



EUROPEAN COMMISSION
DIRECTORATE-GENERAL FOR ENERGY AND TRANSPORT

EUROPEAN MARITIME SAFETY AGENCY

SAFESEANET

INTERFACE CONTROL DOCUMENT

SSN ICD
Issue 0 Revision: 1
Date: 19 October 2004

SAFESENET INTERFACE CONTROL DOCUMENT

History

Issue	Rev	Date	Prepared by	Checked by	Date
0	0	02 June 2004	YTE/UBI	EMSA/LAI/EMB DG TREN	02/06/2004
0	1	28 September 2004	YTE		

LIST OF PAGES

Page	Date of latest revision	Page	Date of latest revision	Page	Date of latest revision
------	----------------------------	------	----------------------------	------	----------------------------

LIST OF ACRONYMS USED IN ICD.	7
PREAMBLE	9
1 INTRODUCTION	10
1.1 Overview	10
1.2 Document Objective.....	10
1.3 Document Organization	10
1.4 Document Amendments and Updates	10
1.5 Reference Documents	11
2 GENERAL OPERATIONAL CONCEPT	12
2.1 General Architecture of the System	12
2.2 Distribution Principles.....	13
2.2.1 Physical flows.....	13
2.3 Security requirement	14
2.4 Definition:	14
3 SAFESEANET PARTICIPANTS	17
3.1 Parties involved	17
3.1.1 Members State Stakeholders.....	17
3.1.2 European Union Institutions	18
3.2 Agreement of the parties	18
4 SAFESEANET FUNCTIONS	20
4.1 Definition of a Data Provider	20
4.1.1 Responsibility of a “Data Provider”	20
4.1.3 Data Provider capabilities	20
4.2 Definition of a Data Requester	21
4.2.1 Responsibility of a “Data Requester”	21
4.2.2 SafeSeaNet Supplied Interfaces for <i>Data Requester</i>	21
5 MESSAGING PROCEDURE	22
5.1 Presentation	22
5.2 Notification	22
5.2.1 PORT NOTIFICATION	24
5.2.2 SHIP NOTIFICATION.....	25
5.2.3 HAZMAT NOTIFICATION	25
5.2.4 ALERT NOTIFICATION	26
Ship identified – Ship not Identified.....	26
5.2.5 SEND E-MAIL NOTIFICATION.....	26
5.2.6 Temporary Measures	26
5.3 Request.....	31
5.3.1 SHIP REQUEST	31
5.3.2 PORT REQUEST	32
5.3.3 AREA SEARCH	32
5.3.4 SIRENAC, BPWIS, EQUASYS.....	33
5.4 Receipt.....	35
5.4.1 Process	35
6 SAFESEANET SYSTEM INFORMATION AND TEST	36
6.1 System information	36

6.2	System Status Change.....	36
6.2.1	SafeSeaNet Changes of Operational Capabilities	36
6.2.2	SafeSeaNet System Failure.....	36
6.2.3	SafeSeaNet Scheduled Outage.....	36
6.3	System Test	36
6.3.1	General guidance	36
6.3.2	Pre test requirement	37
6.3.3	Submission of results – Integration	37
6.3.4	Tests Plan.....	37
7	SYSTEM SPECIFICATIONS.....	38
7.1	Communication Interfaces	38
7.1.1	XML message based interface	38
7.1.2	Default browser-based web interface.....	38
7.1.3	Connection to the Central Index	38
7.1.4	SafeSeaNet Security	40
7.1.4.2	Authorisation	40
7.1.4.3	Authentication.....	41
7.1.4.4	Confidentiality	41
7.2	Operational System Requirements.....	45
7.2.1	Overview	45
7.2.2	Scope	45
7.2.7	Performance requirements	47
8	STATISTICS.....	49
8.1	Edition of statistics	49
8.2	Statistical uses.....	49
	ANNEX A – MEMBER STATE AUTHORITY REFERENCE	51
	ANNEX B – NATIONAL COMPETENT AUTHORITY (NCA)	52
	ANNEX D – STATUS OF PARTICIPANTS.....	59
	ANNEX E/1 - DEFAULT BROWSER-BASED WEB INTERFACE DOCUMENTS FOR NOTIFICATION	60
	ANNEX E/2 - SHIP (MRS) INFORMATION	61
	ANNEX E/3 - HAZMAT INFORMATION.....	61
	ANNEX E/4 - SECURITY INFORMATION	61
	ANNEX E/5 - INTERNATIONAL SITREP Format	61
	ANNEX E/6 - POLREP FORMAT	61
	ANNEX E/7 - LOST/FOUND CONTAINERS (*) REPORT	61
	ANNEX E/8 - WASTE ALERT NOTIFICATION	61
	ANNEX F – MESSAGES DESCRIPTION.....	61

