNet system, and for ensuring that the procedures comply with the requirements described within the Interface and Functionalities Control Document. The NCA responsibilities are defined in Annex III of the Directive.

National SafeSeaNet system is made up of those components, both technical and procedural, of SafeSeaNet that allow the provision, retrieval, and use of information required to implement SSN legal framework within a Member State. Such components are the responsibility of the relevant Member State and can be administered directly by

the NCA, through the establishment of LCAs, or other appropriate arrangements with third parties.

NCA 24/7 – A contact point at national level used for the 24/7 operational contact among the MSs and the EMSA MSS.

AIS Regional Server - The server that allows the collection, storage, backup, filtering and redistribution of AIS data from a group of MS on behalf of the Central SSN system. Such components are the responsibility of EMSA.

Operational Requirements - Focus of the operational usability of SSN and define the information, business rules and responsibilities that should be respected in the SSN system operation. Operational requirements will derive from the legal framework, as interpreted by decisions taken by the HLSG or SSN groups and recorded in SSN documentation.

Technical Requirements – The ICT (information and communication technologies) requirements to be followed for developing, updating and operation of the components that make up National SSN and Central SSN systems. The requirements support the implementation of the operational requirements.

Request/Response mechanism– This describes the flow of activities performed when a Member State requests detailed information on a notification from SafeSeaNet. This involves three actors: the data requester (the Member State requesting the information); the Central SafeSeaNet system (providing the information and/or acting as a "yellow pages") and; the data provider (if the information is not available in SafeSeaNet).

SafeSeaNet Group (SSN Group) – A working group comprising representatives of the Member States, Commission and EMSA with responsibility for managing technical and operational issues related to SafeSeaNet with tasks as defined in paragraph 1.5.

SafeSeaNet system – When mentioned in the IFCD document, comprises both National and Central SSN systems.

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 member States, with a network infrastructure that ensures the easy, reliable exchange of data.

UN/LOCODE - United Nations Code for Trade and Transport Locations (UN/LOCODE) is an international geographic coding scheme developed and maintained by the United Nations Economic Commission for Europe (UNECE).

Data requestor - *4*

Data provider - *4*

4 Action point 4 (IFCD#2 meeting): Propose definitions to 'data requestor' and 'data provider' [SE]

Chapter 2 - SafeSeaNet Overview [5]

Scope: *Consists of a system overview and outlines the business drivers, architecture of the information structure and technologies used. In this chapter there are general indications of the system functionalities and features. Technical specifications will be developed in a separate technical document which incorporates the technical details of the existing and incoming systems (SSN Communication Interface Document);*

Source: *ICD + amendments + XML Reference Guide*

2.1 - General
2.2 – Architecture of the System
7.1.4 – General architecture of the system
7.1 – Communication Interfaces
7.1.1 – XML based interface
5.1 – Types of messages
5.2 – Notifications
5.3 – Request
5.4 – Receipt
7.1.2 – Default browser-based web interface

2.1 Introduction

This chapter provides for a system overview and outlines the main flows of information and system functionalities and actors. Technical specifications are developed in separate technical documents adopted by the SSN Group.

2.2 Overview

The objective of the SSN system is to share and distribute maritime related information on ship's movements and their Hazmat cargos, as well as information on incidents/accidents, to support MS activities for the purpose of maritime safety, port and maritime security, marine environment protection and the efficiency of maritime traffic and maritime transport.

--- Include a new paragraph on business drivers --- **6**

SafeSeaNet is a specialized system established to facilitate the exchange of information in an electronic format between Member States and to provide the Commission with the relevant information in accordance with Community legislation and to support the MS in their information needs.

It is composed of a network of National SSN systems in Member States and a Central SSN system acting as a nodal point. The Central SSN system has different interfaces available thereby allowing optional/alternative means of transmission (as explained in detail further in the document).

---

5 Action point 4 (IFCD#2 meeting): Send a 'clean' version of chapter 2 [Done]

6 Action point 5 (IFCD#2 meeting): Prepare new drafting on 'Business Drivers' [EMSA/DE/NO]

The operation of SafeSeaNet involves a number of entities or users at regional, national and local level. These can vary from those in shipping industry (ships' masters, agents or operators) to national administrations (such as port authorities and coastal stations, Port State Control officers, SAR centres, VTS, ship reporting systems, pollution response bodies, etc.) as per Directive 2002/59/EC as amended.

Implementation of the Directive, as well as other provisions from different instruments of the legislation of the Union, requires the collection and distribution of different information sources mainly through SafeSeaNet.

2.3 Mandatory system functionalities

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

- Port reports (pre-arrival information sent to ports 72 and 24 hours in advance and ship's arrival and departure) as per Directive 2002/59 as amended Article 4 and Directive 2009/16 Article 9and Article 24 (72h pre-arrival information is exchanged on a voluntary base);
- Hazmat reports (information on carriage of dangerous or polluting goods) as per Directive 2002/59 as amended Article 4, Article 13 and Article 14;
- Incident reports (information on accidents and incidents which have occurred at sea) as per Directive 2002/59 as amended Article 16, Article 17 and Article 25, and Directive 2009/16 Article 23 and Article 25;
- Ship Reports (AIS, MRS and LRIT) as per Directive 2002/59 as amended Article 5, Article 6b, Article 9 and Article 23.

It is necessary that the information collected and exchanged through SafeSeaNet complies with the quality and performance standards defined in the IFCD.

The SSN system provides different alternative mechanisms to fulfil the mandatory system functionalities. These mechanism are described in section 2.5.2.

2.4 Additional system functionalities

SafeSeaNet provides for additional functionalities that are supporting its main operation. These functionalities are not considered mandatory, therefore should they become unavailable this would not affect the overall operation of the SafeSeaNet system.

The additional system functionalities are related but not limited to:

- statistics;
- graphical display of information;
- background information display (nautical charts, etc.);

- system monitoring tools;
- secondary or reference data sources (Location codes, SSN users contact details, ship particulars, special lists of ships).

Other additional functionality out of the ones listed above may become part of SafeSeaNet system if agreed at appropriate level among the SSN group, should the need arise.

2.5 SafeSeaNet Architecture

SafeSeaNet is accessible through different interfaces to the user's community, via the Internet and S-TESTA networks. It is designed to be available with a high level of reliability and security.

Following the Change Management Framework, SafeSeaNet interfaces are subject to upgrades, amendments and technical improvements, in order to keep the system updated, correctly implemented and to cope with continued evolution in the national, international or the Union's legislation.

2.5.1 SSN Network organisation

The SafeSeaNet relies on an architecture made upon two main levels:

- National SafeSeaNet system;
- Central SafeSeaNet system.

The LCA is a user that may act as data provider as well as data requester at local level. It is a recipient of the SSN information and feeds the SafeSeaNet system with information.

An NCA assumes on behalf of each participating country, the responsibility for SafeSeaNet management at national level. It is in charge of verifying and maintaining the national network and the procedures for complying with the requirements as described within the IFCD.

