SAFESEANET

Interface and Functionalities Control Document

SSN IFCD

Version: 0.01

Date: 11 January 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)

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

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 SafeSeaNet central 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.

Include here reference to the entire legal framework associated to SSN. The details will be in chapter 2[1]

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

1 Action point 1 (IFCD#1 meeting): Include Legal Framework [EMSA]

Chapter 1 - Introduction

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 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 and future systems. It describes the operational services and procedures, along with information on system performance in terms of data handling, timing, availability and performance requirements. It also provides information on, data quality control, system management, testing and security.

It should be noted that 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 documentation (please refer to section 1.6), and the IFCD contains references where appropriate.

1.3 IFCD Structure

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

- Chapter 1 "Introduction" introduces the IFCD and 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 there are general indications of the system functionalities and features.);
- Chapter 3 "Roles and Responsibilities" defines the users, their roles and the related access rights policy in terms of specific data distribution rules;

- 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 testing procedures and rules, the changes to the system's status and the procedures for performing commissioning tests;
- Chapter 7 "System Security" provides the users with clarifications on security related terminology, policies and procedures.

Each page of the document includes in its header:

- Version Number;
- Date of issue.

The Summary of Amendments is updated with each new revision. Users of the SafeSeaNet system should ensure that their copy of the document includes all the revisions issued, as indicated in the Summary of Amendments page that precedes this section.

1.4 IFCD Administration

The HLSG (group composed of Member States and the Commission) is responsible for approving and for any further amendment to the IFCD in accordance with the Article 2 of the Commission Decision 2009/584/EC of 31 July 2009, establishing the HLSG.
EMSA is responsible to keep the last version of IFCD updated as approved by the HLSG and available in electronic format.

1.5 The SafeSeaNet Group

A SafeSeaNet Group composed of MS representatives and the Commission is established. Other organisations and industry representatives can be invited to participate as observers. The objective of the SSN Group is to manage the technical and operational issues related to SafeSeaNet. EMSA chairs and is responsible to manage the SSN group.
The SSN group has adopted its rules of procedure (in Annex the SSN group 'Rules and Procedures' approved at SSN workshop nr.3, June 2005)**2**.

To this end, the SSN Group aims to:**3**

a) regularly reports 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;

2 Action point 2 (IFCD#1 meeting): Add in annex of the IFCD the document SSN 3/6/1 related to the SSN group rules and procedures (revised if necessary) - Done

3 Action point 3 (IFCD#1 meeting): Review the objectives of the SSN Group [all MS]

c) define the modification and adaptation of the system needed for compliance with the latest regulations and technical evolutions;
d) coordination of the network of SSN users;
e) propose new system functionalities;
f) elaborate and agree the SSN Technical documents and operational procedures.

The SSN group may decide to create SSN Working groups to deal with specific issues related to SSN. The task given to such a group is defined through a Term of Reference validated by the SSN group.

The SSN group consults and reports to the HLSG on any issue related to the HLSG mandate.

1.6 SSN Technical and Operational Documentation

The SSN Group has developed a full set of SafeSeaNet documentation and technical specifications. The IFCD prevails over the SSN documentation.

Together with the IFCD, the SSN 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.

EMSA is responsible to keep the last version of each document updated and available in electronic format and for maintaining all the documentation in line with the latest specifications of the system as approved by the SSN Group.

The technical and operational documentation of the SSN systems is the following:

SSN Interface Reference Guide (mandatory requirement) defines all the communication mechanisms and standards to interface SafeSeaNet, it includes the following documents:

The document defines:

- 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 applications.

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

SafeSeaNet Handbook (mandatory requirement) is the reference document to support MS through preparatory and development phases up to the regular operations within the system. 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 those existing SSN documents.

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

Incident Report Guidelines [4] (for guidance) provides information and advice to SSN Users on how to implement Incident Reports. The Guidelines clarify the rules for exchanging information on maritime incidents, including what information has to be shared, and who is responsible for the transmission of such information.

For the future, the SSN Group may decide to include additional documents to the SSN Technical and Operational Documentation.

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 **[5]**– The system established at central level acting as a nodal point to interconnect all national SafeSeaNet systems and enables the exchange of information. This system is established according to the IT infrastructure and procedures described in the IFCD document;

Commissioning tests - These are 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;

4 Action point 4 (IFCD#1 meeting): Consider including an additional document with guidelines for other messages (separate from Incident Report guidelines?) [FR, DE, NO, SE]

5 Action point 5 (IFCD#1 meeting): Propose new definition for Central and National SSN systems [UK]

- assist the Commission in reviewing the performance of SafeSeaNet;
- approve the IFCD document and any amendments thereto.

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 mechanism – This describes the flow of activities when a Member State notifies SafeSeaNet of information on a vessel or an incident (as defined in the Directive).

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 **5** – The system established at national level allowing for the exchange of maritime information between authorized users under the responsibility of a national competent authority (NCA via a single point of contact). The national SafeSeaNet system shall enable the inter-connection of authorized users and may be made accessible to identified shipping actors (ship-owners, agents, masters, shippers and others) when authorized by the NCA, in particular in order to facilitate the electronic submission of reports in accordance with Community legislation;

NCA 24/7 – The single contact point at national level (thereby strengthening and ensuring 24/7 operational contact between the MSs and with the EMSA MSS).

Regional Servers **6**- The body that assumes on behalf of a group of countries the responsibility for the hosting, maintenance, operation and monitoring of the AIS Regional Server and its connection with SafeSeaNet. The Regional Servers constitute an integral part of SafeSeaNet after properly formalised by means of a contract agreement.

Operational and Technical Requirements **7**– (…)

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.