TABLE OF CONTENTS

Page

History
List of Pages
Table of Contents
List of Tables
List of Figures
List of Annexes

LIST OF TABLES

Table 5/1 Notification Messages Description
Table 5/2 Voyage Information Notification
Table 5/3 List of Data to be notified
Table 5/4 Requests messages description
Table 7/5 Area Search Access
Table 7/6 Role Code
Table 7/7 Users Access Right

LIST OF FIGURES

Figure 2/1 Distribution principle
Figure 2/2. General Architecture
Figure 5/3 geographical sorting
Figure 7/4 National Network Connection
Figure 7/5 Direct connection
Figure 7/6 Security Services
Figure 7/7 Security Measures

LIST OF ACRONYMS USED IN ICD.

The following abbreviations may be used within this document or in reference document:

3DES	Triple Digital Encryptions Standard (168 bits symmetric encryption)
AIS	Automatic Identification System
ARC	Architecture Specification document
B2B	Business-to-Business
CA	Certification Authority
CRL	Certification Revocation List
CS	Coastal Station
CUG	Closed User Groups
DES	Digital Encryption Standard (56 bits symmetric encryption)
DI	Informatics Directorate of the European Commission
DG-TREN	Directorate General – Transport and Energy
DNS	Domain Name Server
DPG	Dangerous or Polluting Goods
EC	European Commission
EDI	Electronic Data Interchange
EIS	European Index server
EMSA	European Maritime Safety Agency
ESP	Encapsulating Security Payload
ETA	Estimated Time of Arrival
ETD	Estimated Time of Departure
HAZMAT	Hazardous Material
HTTP	hypertext Transfer Protocol
HTTPS	hypertext Transfer Protocol over SSL
IALA	International Association of Lighthouse Authorities
IDA	Interchange of Data between Administrations
IETF	Internet Engineering Task Force
IMO	International Maritime Organisation
IP	Internet Protocol
KGW	Key Generation Wizard
LCA	Local Competent Authority
LDAP	Lightweight Directory Access Protocol
LRA	Local Registration Authority
MMSI	Maritime Mobile Service Identity
MPLS	Multi Protocol Label Switching
MPOC	Multi Point of Competent Authority
MRS	Mandatory Ship Reporting System
MS	Member State
MTTR	Mean Time To Restore
NAT	Network Address Translation
NCA	National Competent Authority
NCP	National Contact Point
NN	National Network
PA	Port Authority
PKI	Public Key Infrastructure

QoS	Quality of Services
RA	Registration Authority
RAO	Registration Authority Officer
SLA	Service Level Agreement
SSL	Secure Socket Layer
SSN	SafeSeaNet
TCP	Transfer Control Protocol
TESTA	Trans European Services for Telematics between Administrations
TTR	Time To Restore
URL	Unified Resource Locator
URQ	User Requirement Document reference
WAN	Wide Area Network
XKMS	XML Key Management Specification
XML	Extended Mark-up Language
XSD	XML Structure and Schema Definition

PREAMBLE

Following the accident of the cargo ERIKA off the French coast in 1999, the European Union has adopted several directives for improving the prevention of accidents at sea and the fight against marine pollution. Directive 2002/59/EC adopted by the Parliament and the Council on 27 June 2002 aims at establishing in the Community a vessel traffic monitoring and information system “with a view to enhancing the safety of 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”. This Directive requires Member States and the Commission to co-operate to develop computerised data exchange and to develop the necessary infrastructure to this end.