The mandatory information is provided by the National SSN systems in form of a notification to the Central SSN system that stores it. SSN users can retrieve information related to these notifications by requesting the Central SSN system. Additional details may be requested through the Central SSN system to the National SSN system. The Central SSN system is able to locate and retrieve this additional information and provides it to the data requestor.

The Figure 1 below describes the principles of the SSN system.

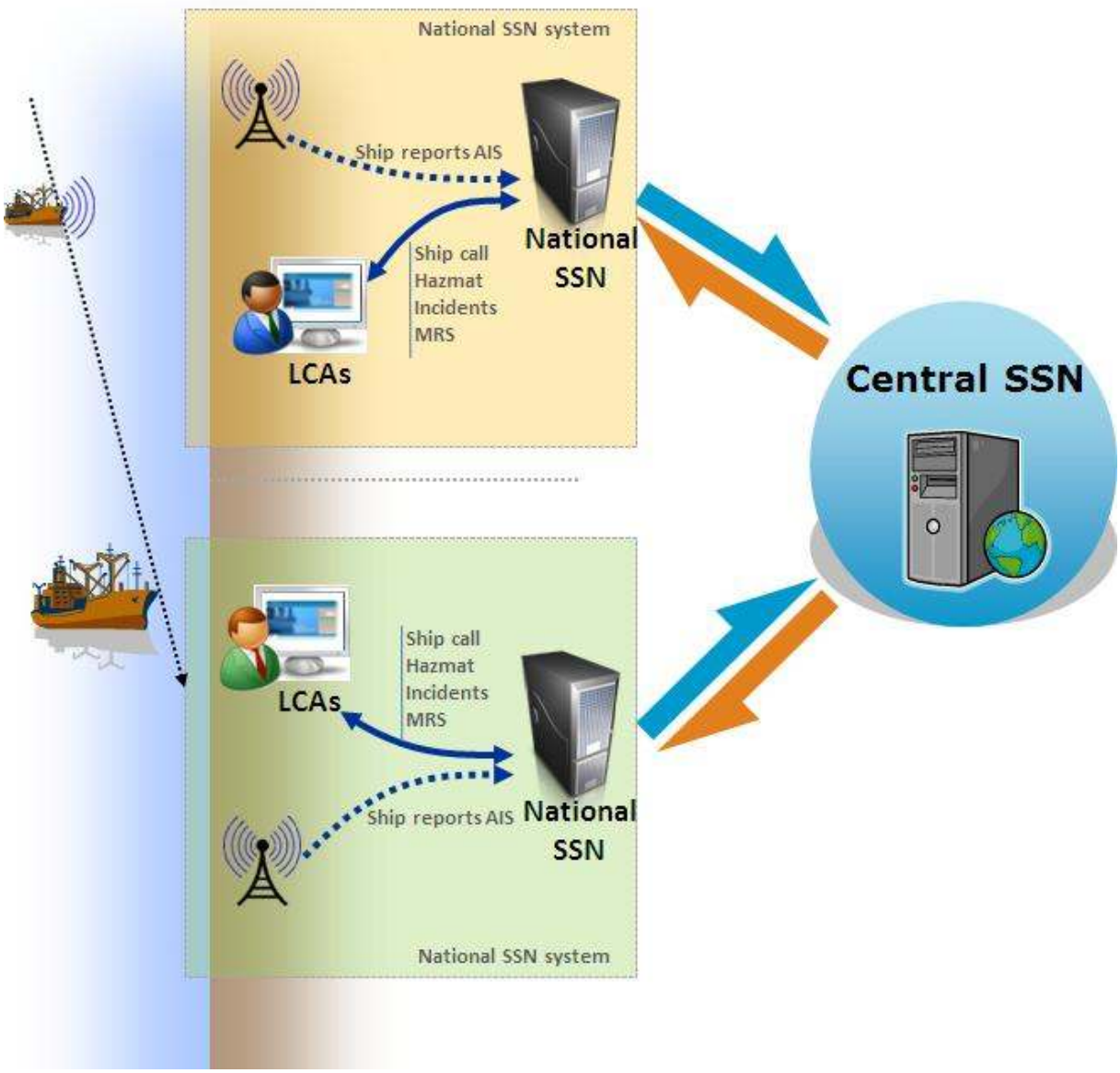

Figure 1 – SafeSeaNet system

While Central SSN system stores centrally some information which serves to respond rapidly and effectively to users requests, detailed factual information is stored at national level. Whenever the information changes (information added, updated, removed under certain conditions) an updated notification is provided by the relevant user; and the Central SSN is updated accordingly.

The NCA may decide to store details of the notifications at the National SSN system level, and answer the requests of detailed information without involving the respective systems at LCA level. Alternatively, details of notifications may be stored in the servers of the LCAs.

2.5.2 Information exchange mechanisms

Central SSN system provides to the National SSN systems different mechanisms to enable the exchange of information. These are:

I. **Message-based mechanism:** exchange mechanism based on individual messages exchanged between National and Central SSN applications. The messages, in XML format, fulfil the needs of both data requester and data provider (e.g. proprietary protocol, web-services etc.). This mechanism is available for notification, request, response.

II. **Streaming mechanism:** mechanism to enable constant real time exchange of AIS data based on predefined criteria between the National and Central SSN systems (either directly or through an AIS regional server). This mechanism is only available for providing AIS information and constitutes an alternative mechanism to the message-based.

III. **Central SSN Web browser-based mechanism:** available for requesting information, provide Incident Reports and may be used to provide information as a back-up solution in case of failure of the national or local SSN system. Also available for system administration.
The Central SSN Web browser-based mechanism has available two interfaces:
- **Textual interface:** provides direct access to Central SSN system, in a textual layout
- **Graphical interface:** provides access through a geographical information system technology to the ship positions enriched with the data indexed in Central SSN (information on pre-arrival, arrival, Hazmat cargo, incidents, etc.) creating a vessel traffic image of the vessels movements in real or near-real time.

Member States can choose the most appropriate interface that fits their national organisation and technical framework, in order to effectively connect to SafeSeaNet.

For notification purposes the message-based mechanism and the streaming mechanism are alternatives for providing Ship AIS information. The availability and performance standards hereafter will be applied to the communication mechanism each MS decides to utilise for the purposes of fulfilling directive obligations.

The table below lists the available mechanism for exchanging information through SSN.

SSN Mechanisms for information exchange		Message-Based	Streaming	Web Browser-Based	
				Textual interface	Graphical interface
Available for:	**Data Providing**	All information	Ship AIS information	Incident reports and In case of failure as a backup mechanism for all information	N.A
	Data Request	All information	N.A.	All information	All information

Table 1 – SSN mechanisms for information exchange

Regardless of the mechanism utilised by the National SSN system for data providing, the information shall be available through all mechanisms for data requesting. The transformation of the data provided will be performed automatically by the Central SSN system.