S-TESTA - A private network that gives public administrations access to modern telecommunications services for daily dealings with other public sector bodies across

6 Action point 6 (IFCD#1 meeting): Propose new definition for Regional servers [EMSA]

7 Action point 7 (IFCD#1 meeting): Include the definition of Operational and Technical requirements [EMSA]

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.

---To be reviewed after the first draft to include additional definitions if needed---

Include a new paragraph on business drivers**8**

8 Action point 8 (IFCD#1 meeting): Include a new paragraph on business drivers [NO/DE]

Chapter 2 - SafeSeaNet Overview

Scope: *Consists of a system overview and outlines the 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

Include requirements regarding Security and Confidentiality, Reliability and Integrity**9**

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

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 SafeSeaNet systems in Member States and a SafeSeaNet central system acting as a nodal point. The SafeSeaNet central system has available different interfaces allowing optional/alternative means of transmission (as explained in detail further in the document)**10**.

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 maritime authorities (such as port authorities and coastal stations, PSC, SAR, VTS, ship reporting, pollution response, etc.) as per Directive 2002/59/EC (as amended), or other categories of users if so agreed by the HLSG.

9 Action point 9 (IFCD#1 meeting): Include requirements regarding Security and Confidentiality, Reliability and Integrity [FR]

10 Action point 10 (IFCD#1 meeting): Include a reference to the optional/alternative means of data transmission to SSN in chapter 2.2 [EMSA] - Done

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 through SafeSeaNet.

2.3 Mandatory functionalities

SafeSeaNet, at its national and central level, is built upon mandatory functionalities which are crucial for the normal operation of the system. The primary scope of SafeSeaNet is to allow the operational exchange of information as per the legislation of the Union. Those are:**11**

- Ship Reports (AIS and MRS)
- Incident reports (Member State information submitted about accidents and incidents which occur at sea)
- Port reports (pre-arrival information sent to ports 72 and 24 hours in advance and ship's arrival and departure)
- Hazmat reports (information on carriage of dangerous and polluting goods);
- Ship Security and Waste information.

The essential system functionalities of the SafeSeaNet system are the sending, receipt, storage, retrieval and exchange of information required by EU legislation.

The information collect and exchanged through SafeSeaNet must comply with the quality and performance standards defined in the IFCD.**12**

2.4 Additional 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;
- 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.

---

11 Action point 11 (IFCD#1 meeting): Move the "information to be exchanged" under chapter 2.3 [EMSA] - Done

12 Action point 12 (IFCD#1 meeting): Include a reference to the quality of the information and performance in chapter 2.3 [EMSA] - Done

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 four main levels:

- Local Competent Authorities (LCA);
- National SSN system (NCA);
- Central SafeSeaNet system;
- Regional servers, which may act on behalf of Member States to provide specific information; and
- Other systems (Thetis, LRIT DC, CleanSeaNet)

The LCA is the end user that may act as data provider as well as data requester. It is the 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 SSN central system is able to locate and retrieve information from a data provider and provide it to a data requester. The Figure 1 bellow describes the SSN network.

SafeSeaNet users may decide to store data at NCA level, and then NCA may answer the requests of detailed information without involving the respective users systems at LCA level. Alternatively, data may be stored in the servers of the LCAs or there may be combined data storage model.