In order to contribute to fulfil this objective, the Commission has launched in the end of 2001 the development of a European Platform for Maritime Data Exchange, and this became SafeSeaNet.

The main objective of the SafeSeaNet is the development of a European Platform for Maritime Data Exchange between maritime administrations of the Member States of the European Union, by:

- Setting-up a telematic network between all the maritime EU Member States for their co-operation in preventing maritime pollution and accidents at sea.
- Creating this network taking into account new technologies such as XML and the Internet/TESTA network, making it flexible to cope with future technological developments.

SafeSeaNet also take into account the follow-up of the PRESTIGE accident, and in particular the call made by the Council in its conclusion of 6 December 2002 to strengthen the mechanisms for the control of traffic along the coasts of the Member States.

The implementation of Directive 2002/59/EC, as well as other provisions of EC legislation, requires the collection and distribution of various kinds of data. It concerns vessel traffic monitoring, dangerous cargo details, results of ship inspections, information related to ship waste and cargo residue. SafeSeaNet is the improvement of the exchange with a better standardisation and a profusion of transfer mechanisms – from phone or fax to electronic messages (often via EDIFACT), which will improve an efficient implementation of the EU maritime safety legislation.

In addition, SafeSeaNet has been designed for providing, as necessary, new services coming from a large community of users with objective to contribute to the implementation of others community policies like environmental protection, security, immigration, etc...

1 INTRODUCTION

1.1 Overview

The purpose of the SafeSeaNet Interface Control Document is to describe the system in terms of the message scenarios, the message functions and the relation between the messages. The document details the message timing and performance and the data interchange protocol and parameters. It specifies the data content of the required message functions and describes those messages.

1.2 Document Objective

The SafeSeaNet System is operated in accordance with the Directive 2002/59/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 June 2002 establishing a Community vessel traffic monitoring and information system and repealing Council Directive 93/75/EEC.

Annex III of the Directive 2002/59/EC requires the Commission in consultation with Member States to develop and maintain the Interface Control Document.

The purpose of this document is to:

- Describe the SafeSeaNet system and functionality,
- Define the corresponding procedures to be implemented by Members State for distributing electronics messages.

1.3 Document Organization

The SafeSeaNet policy with regards to Members States is contained in the text of this SafeSeaNet Interface Control Document.

A description of SafeSeaNet general operational concept is given in section 2.1

Section 2.2 describes the Distribution Principle for exchanging messages between Members States points of contact.

The Annexes to this SafeSeaNet Interface Control Document provide:

- a) Pertinent information needed by Members States to support operational activities (Annex A)
- b) A description of the SafeSeaNet actors (Annex B to D)
- c) [Notification forms \(annex E/1 to E/8\)](#)
- d) A summary of messages to be used in SafeSeaNet ([Annex F](#))

Except for the operational procedures which cannot be changed without appropriate co-ordination with all MS, other operational information in the Annexes to the SafeSeaNet Interface Control Document is subject to change and needs to be kept current between scheduled SafeSeaNet meetings.

1.4 Document Amendments and Updates

Amendments to the main text of the SafeSeaNet Interface Control Document and the operational procedures of the SafeSeaNet Interface Control Document Annexes, but excluding Annex A to C of the SafeSeaNet Interface Control Document Annexes, shall be approved by the Members State.

Members States actors' status information in Annex D of the SafeSeaNet Interface Control Document Annexes can be amended by the responsible Members State's actor.