2.5.3 Messaging process

a) Message based mechanism:

- Notification
  - the *data provider* gathers the necessary information to be sent to SSN;
  - it sends a "notification" message to its National SSN system; then
    - the National SSN system compiles the message in the SSN compliant format; and
    - the National SSN system forwards it to the SSN;
  - on receipt the SSN determines whether the notification is well formatted and if so it stores it;
  - if not well formatted the notification is rejected by Central SSN system and the National SSN system should resend the corrected message.

- Request and response
  - the *data requester* sends a "request" message to its National SSN system;
  - the National SSN system then forwards it to the Central SSN system;
  - the Central SSN system determines whether the request shall be granted access to the requested information 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 available in MS national server (available through document download), SSN retrieves the information and forwards to the requester (via National SSN system);
    - for other information, SSN forwards the request to the National SSN system of the user where the requested information is located, which, in turn, forwards it to the end user that owns the information;
    - The *data provider* that owns the information then answers with the detailed information that is transmitted (via National SSN system) back to SSN that forwards it to the data requester.

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

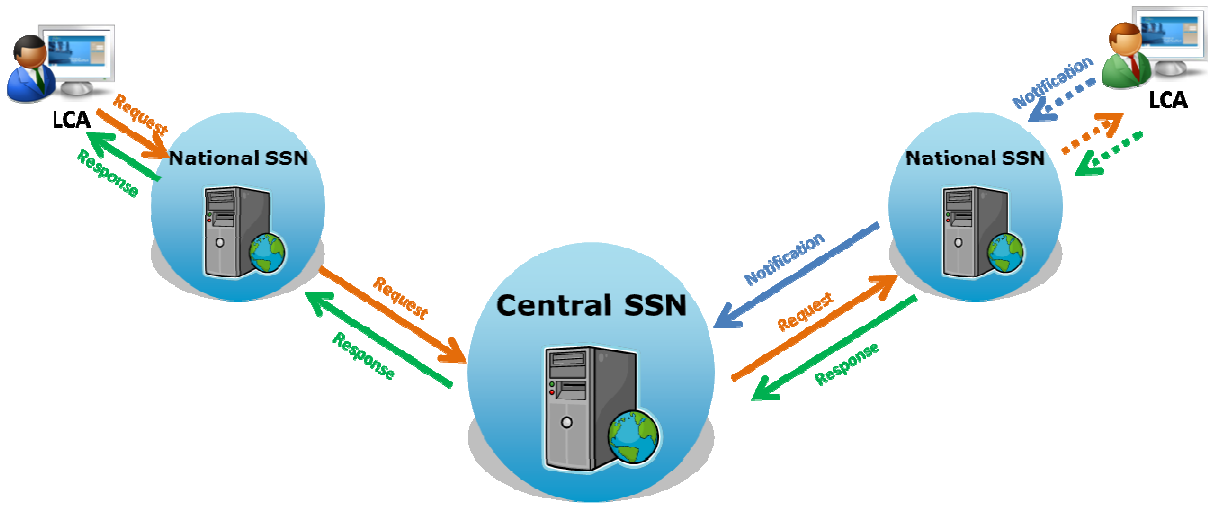

Figure 2 - Sequence diagram of notification, request and response mechanisms

b) Streaming mechanism:

The SafeSeaNet is equipped with a Streaming mechanism, a software process deployed at regional and national level to enable the exchange of AIS information from the AIS regional servers or National SSN systems to the Central SSN system.

The main function of the Streaming mechanism is to establish and manage the secured connection between an AIS regional server or National SSN system and the Central SSN system.

This mechanism was developed to enable the near real time exchange of ship positions originated from the AIS network.

2.6 Co-operation with other EU systems [7]

The Central SSN system interfaces with other EU systems for the purposes of integrated maritime policy subject to agreement regarding the access rights policy.
The current systems to which the Central SSN interfaces are:

- **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 in the Paris MoU. The system is pivotal in the daily PSC operations of all EU and non-EU member States of the Paris MoU. The entire process of port call registration, targeting, selection, reporting of inspections with

7 Action point 7 (IFCD#2 meeting): Send draft on section 2.6 'Co-operation with other EU systems' [Done]

corrective actions, publication of details and production of statistics as stipulated in the Directive 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. On the basis of Directive 2005/35/EC on ship sourced pollution, the CSN provides a monitoring service to national maritime administrations in EU coastal Member States, EFTA countries and candidate countries in their area of interest. On request CSN is providing the European Commission with services outside the waters of the before mentioned countries. CSN's main objectives are locating illegal oil discharges, identification of polluters, monitoring of accidental spills and the detection of vessels. The system offers analysis of satellite images, alerts on oil spills together with vessel detection and potential polluter information in near real time.

- **EU Long-Range Identification and Tracking Cooperative Datacentre (EU LRIT CDC)** – Following the adoption of amendments to the International Convention for the Safety of Life at Sea (SOLAS) introducing the Long-range identification and tracking of ships within Chapter V, the Council of the EU in its Resolution of 2 October 2007, agreed to the setting up of an European LRIT Data Centre managed by the Commission through the EMSA. Subject to the provision of 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 any charge, LRIT information in relation to the search and rescue of persons in distress. Following the dispositions of Directive 2002/59/EC as amended the Council agreed to make use of the SafeSeaNet system to facilitate the sharing of LRIT information between the MS and to fulfil the IMO requirements. The EU LRIT CDC is in operation since 04 June 2009.

- **LRIT EU Ship Database** – the EU Ship data base is a component of the EU LRIT CDC. The purpose of the ship data base is for the registration of ship instructed by their national administration to report to the EU LRIT CDC. The ship database is on line accessible by Administrations that are responsible for registering ships and updating the identification details as requested by SOLAS Chapter V/19.1. The ship database automatically transmits the updated data to the EU LRIT CDC.

The information exchange between the SSN system and other EU systems is made respecting the access rights policy defined in Chapter 3.
The co-operation between the Central SSN system and the other EU systems described above can be summarised as follows. The Figure 3 illustrates the information exchange between the systems.

- **SSN / THETIS:** the Central SSN system provides to the THETIS system the information received from the National SSN systems, concerning pre-arrival, arrival and departure information of any ship calling at an EU port or anchorage, together with an identifier of the port concerned.

- **SSN / CSN:** the Central SSN system provides to the CSN system the ship positions and identifiers (transmitted by the national AIS network) in order to allow the identification of vessels and possible polluters (within a limited timeframe and area).

- **SSN / EU LRIT DC:** Data stream of LRIT information is established between the EU LRIT CDC and the SSN system. EU Member States can visualize the LRIT information they are entitled to receive.

- **SSN / EU LRIT Ship database:** An interface is established between the SSN database and EU LRIT ship database for the purpose of enrichment of ship information detained in the SSN system. The ship information registered within the LRIT Ship database (master database) is regularly communicated to the SSN data base for crosschecking with ship information received from other applications.