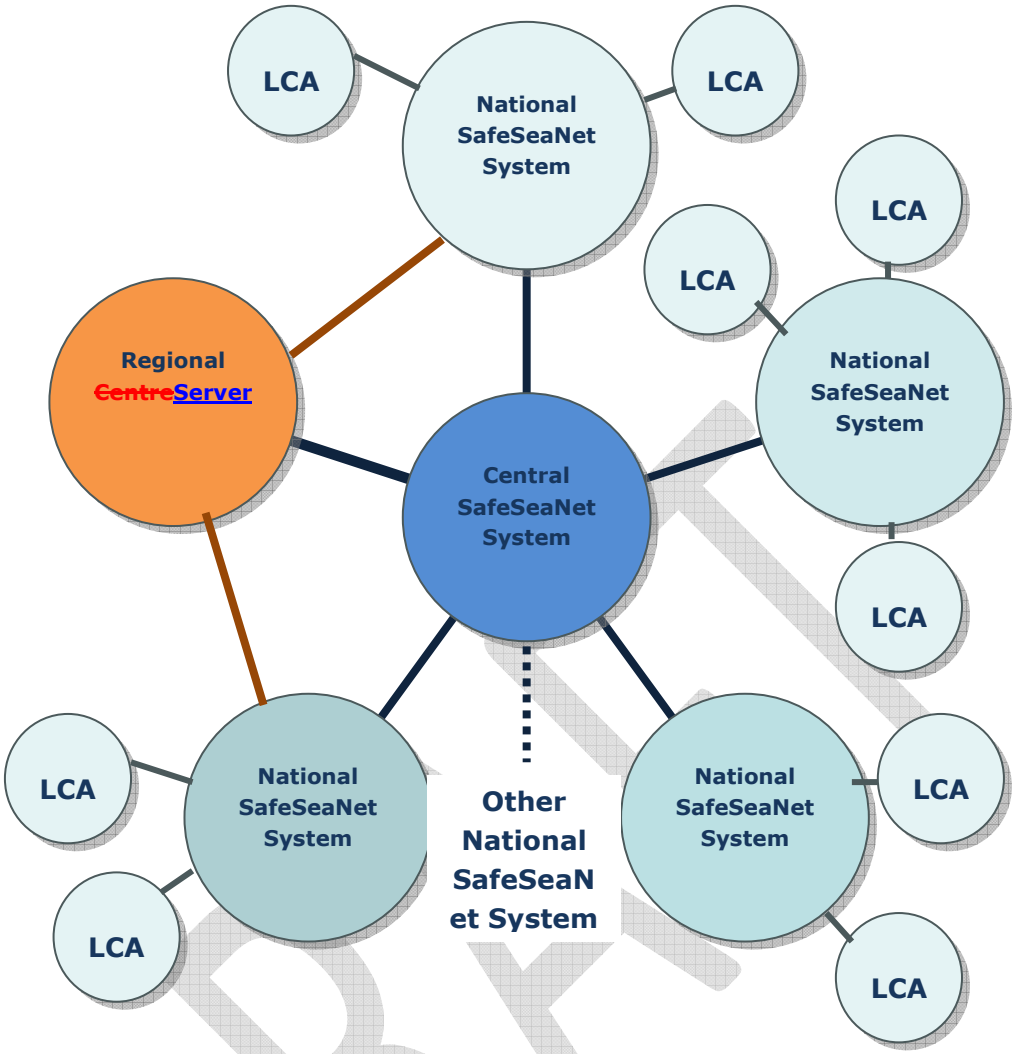

Figure 1 – SafeSeaNet network[13]

While Central SafeSeaNet system and Regional Servers store[14] centrally some information which serves to respond rapidly and effectively to users requests, detailed factual information is stored at data provider's level. Whenever the information changes (information added, updated, removed) an update notification is provided by the relevant user as a consequence of these changes; and the SSN central is up-dated accordingly.

2.5.2 Information exchange [15]

SafeSeaNet provides different mechanisms to enable the exchange of information. These are:

I. Notification, request and response mechanisms:

---

13 Action point 13 (IFCD#1 meeting): Review Figure 1 to include 'Other systems' that interact with SSN [EMSA]

14 Action point 14 (IFCD#1 meeting): Include a clarification regarding the data storage in chapter 2.5.1 [EMSA]

15 Action point 15 (IFCD#1 meeting): Review the drafting of the chapter 2.5.2 "Interfaces" [DE]. FR to provide a diagram and a description in support of chapter 2.5.2: interfaces between SSN-central with other systems [FR]

- **XML message-based interfaces:** interface to enable its users' applications to communicate programmatically within the SafeSeaNet system. They consist of a set of XML messages fulfilling the needs of both data requester and data provider (e.g. proprietary protocol, web-services etc.);

II. **Streaming mechanism**
- **Streaming Interface:** interface to enable its users' applications to communicate programmatically by exchanging flows of data based on predefined criteria with the SafeSeaNet system.

III. **Web browser-based interface:** only available for requesting information and to provide information as a back-up solution in case of failure of the national SSN system.

This interface enables the authorised users to request and obtain information from SSN, such as:

- a direct access to the data stored at central level, in a textual layout.
- a graphical information system technology to formulate a pan-European vessel traffic image with the aim at tracking vessel movements in real or near-real time.**16**

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

16 Action point 16 (IFCD#1 meeting): Clarify further in the IFCD the conditions to access SSN GI (and more important its AIS tracking information). Explore the relationship between the IFCD and the CoUs [EMSA]

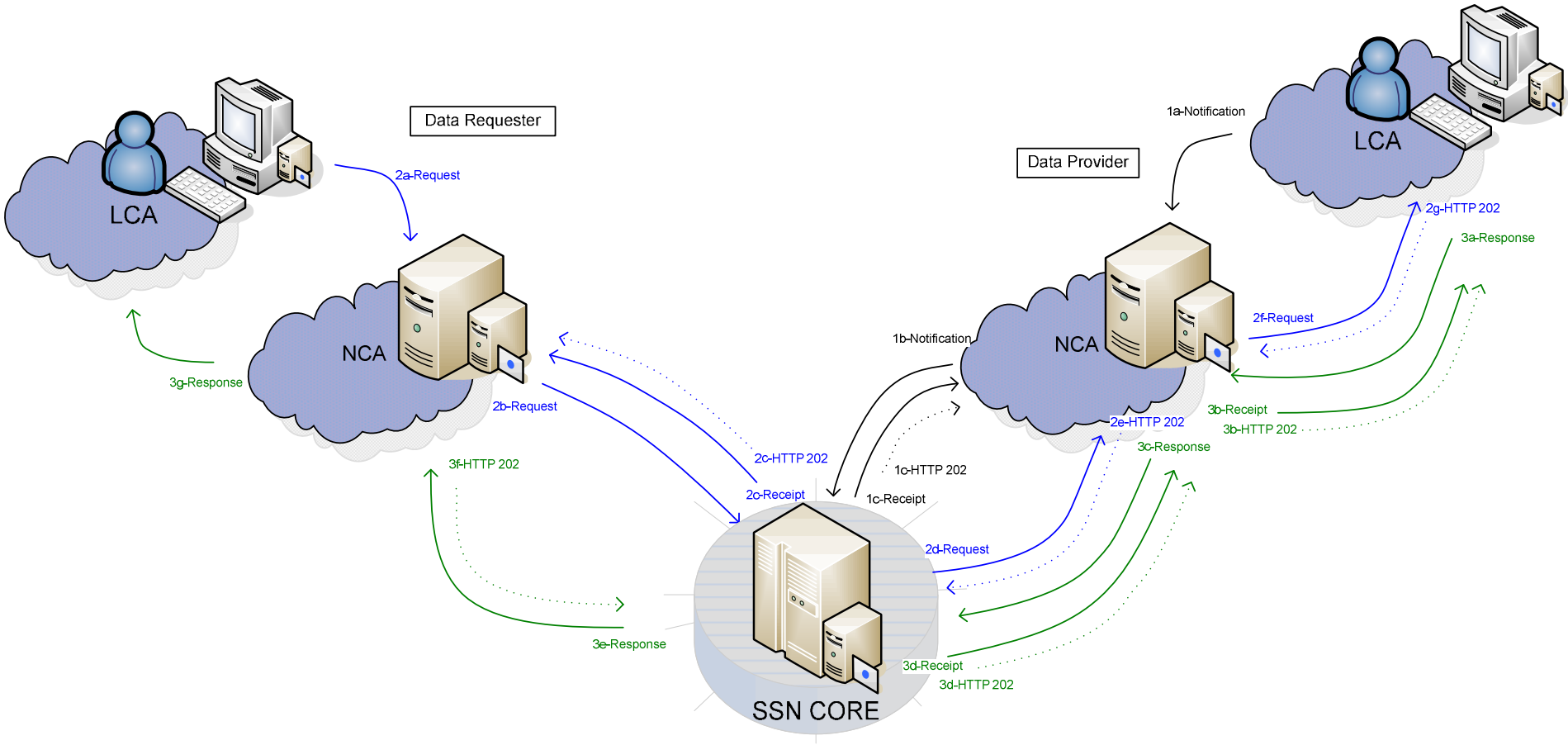

Figure 2 – General network architecture17

17 Action point 17 (IFCD#1 meeting): Review Figure 2 and move it to chapter 2.5.2 [EMSA]

2.5.3 Messaging process

a) Notification, request and response mechanism:

- Notification
  - the *data provider* gathers the necessary information to be sent to SSN;
  - it sends a "notification" message to its NCA; then
    - the NCA compiles the message in the SSN compliant format; and
    - the NCA (via the National SSN system) forwards it to the SSN;
  - on receipt the SSN determines whether the notification is well formatted and in such a case it stores it;
  - if not well formatted the notification is rejected by SSN.

- Request and response
  - the *data requester* sends a "request" message to its NCA;
  - the NCA then forwards it to the Central SSN system;
  - the SSN determines whether the request shall be granted access to the requested information:
    - in the case of information stored at SSN central 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 NCA 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 3 below.

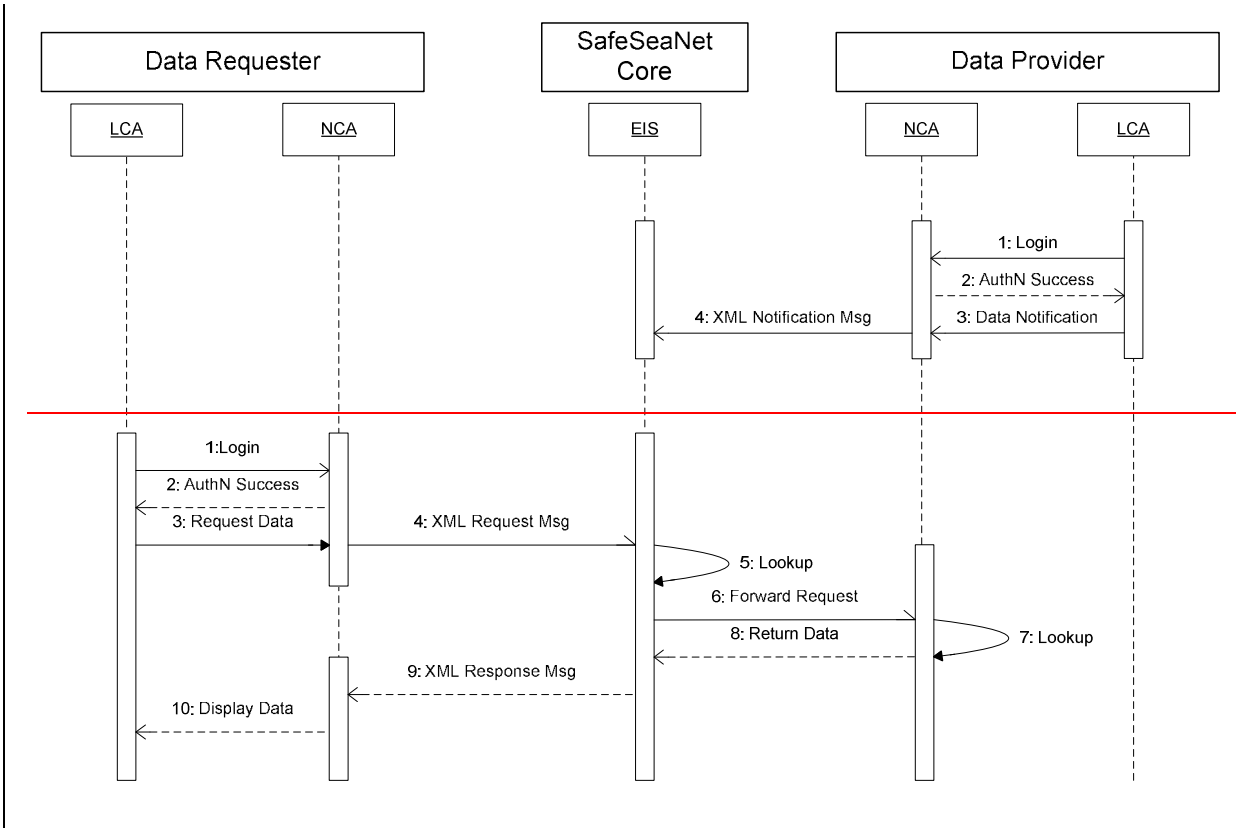

Figure 3 - Sequence diagram of notification, request and response mechanisms[18]

b) Streaming mechanism:

The SafeSeaNet is equipped with a Streaming Interface (SI), a software process deployed at regional and national level to enable the exchange of information between the SafeSeaNet central system and regional or national systems.

The main function of the Streaming Interface is to establish and manage the secured connection between a national or regional system and the SSN central system.