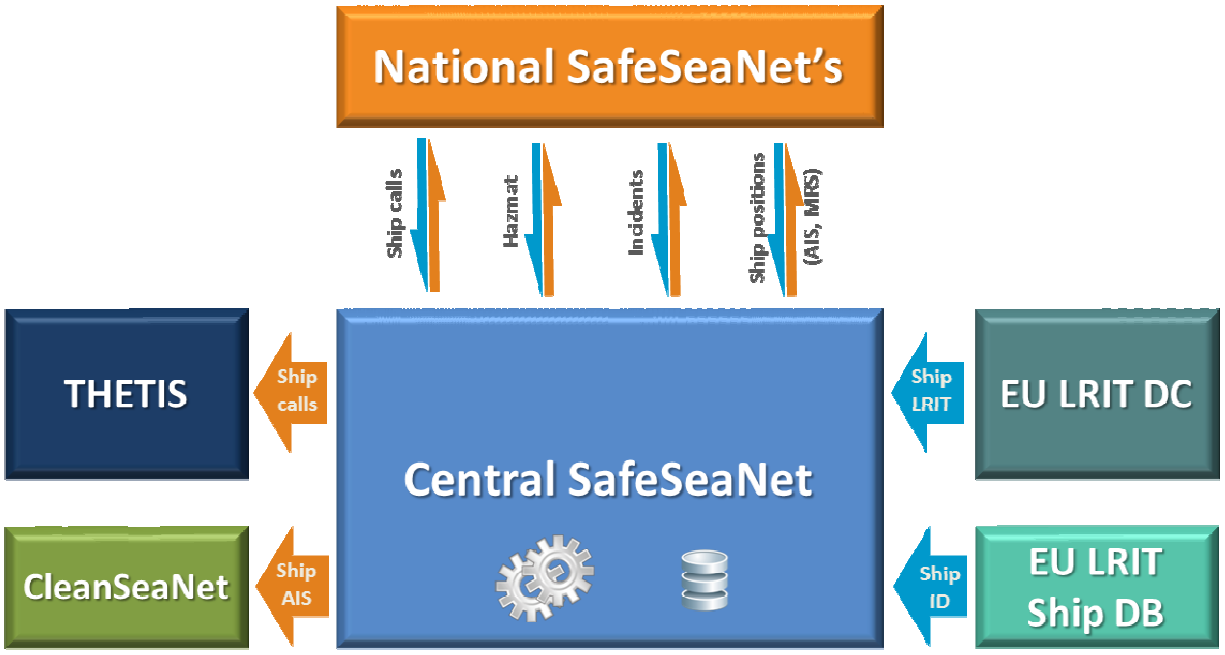

Figure 3 – Central SSN system interfaces with other EU systems

2.7 Other general requirements

The SSN system complies with the following requirements, regarding all information provided by the NCA or LCA. Hereunder, the owner of the information is the NCA or LCA who has provided the information to SSN

Reliability - SSN guaranties that the information is available, accessible and usable in the defined conditions (conditions regarding the availability of the environment are defined at chapter 4.3 and conditions regarding data storage are defined in chapter 4.4).

Confidentiality - SSN guaranties that information is shared only among authorized persons or organisations (e.g. the information can be accessed only by the owner of the information or by accepted users at moment agreed by the owner).
The level of confidentiality is defined for each category of information in chapter 7.2 (accepted users, interfaces where the information is accessible, duration when the information is accessible).

Integrity - SSN guaranties that the information is authentic and complete.
The information stored in the Central SSN system is not modified unless by:

- its owner;
- the NCA covering the owner;
- Central SSN system, according to rule or procedure defined in the SSN documentation.

Traceability - SSN gives the possibility to verify the history, location, or application of the information by means of documented recorded identification.
The following actions are traced by the Central SSN system (user identification, time stamp, description of action) and made available to the owner of the information at all time:

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

The requirements above are translated into measures to be applied to the whole SSN system. They are listed in chapter 7.

Chapter 3 - Roles and Responsibilities

Scope: *Defines the users, their roles and the related access rights policy in terms of specific data distribution rules;*

Source: *Directive 2002/59 EC + amendments, HLSG Access Rights Policy*

3.1 General provisions

3.2 Rules for data distribution

3.3 User management including access rights

3.4 Definition of functional roles

3.4.1 System Administrators

3.4.2 Data Provider

3.4.3 Data Requester

3.5 Definition of users and user groups

3.5.1 Designation of users

3.5.2 Parties involved

3.5.3 Responsibilities of users

3.5.4 European Union Institutions and Agencies

3.5.5 Member States authorities

3.5.6 MS overseas departments and territories

3.5.7 Third Countries

3.6 Specific needs

(e.g. studies or research projects, pilot projects)

3.7 Regional collaboration

Chapter 4 - SafeSeaNet Performance [8]

Scope: *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 elements of SafeSeaNet.*

Source: *ICD+ amendments, Network and Security Reference Guide + LRIT requirements*

2.3.1 Information reported
2.3.2 Physical flows
2.3.3 Storage of data
7.2.4.4 Information Archival and Retrieval
7.2.5.6 Access to Archived Information
7.2.4 System timing and performance
7.2.5.3 Additional Timing Requirements
7.2.3 Availability of the SSN system
7.2.5.1 Availability
7.2.4.3 Backup Provisions
7.2.5 Performance requirements
7.2.5.5 Processing Time
5.2.5 Communication requirements

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 within 1 minute between the two systems.

SSN data requesters should receive the information requested through SSN within 4 minutes of the request**9**.

The timeframes above should be respected for 95% of the information exchange over any 24h period and for 99% of the cases over a one year period.

The NCAs should respond to requests for archived data as per point 4.2 below within 5 working days.

8 Action point 8 (IFCD#2 meeting): Send a 'clean' version of chapter 4 [Done]
9 Action point 9 (IFCD#2 meeting): Confirm the timeframes for the information exchange [Done]

4.2 Timeframes for data storage[10]

The data shall be available through the SSN system:

a) five (5) years minimum for data related to incidents and accidents; and
b) two (2) months minimum for data relating to port (from ship departure) and ship notifications.

The above data should be archived for at least five (5) years, down-sampled when necessary. The archived data should be made available upon request by another NCA or EMSA. This type of data would be used for purposes such as statistical analysis or studies on traffic flows.

4.3 System availability requirements

System availability is the availability of the hardware and software necessary for the performance of the mandatory functionalities of the SSN system as per Chapter 2 - SafeSeaNet Overview.

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

Availability of the SSN system shall be maintained at 99% 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 provisions

Backup procedures should be implemented on each SafeSeaNet system component for the event of a failure or in case of a scheduled interruption.

The NCA shall ensure that the SSN messages are stored and transmitted to the Central SSN system when communications and/or systems are recovered. The National and Central SSN systems should be able to resend messages for up to 30 days.

The body in charge of the SSN affected system component must be capable of informing other participants in the SafeSeaNet system using the operational procedure referred to in Chapter 5 - and in the SSN Handbook.