This interface was primarily developed to enable the near real time exchange of ship positions originated from the AIS terrestrial network. This interface allows generating a combined maritime traffic image of the EU waters combining ship positions with ship and voyage information.

The SSN streaming mechanism is described in Figure 4 below.

18 Action point 18 (IFCD#1 meeting): Simplify the figure for having a more simple description of SSN [FR]

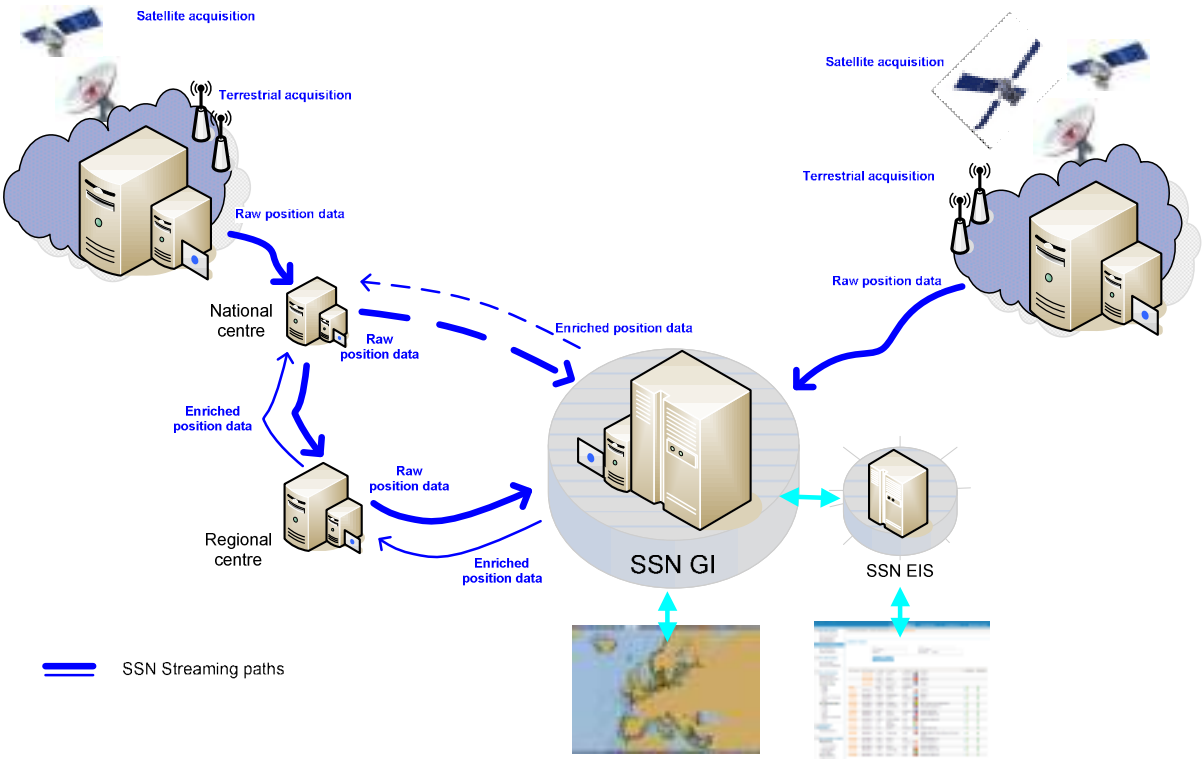

Figure 4 – Streaming data exchange architecture19

2.6 Co-operation with other systems

The Central SSN system interfaces with other EU systems for the purposes of integrated maritime policy subject to agreement regarding the access rights policy**20**.

List the systems that interface with SSN (Thetis, LRIT EU DC
Cooperation with third countries ?? Footnote

Include diagram

19 Action point 19 (IFCD#1 meeting): Review Figure 4 [EMSA]
20 Action point 20 (IFCD#1 meeting): Chapter 2.6 to be reviewed [EMSA]

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

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 SafeSeaNet 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.

SSN data requesters should receive the information requested through SSN within 15 minutes of the request.**21** Check if 120 s??

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 month period.

The NCAs should respond to requests for archived or "off-line" data as per point 4.2 below and other types of messages from other NCAs within 5 working days.

21 UK: while we support this timing it is of course overridden by the timeout value of the messages which is in most cases 60-120 seconds – how are we to reconcile to two?
FR: Same as above. This is applicable to on-line data only.

4.2 Timeframes for data storage

SafeSeaNet shall be able to archive and retrieve any message transmitted or received:

a) for "online data" or data made available through automated requests through the system for operational purposes, storage timeframes would be:
   - five (5) years minimum for data related to incidents and accidents; and
   - two (2) months minimum for data relating to position and voyage information.

b) for "offline data"**22**, or data that is not available through automated requests (i.e. data available only on the basis of an ad-hoc request to the Member State owning the information or to EMSA), the storage timeframe should be at least five (5) years for all such data. 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**23** necessary for the performance of the essential functions of the SSN system as per Chapter 2 - SafeSeaNet Overview.

The SafeSeaNet system shall be maintained in operation twenty-four hours a day, seven days a week and personnel shall be made available to satisfy the essential functions of the system.

Availability of the SafeSeaNet system shall be maintained at 99% over a period of one year, with the maximum permissible period of interruption being 12 hours**24**.

The downtimes or periods of unavailability relating to scheduled interventions, not exceeding 15 minutes (limited to 12 hours per year) and announced in accordance with the procedures defined in the SSN Handbook, should not be taken into account for the purpose of calculation of the downtimes or periods of unavailability of the systems.**25**

---

22 **FR:** about AIS data we should specify the sampling (ie 1 message every 2 hours per ship for instance). Is this relevant to keep this amount of data for 5 years? Could this be done at SSN level for AIS?