10 Action point 10 (IFCD#2 meeting): Confirm the timeframes for data storage [Done]

4.5 Additional system performance requirements

Invalid messages (those not compliant with standards set in the SSN interface reference guide) should be less than 0,1%.

When the Central SSN system receives an invalid message, an error message shall be produced and forwarded to the National SSN system.

When Central SSN system transmits an invalid message, the National SSN system should inform the EMSA MSS as soon as possible.

4.6 Data quality

MSs should introduce in all components of the system the automatic data quality rules agreed by the SSN Group.

Reports missing (that should have been provided in accordance with the SSN legal requirements) should be less than 0,1% per type.

MSs should put in place, in cooperation with EMSA, the appropriate control mechanisms to investigate data quality issues that affect more than 0,1% of the reports per country and type (as per chapter 2.3) per month.

4.7 Network coordination

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

EMSA provides a 24/7 monitoring of requirements and network coordination and helpdesk for the SSN system.

Monitoring procedures and operational communication procedures among the NCA 24/7 and between these and EMSA 24/7 should be agreed at the level of the SSN Group within the framework chapter 5 below.

Chapter 5 - Operational Services and Procedures [11]

Scope: *Covers the services and operational procedures and best practices maintained by both the Central and National SSN systems;*

Source: *ICD + amendments, SSN Handbook*
7.2.1 – Overview

5.1 Overview

The standards contained in this chapter provide a framework for the functions of the National SSN systems and the Central SSN system, including the transmission of messages, performance levels and operating procedures.

SafeSeaNet is organized to ensure:

a) Speed (timely exchange of messages);
b) Reliability (distribution of message and system information in the event of failure of communication link or other);
c) Accuracy (correctness of information delivered);
d) Efficiency (economic and smooth flow of message);
e) Accountability (tracking of messages in the system);
f) Security (confidentiality and authenticity).

National SSN systems that meet the specified standards of performance are commissioned to operate within the SafeSeaNet system.

5.2 Operational Services[12]

5.2.1 Continuity of services

Continuity of services involves the evaluation of values, threats, risks, vulnerabilities and development of countermeasures to ensure continuation in the event of a disaster[13].

The NCAs responsible for the management of the national SSN systems as well as EMSA, responsible for the Central SSN system should ~~The Central and National SSN systems must~~ ensure that a Business Continuity Plan (BCP) is in place. The BCP ~~must~~ should, at the minimum, contain an outline of the approach to ensure the continuity of services in the case of disaster/ unexpected events. The BCP ~~must~~ should cover the ~~essential~~

11 Action point 11 (IFCD#2 meeting): Send a revised draft of chapter 5, based on the comments received during meeting [EMSA]

12 **SE:** What is meant by op. services and who are the services for? the chapter describes services to users, NCAs and database managements? Very unclear what the purpose of this section is?
The whole section needs to be reviewed. Some issues have already been mentioned

13 **SE:** Not a very good word...meaning catastrophe or technical breakdown? They can both be disastrous...
NL: What is a disaster?

mandatory functionalitiess (listed in Chapter 2.3) and apply risk reduction or recovery options in case of disaster/ unexpected failures of the system.**14**

Example: Business Continuity Plan on the National level cover, for example, the following situation: National SafeSeaNet system is down. Responsible MS executes rollout of the backup procedures for ensuring that information about the cargo carried onboard of reported ships will be available for other SSN participants when e.g. calling a designated service/ person in case of emergency.

The objectives set for the Continuity of services are:

- Meeting requirements of the availability of the Nnational SSN systems (as specified in the Chapter 4 - SafeSeaNet Performance);
- Ensuring, by means of the backup procedures (given in 4.4 - Backup provisions), that information required by the dDirective can be still available;
- Ensuringe that information is recovered after anythe period of the down-time period/ disaster/ failure.

In order to ensure the continuity of service of SSN, MSs should establish a permanent service at the National Competent Authorityics (the NCA 24/7 further in the document) and which is further described in the sectionpoint 5.2.3 - System support services. The same 24/7 service is established at central level by the EMSA Maritime Support Services (MSS).

Theose NCA 24/7 services should also be responsible for executing of SSN operational procedures which will covering e.g. countermeasures to ensure continuation of the mandatory functionalities in the event of a disaster system breakdown and may perform some of the functions described hereafter.**15**

14 **UK:** the specific requirement for a BCP is new and while we are committed to ensuring Business Continuity we are unclear that this is a helpful approach as the SSN functions are integrated into the wider operations of various authorities and so also Business Continuity provisions will similarly be integrated within the general BCPs maintained for each authority. Also depending on the situation that is being recovered from it may well be the case that the maintenance of SSN reporting is not a possible or a priority. If this becomes a requirement will the Central SSN BCP be made available to MS

EMSA: we are currently implementing a BCP for the Central SSN system. This is a proposal to be discussed. Some back-up procedures were discussed within the SSN WG operations already.

SE: Rephrase

15 **SE:** Rephrase

5.2.2 Reference Databases' management[16]

Reference Databases are those that are used on the local level to support reporting obligations. Non–exhaustive list of those databases includes: location codes database (LOCODES), ship database, users database, dangerous and polluting goods database~~etc~~**17**.

Data exchanged in the SSN system should be coherent and of the best possible quality. To ~~Therefore, each SSN participant~~**18** ~~should maintain and keep updated local databases which will~~ **19** be used by the data providers (~~masters, operators, agents etc~~.) as a reference, when notifications required by the Directive are provided to the competent authorities.

Example: Examples of the use of local databases - Master notifying departure of the vessel with dangerous or pollution goods (HAZMAT) on board should have access to the reference database which will include a list of HAZMAT cargoes. The master should also have access the list of locations LOCODES to give the proper reference to the destination port.
Coastal station reporting incident of the vessel in their area of responsibility should have access to the reference database, which will provide correct and up-to-date identifiers of the vessel.

5.2.3 System support services 20

Member States must guarantee that an effective exchange of the information referred to in the Directive takes place on the national level.

This must be executed by means of the designated **NCA 24/7** services, which will cover at least the following services on a 24/7 basis:**21**

---

16 **UK:** we accept the importance of data quality – but do not believe that the ways of achieving it should be prescribed

SE: agrees with some of the content, but...the big problem about databases is that there are too many local databases which confuses the users (masters especially who travel between MSs). EMSA is today providing the MSs with the latest UN Locodes also with SSN specific codes. SE proposes that EMSA is given the task to provide MSs with some of these databases e.g. HAZMAT-lists. This would mean that all MSs have the same list in their national systems when a HAZMAT-notification should be made by the master. Today some products are NOT considered to be HAZMAT in some MSs. IMO is also updating some lists regularly which means that this issue needs to be administered by someone – preferably EMSA.