EMSA: sampling to be proposed for storage of AIS data

23 **UK:** This requirement is still not clear enough

24 **FR:** considering the operational requirements (for instance for the implementation of Dir 2009/16), this is not sufficient and should be set to a maximum of 4 hours

EMSA: proposal to be discussed

25 **UK:** are these exclusions independent or does it only apply if all 3 are true at once

EMSA: only applies if all three are true at once

FR: in a state-of-the-art approach, availability of the system should be defined considering any type of intervention. This paragraph should be removed

The availability requirements above apply independently to each national SSN system**26** (including the communication links to the Central SSN) and to the central SSN system (and communication links to the national systems).

4.4 Backup provisions**27**

In the event of a failure of a SafeSeaNet system element or in case of a scheduled interruption, the system management concerned shall implement backup procedures.

The national and central SafeSeaNet systems ~~shall~~ should be able to**28** archive messages for back up at least during 30 days**29**. The NCA shall ensure that the SSN messages are stored and ~~transmit~~transmitted ~~the SSN messages~~**30** when communications and /or systems are restored.

EMSA shall ensure that ~~T~~the Central SSN ~~shall~~ retries~~y~~**31** sending messages over 2 seconds for a maximum of 5 times**32**.

EMSA: proposal to be discussed

26 **UK:** what about the downtime of an LCA? Or when the AIS system is interrupted but all the National SSN system is operational?

EMSA: a downtime of one LCA should be considered partial downtime. It would not be taken into account in this "system availability requirement" but in the reports on data quality checks. For the AIS notifications should still be provided at least every 2 hours (via XML or proxy) the downtimes could be limited to 2hours?

27 **FR:** unclear. This chapter should be split to cover the requirements in terms of: back-up: security against the loss of data, Recovery after a temporary failure

EMSA: propose redraft

28 **SE:** change to "should be able to archive messages..."

29 **UK:** given 4.3 only permits 12 hours of downtime why is 30 days referred to here?

EMSA: the 30 days are to respond to unforeseen circumstances (business continuity)

30 **UK:** depending on the type of failure this might not be possible – if it is due to the national SSN database being corrupted for example

EMSA: is there not a back-up data base that can be used for failover??

SE: change to "The NCA shall ensure that the SSN messages are stored and transmitted when..."

31 **SE:** change to " EMSA shall ensure that the Central SSN retries sending messages..."

32 **UK**: this seems of little value as it only provides a 10 second window for the recovering of connection - more realistic would be to retry at 5 minute intervals.

FR: this should also be applicable to NCA requesting SSN. This is not sufficient to guaranty the integrity of the distribution of the information. What happens after these 5 times?

EMSA: we agree that this requirement that came from the ICD can be reviewed. To be discussed at the meeting.

The ~~affected element~~authority in charge of the SSN affected system (national or central)**33** must be capable of informing other participants**34** in the SafeSeaNet System network using status messages as defined in Chapter 5 - and in the operational procedures in SSN Handbook.

4.5 Additional system performance requirements

Messages lost, missing or invalid messages ~~or corrupted~~ **35** should be less than 0,1%. When the Central SSN system receives ~~a corrupted~~an invalid message, an error message shall be produced and forwarded to the NCA/LCA.

When SafeSeaNet emits a corrupted message, the LCA/NCA recipient shall inform the EMSA MSS.

4.6 Data quality

~~To ensure an operational use of the data in the SafeSeaNet system~~**36**, MSs should~~all participating authorities commit~~**37** ~~to~~:

- introduce in all components**38** of the system the automatic data quality rules**39** agreed by the SSN Group,
- ~~to~~ put in place, in cooperation with EMSA, the appropriate control mechanisms to investigate data quality issues that affect more than 0,1%**40** of the messages per country and type of message per month.

---

33 **SE:** what does "affected element" mean? Can an element inform other participants? Consider rephrasing.

34 **FR:** procedures and means of communication of the failure to the NCAs need to be defined here

EMSA: defined in Chapter 5 - and in the operational procedures in SSN Handbook

35 **UK:** confirm that this means just malformed messages

FR: 'Lost' and 'corrupted' need definition. A timeout should be defined (for lost message)

EMSA: this includes missing and invalid messages. Text redrafted. Timeout to be discussed

36 **SE:** what has the operational use of the data got to do with the data quality? The sentence and the meaning of it is unclear

37 **SE:** it's impossible to speak for other authorities in this matter. Propose rephrase to "MSs should ensure that national participating authorities should commit to..." (if this is what is means?)

38 **NL:** we have our doubts on this subject, we will explain our doubts at the meeting

39 **UK:** can these be documented somewhere?

EMSA: included in the XML reference guide "and in future communication reference guide"

40 **UK:** we would like to review this figure

SSN data providers should make the information available in the National SSN system within maximum 15 minutes upon receiving this information from the origin of the process. > Move to chapter 4.6 Data Quality

4.7 Network coordination

Each NCA and EMSA will maintain a 24/7 contact point that will be available to manage SSN related requests relating to daily operations or reporting from any ~~of its national users~~ other SSN NCA or EMSA **41** ~~of the system~~ on a 24/7 basis.

EMSA will provide a 24/7 monitoring**42** of the above requirements and network coordination and helpdesk for the SafeSeaNet system.

Monitoring procedures and ~~O~~operational communication procedures among the NCA 24/7 and between these and EMSA are agreed at the level of the SSN Group (and defined in the SSN Handbook) within the framework of the chapter 5 below.**43**

41 **UK:** this needs to be clarified – for example an NCA is not required to deal with a issues around the reporting of a user in another MS

42 **UK:** the measures used for monitoring should be agreed by the SSN Group and recorded in SSN Handbook

43 **SE:** these operational procedures should all be included in IFCD chapter 5 and reference should be to that chapter – not the handbook. Mentioning that they "are agreed at the level of SSN Group" is very unclear to newcomers of the SSN Group and should be taken out.

EMSA: the operational procedures are included in chapter 5. However, they are detailed in the SSN Handbook. It is not possible to detail every procedure in the IFCD

Chapter 5 - Operational Services and Procedures

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 system and the Central SSN system, including the transmission of messages, performance levels and operating procedures.

SafeSeaNet must be 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

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.

The Central and National SSN systems must ensure that a Business Continuity Plan (BCP) is in place. The BCP must contain an outline of the approach to ensure the continuity of services in the case of disaster/ unexpected events. The BCP must cover the essential functions (listed in Chapter 2.3) and apply risk reduction or recovery options in case of disaster/ unexpected failures of the system.**44**

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:

- Meet requirements of the availability of the National 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 directive can be still available;
- Ensure that information is recovered after the period of the down-time/ disaster/ failure.

In order to ensure the continuity of service of SSN, MS should establish a permanent service at the National Competent Authorities (the NCA 24/7 further in the document) and described in the point 5.2.4 - System support services. The same service is established at central level by the EMSA Maritime Support Services (MSS).

Those NCA 24/7 services should be responsible for executing of SSN operational procedures which will cover countermeasures to ensure continuation in the event of a disaster and may perform some of the functions described hereafter.

---

44 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.

5.2.2 Communication services by phone, fax, e-mail[45]

For the purpose of the SafeSeaNet operations and ensuring the system performance requirements, the following types/directions of communications can be considered:

- Between SSN participants – e.g. to retrieve information in the system;
- Between SSN Participants, and SafeSeaNet administrator (EMSA MSS) – in order to ensure continuous exchange and retrieve information required by the Directive;
- Between SSN (National Competent Authorities) , data providers, requestors and LCAs - to ensure receipt, storage, exchange and retrieve information in the system;
- Between EMSA MSS and other users.**46**

SSN Authorities have to ensure that effective communication links and their backup provisions are in place to fulfil the above types of communications.

5.2.3 Reference Databases' management[47]

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~~**48**.

Data exchanged in the SSN system should be coherent and of the best possible quality. To ~~Therefore, each SSN participant~~**49** ~~should maintain and keep updated local databases which will~~ **50** 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.

---

45 **FR:** a procedure was defined previously (SSN 12): cf how to be sure if the contact has the right to retrieve information?
46 **UK:** this list will need to be clarified
47 **UK:** we accept the importance of data quality – but do not believe that the ways of achieving it should be prescribed
48 **UK:** see above comment on the use of 'etc'
49 **FR:** and Central SSN
50 **UK:** we accept the importance of data quality – but do not believe that the ways of achieving it should be prescribed

5.2.4 System support services

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:**51**

- Notify the SSN on a continuous basis**52** (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**53**;
- 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**54**;
- ~~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**55**;
- ~~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;

---

51 **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)

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

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

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

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

- 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 **56** (failures in another MS or in the SSN application/ hardware/ network);
- Provide support to users at National level.**57**

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;
- System assessment regarding the quality of the information provided by the National SSN system;
- Providing feedback to the development teams**58**;
- 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**59**. 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)60.**

---

56 **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

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

58 **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

59 **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

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

EMSA: detailed list for the MSS to be included

5.3 Operational Procedures[61]

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.**62***

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.**63**

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.

---

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

62 **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"

63 **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"

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:

- 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.**64**

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.

---

64 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

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**65** 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**66**.

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.**67**

---

65 **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

66 **FR:** not very clear

EMSA: propose redraft

67 **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 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.**68**

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

---

68 **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.**69**

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.**70**

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.

---

69 **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

70 **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

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.

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[71]

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.

---

71 **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

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 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[72] and new requirements arising from legal requirements.

---

72 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

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 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**73**:

- 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;**74**
- 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.**75**

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:

---

73 **FR:** rather than a presentation of the document, the high level principles should be explained here

EMSA: propose redraft

74 **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

75 **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

- SSN Communication Interface Document**76**;
- Network and Security Reference Guide.

The CMF will not be ~~invoked~~applied**77** under the following conditions:

- Changes applicable to EMSA's internal organisation and/or operation;
- Changes proved**78** 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.**79**

6.3.2 Change management process**80**

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**81**. 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

76 **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

77 **FR:** propose 'applied'

78 **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)

79 **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

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

81 **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

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.

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

Annex 1 - Rules and Procedures of the SafeSeaNet Group[82]

PART I – OBJECTIVES

Rule 1: Objectives

The objective of the SafeSeaNet Group is to provide the primary focal point for SafeSeaNet. To this end, the SafeSeaNet Group aims :

A. Regularly report on the SSN activities of the Member States and EMSA
B. Monitor and support the adaptation of the system with the users' requirement
C. Define the modification and adaptation of the system needed for complying with the latest regulations and technical evolutions
D. Encourage and support the entrance of new users
E. Propose the new system functionalities
F. Elaborate and agree the SSN supporting documents
G. Deal with the traffic monitoring related issues as defined in the Directive 2002/59 and the EMSA regulation No. 1406/2002.
K. Examine how the traffic monitoring infrastructure data (including the Long Range Identification and Tracking issues) could be linked or integrated in SafeSeaNet

PART II - COMPOSITION

Rule 2: Participation and Attendance

A. A SafeSeaNet Group is established in accordance with Article XX of the Interface Control Document. It consists of Delegations from the Members State, the EFTA and the acceding States. The Delegations may be accompanied by deputies, technical advisers and industry representatives who will be Members of the Participant's delegation.
B. The Delegation shall be designated by the Member State. Each Delegation shall notify the EMSA Secretariat, the names and functions of the members of the delegation 1 week before the meeting.
C. EMSA, as well as the EMSA staff involved in SafeSeaNet system shall support the meetings of the SafeSeaNet Group.
D. States participating in the SafeSeaNet system are entitled to attend the meetings of the SafeSeaNet Group, receive all the relevant documents pertaining to the meeting, submit papers, propose agenda items and participate in the discussion.
E. Each Delegation must ensure that members of the delegation represent the views of the Member States and speak under the authority of the Member State.