17 **UK:** see above comment on the use of 'etc'

18 **FR:** and Central SSN

19 **UK:** we accept the importance of data quality – but do not believe that the ways of achieving it should be prescribed

20 **SE:** Unnecessary since this has already been mentioned before. (Or move to this section?) Anyway it needs to be reviewed and rephrased.

21 **UK:** we would want clarification on which of these services actually have to be carried out on a 24/7 basis – for example we see no requirement for "providing feedback to the development teams" to be a 24/7 function

FR: the list below apparently comes from the report of the working group on SSN operations (SSN12). In the document, the list included whether each individual service would be done on a 24/7 or not. A priority was provided. In addition, it was decided that implementation would be done on a voluntary basis. Suggestion to reuse the document here

EMSA: list redrafted based on the report of the working group on SSN operations (SSN12)

- Notify the SSN on a continuous basis**22** (provide service according to the requirements defined in Chapter 4 - SafeSeaNet Performance);
- Respond to direct request of information from SSN: MS are obliged to respond to any request according to the agreed response times**23**;
- Backup solution for providing information to SSN users in case the national system or connection failures;
- To ensure that all messages, received or transferred through its system are transmitted to SSN**24**;
- ~~Manage reference database at National level;~~
- ~~Manage Users at National level;~~
- ~~Manage LOCODE Database at National level;~~
- SSN Incident Report Distribution service at National level: incident reports received from another MS should be distributed among the relevant ~~NCA/~~LCA within the country**25**;
- ~~System assessment regarding the quality of the information provided by the National SSN system;~~
- ~~Providing feedback to the development teams;~~
- ~~Providing off-line (historical) data based on SSN request (data which is not automatically available via SSN);~~
- Monitor the performance of the communication system within its service area to determine degradation of its operational capability;
- Monitor the data providers communication links. The communication links should be monitored;
- Monitor its own operation to ensure availability and to avoid the distribution of unreliable or corrupted messages;
- Immediately notify the MSS in case of unavailability to receive, process or transmit data according the IFCD specifications;
- Reception and distribution of reported technical failures from the MSS in EMSA to its national users **26** (failures in another MS or in the SSN application/ hardware/ network);
- Provide support to users at National level.**27**

The NCA 24/7 (or NCA itself) should also be ensure the additional non time critical SSN related services:

- Manage reference database at National level;
- Manage Users at National level;
- Manage LOCODE Database at National level;

---

22 **FR:** unclear. This is a functionality of the national SSN system. Not a service of the national support service. Suggestion to remove

23 **FR:** where is this obligation? To be defined and be agreed with the MS (HLSG)

24 **FR:** unclear. This is not a service as such but a requirement. Suggestion to remove

25 **FR:** distribution to the relevant NCA should be done by SSN

26 **FR:** this sounds redundant with bullet 8

EMSA: the previous bullet is regarding failures at national level that the NCA 24/7 should inform MSS. This bullet is to inform the national users of any reported failure in SSN

27 **FR:** support of national users is the responsibility of the MS. This is out of scope of the IFCD.

- System assessment regarding the quality of the information provided by the National SSN system;
- Providing feedback to the development teams**28**;
- Providing off-line (historical) data based on SSN request (data which is not automatically available via SSN).

According to the definition given in Chapter 1, EMSA, on behalf of the European Commission is responsible for the management of the SafeSeaNet central system**29**. It includes: monitoring of the continuity of service on central level and connections with Member States, monitoring and reporting on data quality and availability, IT and engineering support restricted to the user interfaces and communication interfaces with SafeSeaNet. EMSA executes those duties using its 24 hour-a-day operational service – **Maritime Support Services (MSS)30.**

5.3 Operational Procedures31

In order to follow requirements of the IFCD, the SSN group has agreed on a set of detailed operational procedures.

Those procedures cover multiple aspects/ chapters of the IFCD and they form so called "SafeSeaNet Handbook" document.

*Comment: to be decided if the above procedures need to be listed in the IFCD or if it enough to keep the above definition.**32***

---

28 **FR:** unclear. If that is the SSN development team, then this is done by the SSN group or the MSS. If that is the national development team, then this is out of scope of the IFCD

29 **UK:** there seems to be a confusing use of the term "the SSN System" throughout the document - sometimes it seems to be the just the Central system and sometimes it seem to encompass both Central and National – and particularly we are not clear of the scope of the term in this case

EMSA: it refers management of the central system but some monitoring tasks on the links to the national systems as explain within the paragraph

30 **FR:** the same approach with a list as above should be applied to the MSS

EMSA: detailed list for the MSS to be included

31 **FR:** suggestion to replace that chapter with the list of procedures from the Working Group on SSN operations

SE: This is confusing – this is the IFCD. If the SSN group has agreed on something maybe it is too detailed to be mentioned here? Maybe we should only describe the operational responsibilities of each user/authority? The whole section needs to be further discussed.

32 **UK:** from the paper at SSN 14 and the discussions at the HLSG the UK understand was that the IFCD was going to absorb most of the other SSN documents – however this version of the document seems to be set out on a different route, with all the other documents remaining extant. Although the UK does not have a firm view of which is the most effective route, we would be concerned about the whole governance of this project if at this early stage we are already acting counter to the direction given by HLSG

EMSA: to be discussed: The view of EMSA is that the IFCD should not "absorb" all the other SSN documents but be an intermediate step between the "user requirements" in the directive" and the more than 500 pages of detailed specifications in the SSN documentation; It should contain as its name indicates the "functional requirements"

5.3.1 Communication Procedures

NCAs have to ensure that there are means in place at national level, which will cover reliable and secure communication with data providers and/or data requestors.

For that purpose:

- the data security and protection policy should be implemented and executed, and
- proper identification of the data providers and requestors should also be ensured when data is exchanged electronically but also when information is requested using traditional communication is means e.g. phone, fax, e-mail.**33**

Regarding Central SSN system and its connections with the National SSN systems, the communication procedures for reliable and secure connections are defined in the Network and Security Reference Guide document.

5.3.2 LOCODEs management procedures

Location Code List (LOCODE) is the location defined as any named geographical place, recognized by a competent national body, either with permanent facilities used for goods movement associated with trade, and used for these purposes, or proposed by the government concerned or by a competent national or international organization for inclusion in the UN/LOCODE.

A five-character code element is provided for each location included UN/LOCODE and consists of:

> a) two letters identifying the country, according to the ISO 3166 two-letter Code for the representation of names of countries, and UN/ECE/FAL recommendation No. 3, and
> b) three characters identifying the location within the country. The code system may be referred to as the "United Nations LOCODE" (UN/LOCODE).

The identification in a unique and unambiguous way of any place involved in international trade is therefore an essential element for the facilitation of trade procedures and documentation.

Each NCA (According to Annex III of Directive 2002/59) is responsible for maintaining up to date lists of its own active ports and to recognise or propose any named geographical place as a location for inclusion as a UN/LOCODE in order to ensure that these locations are designated.

The SSN LOCODE list includes the following types of LOCODEs:

33 **UK:** will any minimum standards be defined for this?
EMSA: in the case of exchanged electronically is already defined (user ID). For phone, fax, e-mail the SSN WG operations discussed over this and concluded that the "cross-border" communications would only be between NCAs and with the MSS and therefore facilitating the identification of the e-mail, telephone of fax requiring from a common "contact list"

- UN/LOCODEs, included in the last version available of the UNECE list with port function (3);
- "SSN Specific LOCODE", additional codes for use within SSN that are not formally recognised in the UNECE list ("ZZUKN", "ZZCAN" and way points "XZ") or that are in the process of being recognised.

EMSA is responsible for the management of the SSN Specific LOCODES list.**34**

5.3.3 Inconsistencies management

For the purpose of data quality, Maritime Support Services perform regular check of the data quality and report inconsistencies to Member States' NCAs, to the SSN group and to the HLSG.

Member States NCAs must perform regular data quality check of the information provided by their data providers and maintain procedures which will allow quick and efficient correction of the inconsistent data.

Reported inconsistencies should be corrected without delay**35** if the information can still be of operational use and the causes for the inconsistency should be analysed and rectified.

5.3.4 Early warning procedures

SafeSeaNet system provides number early warning services (e.g. banned vessel detection or SHT detection warnings) as well as the "ship of interest" tracking and reporting. Member States NCAs should implement procedures to disseminate agreed early warnings to the parties concerned**36**.

---

34 **UK:** remains concerned about the use of SSN Specific LOCODEs – we feel that many of those in use add no value in terms of data quality and serve only to confuse the end users of the data

EMSA: to be discussed. The UNECE list is only updated once a year (some years without new version). The process to include a new locode in UNECE lists is too long

FR: why detail this here? Suggestion to remove that part

35 **UK:** committed to improving the data quality within SSN however we question the value of this requirement – often the inconsistencies are reported to the NCA days after the voyage and while we see the value in investigating and understanding the reason for the issue to prevent reoccurrence we see no value in resending a time expired notification

EMSA: if a MS consider not relevant resending a time expired notification, the general rule could be nuanced

36 **FR:** not very clear

EMSA: propose redraft

5.3.5 Handling of exemptions

The Member States which decide to implement the exemptions have to follow procedures allowing companies, meeting criteria of the Article 15 of the Directive, to register exemptions from reporting obligations. At the same time the NCAs has to ensure that the conditions for exemptions are maintained and that data listed in Annex I is available upon request.**37**

37 **UK:** what is point of statement such as this which does not add anything to our understanding of the directive?

FR: a procedure should be established?

EMSA: consider redrafting to include the SSN functionality supporting this requirement

Chapter 6 - System management and Tests

Scope: *Describes the testing procedures and rules, changes to the system's status and the procedures for performing commissioning tests;*

Source: *Change management Framework, MS Commissioning Test Plan, Procedures for new developments*
Source: ICD+ amendments

6.1 System Status Change

System status changes (Central and National SSN systems) are the result of system element and system function failures, scheduled maintenance, integration or testing of new system elements.

All changes of system status that would impact on the working of any component of the SafeSeaNet system will be notified by the NCA 24/7 to EMSA's Maritime Support Services (MSS) that shall inform the SSN user's community. The same procedure shall be applicable to system status changes of the Central SSN system. The MSS shall inform**38** the NCA24/7 that shall inform the user community at national level (LCAs).

The procedures for communication of system status change to ensure the proper information flow between data provider and SSN users are defined in the SSN Handbook document.**39**

6.1.1 Changes of Operational Capabilities

Changes in operational capabilities resulting from new equipment or new/update system software which impact upon the operation of the SafeSeaNet should be notified by

38 **NL:** At least a day in advance

39 **FR:** EMSA should ensure proper information of every SSN user. We suggest a dedicated web page indicating the status of each NCA and LCA systems and the scheduled back to normal
EMSA: proposal to be considered

EMSA's MSS to the concerned participants. The system administrator will provide advance notification as defined in the SSN Handbook document.**40**

6.1.2 System Failure

System status changes resulting from either a failure of a system element or a system function will be reported as soon as possible to SafeSeaNet users by the NCA 24/7 and MSS.

6.1.3 Scheduled Outage

System change status for any system element or function, which results from scheduled outages for maintenance, integration or testing, will be notified by the responsible NCA to all LCAs. The responsible NCA should provide advance notification as early as possible before interrupting operations, including a description of the planned arrangements taken, if any.

The same procedure shall be applicable to the Central SSN system, for which the EMSA MSS has the responsibility to inform the NCAs 24/7.

6.2 System Commissioning

This chapter provides guidance on principles governing the performance of tests which Member States will endeavour to implement for the purpose of ensuring efficient system operations.**41**

The commissioning process is required to ensure that the NCA provides for reliable, timely and accurate exchange of data and system information within the SSN network The Commissioning process is defined in the document MS Commissioning Tests Plan.

The commissioning process covers all the SSN exchange of information available through the SafeSeaNet interfaces.

If in the future alternative technical means are considered to transmit information to SSN, the new tests shall be incorporated in the MS Commissioning Test report following the same procedure.

---

40 **UK:** we would like to see much more detail on this

EMSA: proposal for more detail should consider what can be left for the relevant part in SSN Handbook

41 **UK:** it is unclear why the rare event of Commissioning is described in detail but the regular event of "System Status Change" is not.

What is missing is the level of change the prompts the need for commissioning. Also we would like there to be a process whereby changes to the EIS are formally validated while on Training environment to ensure that connections with all National systems remain valid before the change is applied to Production

FR: suggestion to describe the details and procedures regarding commissioning in a specific document. General principles only should be included in the IFCD.

EMSA: consider to redraft and reduce the level of detail

6.2.1 General guidance

Before entering into the production site of the SafeSeaNet system, an NCA shall perform commissioning tests and provide the data, which is specified in the document "MS Commissioning Tests Plan" to the SafeSeaNet system manager (EMSA). The commissioning tests verify that the system developed by a Member State is able to provide and receive messages exchanged between users in accordance with the system specification.

6.2.2 Test Plan[42]

A test plan is described in the document MS Commissioning Test Plan. The objective of this document is to recommend and describe the testing strategies to be employed by users to:

- Identify the functional requirements as target for testing;
- Recommend and describe the testing strategies to be employed;
- Identify the required resources;
- Recommend and describe the test organisation;
- Present a list of tests scenarios to execute; and
- Provide a support for test and bug reporting.

The tests to be performed, test data to be delivered and the reporting requirements from SSN management to analyse and evaluate the testing results are all indicated in this document and its addendums.

6.2.3 General commissioning procedure

The commissioning is performed at the request of a Member State. For that a formal request is forwarded to EMSA's Maritime Support Services in order to get an appointment for performing the commissioning.

The tests are performed by the Member State. At any time prior or during the commissioning tests, the Member State may request EMSA support. The request should be addressed to EMSA's Maritime Support Services.