PART III - MEETINGS

Rule 3: Location of Meetings

82 As approved by SSN workshop nr.3 in June 2005, document reference SSN 3/6/1.

The SafeSeaNet Group shall meet at the location where the EMSA premises lie unless the participants decide otherwise.

Rule 4: Dates of Meetings

A. The SafeSeaNet Group shall meet as decided on a common agreement, normally three times per year, but not less than once in any twelve-month period.
B. The dates of meetings of the SafeSeaNet Group shall be communicated to the Commission that will always be invited to attend and present the Commission views under the permanent agenda item II which is "INPUT FROM THE COMMISSION".

PART IV - OFFICERS

Rule 5: Chairperson

A. The Chairperson of the SafeSeaNet Group and the Chairperson of each Specialised Working Group of the SafeSeaNet Group will be EMSA officials designated by the EMSA.
B. The Chairperson may designate a deputy from the attendee delegation to assist him/her to the conduct the meeting. In the event the deputy chooses to present his/her delegation's position in the meeting, he/she shall indicate clearly that he/she is doing so as member of his/her delegation.

Rule 6: Responsibilities of the Chairperson

A. The Chairperson shall exercise his/her responsibilities under the authority of the EMSA and in accordance with the Terms of Reference defined in the agenda.
B. During meetings the Chairperson shall act in accordance with customary practice. The Chairperson shall open and close the meetings, direct the deliberations, give the floor to speakers in the order in which they request it, strive to seek unanimity, announce the conclusions of the discussion and prepare a report for the SSN Working Group.
C. Between the meetings, the Chairperson shall:
   (i) ensure the appropriate co-ordination;
   (ii) ensure the preparation and distribution of documents.

PART V - PROCEDURE FOR THE MEETINGS

Rule 7: Meeting Preparation

A. Agenda

A.1 A provisional agenda for the subsequent meeting shall be established at the conclusion of the meeting.
A.2 Additional items may be added to the provisional agenda at the request of a delegation, up to **30 days** prior to the opening date of the meeting.
A.3 Items relating to urgent matters may be proposed at any time by Delegations.
A.4 EMSA shall prepare the provisional agenda of the meeting.

A.5 The provisional agenda will be subject to approval as the first item of business of the meeting.

B. Documents for Meetings

B.1 Documents addressing items of the provisional agenda shall be submitted to EMSA for distribution, **30 days** prior to the opening date of the meeting. EMSA shall make accessible these documents through the EMSA web site at least **2 weeks** prior to the opening date of the meeting.

B.2 Documents submitted in support of additional agenda items referred to in Rule 7.A.2 above shall be provided to EMSA not later than **2 weeks** prior to the opening date of the meeting. EMSA shall make accessible these documents to Delegations not later than **2 week** prior to the opening date of the meeting.

B.3 Documents received by EMSA after the above mentioned time limits shall be distributed as information papers and may be considered at the meeting with the agreement of all members, or at subsequent meetings.

B.4 Information papers may be submitted at any time.

B.5 Information papers submitted for establishing proposed agenda items for subsequent meetings may be presented during a meeting.

B.6 Documents in support of urgent matters, as provided for in Rule 7.A.3, may be submitted at any time prior to or during a meeting.

Rule 8: Proceedings

A. Delegates may submit proposals for discussion during the course of a meeting.
B. No commercial marketing activity shall take place during SSN Group meetings.
C. Presentations on commercial products for the purpose of providing technical information to delegates may be made at the request of a Delegation, with the approval of the Chairman of the SafeSeaNet Group.

Rule 9: Meeting Records

A. The SafeSeaNet Group shall, at the beginning of each meeting, approve the Report of the previous meeting,
B. The Report shall be the only official record of the meeting of the SafeSeaNet Group and its Specialised Working Groups.
C. The technical specifications, plans, standards and reports agreed to by the SSN Group shall be appended to the Report of the SSN Group in the form of annexes.
D. Delegations may request the inclusion of their statements in the Report.

PART VI - OTHER PARTICIPANTS

Rule 10: Observers

A. Authorities, Institutions, Agencies, European and international organisations may be invited by EMSA, to participate as observers at the meetings of the SafeSeaNet Group.
B. Observers shall notify EMSA of the names and functions of members of their delegation before the beginning of the meeting.

C. Observers at SafeSeaNet Group meetings may receive all the relevant documents pertaining to the meeting, submit documents for consideration during the course of a meeting, and participate in the discussion at the invitation of the Chair.

PART VII – SPECIALISED WORKING GROUPS OF THE SAFESEANET GROUP

Rule 11: Specialised Working Groups

A. The establishment of Specialised Working Groups of the SafeSeaNet Group and their Terms of Reference are decided by the SafeSeaNet Group.
B. The Rules of Procedure of the SafeSeaNet Group are applicable to the Specialised Working Groups.

PART VIII - MISCELLANEOUS

Rule 12: Public Relations

The SafeSeaNet Group may recommend public relations actions to EMSA, but not make press releases or take public relations initiatives without the approval of EMSA.

Rule 13: Languages

The working language of the SafeSeaNet Group and its Specialised Working Groups is English.

Rule 14: Amendments

The SafeSeaNet Group may recommend amendments to these Rules of Procedure.