The results of the tests shall be documented in a test report. The test report and the data files (if any) are submitted to EMSA for revision.

EMSA shall analyse and evaluate the test report and if test results comply with SafeSeaNet requirements, EMSA validates the results.

Member States may perform a part or parts of the tests and gain approval on those parts of the system. In cases where Member States take this option, they still must undergo

42 **FR:** test plan should be validated by SSN Group?
EMSA: the MS commissioning test plan is part of the SSN documentation and is validated by the SSN group

tests for the remaining part of the system requirements before they can use them in production.

6.2.4 Pre-Commissioning tests advance notice

Prior to commencing the commissioning test, the NCA shall give advance notice of the action intended to the EMSA's Maritime Support Services. At this stage, the NCA should review the SSN Handbook for commissioning test procedure and check if all the conditions to initiate the testing phase are met. This is important to organize and execute properly the commissioning tests.

6.2.5 Submission of results – Integration

The results of the commissioning test shall be documented in a test report. It shall include a test cycle report drafted by the test manager in accordance with the test plan and also a bug report.

The complete report and the data files (if any) shall be submitted to the to the EMSA's Maritime Support Services for further evaluation. If the tests are considered accepted, EMSA issues a test acceptance form and updates the status of operation of the Member State. In this process the Member States becomes officially recognized participants in the SafeSeaNet network.

The result is then communicated to SSN Group: a new member has passed commissioning tests and will become integrated in the SSN network with the possibility to exchange maritime information.

During the first period of integration, EMSA's MSS will closely follow its activity to ensure that a Member State is entering the production site of SSN with all required data. A report will be issued to the Member State with feedback on the quality of the information provided.

6.3 Further developments and planning

The SSN group is responsible for developing the system to integrated added value functionalities[43] and new requirements arising from legal requirements.

The implementation of the new developments at national and central level requires a close coordination. With this objective, the SafeSeaNet Change Management Framework document is defined.

The purpose of the SafeSeaNet Change Management Framework (CMF) is to define and control the process by which changes to the SafeSeaNet are introduced, coordinated and

43 **UK:** this is only true if the HLSG has directed the group to carry out a specific item of work – the SSN Group's only ongoing responsibility is to ensure that SSN allows Member States to fulfil their legal obligations

decided. This framework applies to all parties to the SafeSeaNet system including EMSA and the participating Member States.

The objective of this document is to**44**:

- Establish a formalised and binding process by which changes to the SafeSeaNet system are introduced, coordinated and evaluated;
- Identify the actors involved in the Change Management Process (CMP), along with each actor's roles and responsibilities within the CMP;
- Determine methods for classifying and prioritising change proposals;**45**
- Establish documentation and reporting standards for the purposes of providing an appropriate measure of accountability for each instance of the CMP.

Amendments to this document will entail cooperation between EMSA and the participating Member States. SafeSeaNet's CMF will, in fact, be invoked in order to coordinate modifications to the Change Management Process itself. Changes to the CMF will be proposed by EMSA or the participating Member States to the SSN group.**46**

6.3.1 Change management and scope

The CMF will be invoked in all cases where a proposed change will impact the SafeSeaNet system's specifications and hence the Member States' national SafeSeaNet implementations.

Changes to the following SafeSeaNet system documents are of particular relevance to the CMF:

- SSN Communication Interface Document**47**;
- Network and Security Reference Guide.

The CMF will not be ~~invoked~~applied**48** under the following conditions:

44 **FR:** rather than a presentation of the document, the high level principles should be explained here
EMSA: propose redraft

45 **UK:** this is an area of concern for the UK as it seems that EMSA has often classified changes as minor without any awareness or consultation with MS about the impact on National systems. MS have then found themselves subject to criticism when following the change there has been a disruption to their provision of data to the central system

46 **UK:** believe that the HLSG should be the owners of the Change Management Framework
EMSA: this is a technical and operational document. The system further developments are arising from legal requirements or from HLSG. The main lines for the change management should be in the IFCD. The CMF is within the scope of the SSN group

47 **FR:** this document is not listed in §1,6. The XML reference guide and the SSN Web Interface User Manual should be included. As a general: any changes that affect the IFCD should be covered by the CMF.
EMSA: document renamed to SSN Interface Reference Guide

- Changes applicable to EMSA's internal organisation and/or operation;
- Changes proved**49** to have no effect on the Member States' national SSN implementation;
- The CMF cannot be deployed to block changes to the SSN programme that result from commission directives or legal obligations.**50**

6.3.2 Change management process**51**

An effective CMF seeks a balance between accountability and flexibility. On the one hand, the process must be able to identify actors and responsibilities, set timelines, mandate due diligence, etc. On the other hand, the presence of a formal CMF should not discourage the on-going contribution of ideas to SafeSeaNet**52**. It must have the scalability to bring control mechanisms to bear in proportion to the size and/or complexity of the proposed change. In all instances, change proposals should be communicated to all participants.

The CMF will act as the over-arching guide for effecting change to the SafeSeaNet programme within the defined scope. The CMF will be the process by which consensus approval among participating Member States will be sought in relation to changes proposed for SafeSeaNet. It will ensure that all on-going change proposals are given a high degree of visibility within the SafeSeaNet community, and will serve to solicit opinions and suggestions from as many perspectives as it might take to render a balanced decision with regards to the change request itself.

The CMF is a step-by-step guide that provides a standard structure for each instance of the Change Management Process.

---

48 **FR:** propose 'applied'

49 **UK:** following on from comment about - How will this be proved?

EMSA: changes that do not have an impact on the national SSN systems (e.g. web interface)

FR: unclear. This could be in contradiction with the IFCD (changes which would have an effect on SSN performance or SSN network structure for instance)

50 **UK:** while we agree with this in principle it is only a valid statement if the CMF is taken into account when commission directives or legal obligations that will require changes to SSN are introduced, ie when the implementation timescales are agreed they must have due consideration of the CMF

EMSA: agreed but this is for COM and COUNCIL to take into account

FR: unclear. What does 'deployed to block' stands for?

EMSA: changes in SSN coming from commission directives or legal obligations cannot be block by the CMF

51 **FR:** too detailed? This should be in the CMF

52 **UK:** one of the key areas which would need to be included is the use of pilot projects – and in particular the way in which the success of such projects is assessed before any decision on wider roll out is taken

EMSA: reference to pilot projects to be included

Chapter 7 - System Security

Scope: *Reflects upon the outcomes of the security study EMSA is launching and provides the users with clarifications on security related terminology, policies and procedures;*

Source: *Follow-up of the "Study on SSN network and information security, data protection and confidentiality" (to be launched mid-2010)*

7.1 Terms and guidelines

7.2 Security management policy

7.2.1 Data classification

7.2.2 Data exchange

7.2.3 Archiving of information

7.2.4 Standardised accrediting scheme

7.2.5 Business continuity processes

7.2.6 Security policy for further developments

7.2.7 Management of removable media and data loss prevention