Information provided in Annex A to D of the SafeSeaNet Interface Control Document Annexes can also be updated as necessary by EMSA on the basis of official available information. This SafeSeaNet Interface Control Document will be subject to review at regular Members State meetings.

Each page of the document includes in its header an Issue number, a Revision number and the date of the revision. The last revision date of each page of the document is listed in a summary page updated with each new revision.

Users of this SafeSeaNet Interface Control Document should ensure that their copy of the document includes all the revisions issued by EMSA, as indicated in the History page **(tbc)** and the List of Pages **(tbc)** which precede this section.

1.5 Reference Documents

- a) SafeSeaNet User manual, version [1.5 of 22 June 2004](#)
- b) SafeSeaNet XML Messaging Reference Guide [version 1.6 of 26 July 2004](#)
- c) SafeSeaNet Network & Security Reference Guide version 1.0 of [02 April 2004](#)
- d) [Procedures and Guidelines for the registration of new web server certificates version 1.0 on 14 Sept. 2004](#)
- e) [SafeSeaNet test Plan on 19 December 2003](#)

2 GENERAL OPERATIONAL CONCEPT

In pursuance of the international, regional or national regulations, ships shall report a important amount of data during their voyage at destination and within the European waters.

According to the Directive 2002/59/EC, it is the responsibility of the ship operator, agent or master to notify the competent authority prior to entry into a port of a Member States, and additional information when carrying hazardous goods on board within the European waters. Also, Member States shall monitor the mandatory ship reporting system when ships are navigating within their vessel traffic system in accordance with IMO recommendation.

A clear distinction must be **made** between the information transmitted by the ships to the shore, as a "Ship to Shore" notification flow and the information exchanged on shore through the "European Index server" as a Shore to Shore notification flow.

SafeSeaNet aims at facilitating the "Shore to Shore" notification exchange of data in a comprehensive format. The exchanged data should be received from different external system existing or planned to be implemented, and adapted to the SafeSeaNet system specifications.

It's a specialised network established to facilitate the exchange of data in a electronic format between the maritime administrations of the Members States. The system is working with an objective to comply with the Community legislation of maritime safety, namely Directive 2002/59/EC and also of other texts related to port reception facilities and on port state control.

The SafeSeaNet system is based on the implementation of two different interfaces accessible by the maritime community trough the Internet network.
It has been designed to be available on round the clock basis with a high level of reliability and security.

2.1 General Architecture of the System

The core of the SafeSeaNet architecture consists of the SafeSeaNet XML Messaging System. It acts as a secure and reliable "yellow pages" index system in a "hub and spoke" **network** (including authentication, validation, data transformation, logging,...) for sending requests to and receive notifications and responses from participants identified as *data provider* and *data requesters*.

Detailed factual information is stored at local authority level. Whenever the information changes (information added, updated, removed) the local authority sent a notification to the European Index. Thanks to these notifications, the European Index knows the location of the information.

This also implies that whenever an indexed location (this is the location the European Index knows about) receives information, it must send this fact to the European Index. At the moment, the current location of the information and any subsequent queries about this information will be redirected to this location.

The SafeSeaNet System relies on a distributed architecture made of 3 levels;

- Local Competent Authorities (LCA)
- National Competent Authorities (NCA)
- The central index,

A local Competent Authority is the end entity that can range from Port Authorities, Coastal Stations to Harbour Commercial Organisation. It is the recipient of the "ship to shore" messages and feed the SafeSeaNet system with that message. It can request the system for receiving information.

A National Competent Authority or a MPOC assumes on behalf of its country the responsibility of the SafeSeaNet management. It is in charge to verify and maintain the national network and procedures compliant with the requirements as described within the Interface Control Document.

A NCA should acts as an LCA at national level.

The central index is a part of the European Index Server. It is able to locate and retrieve information from one Member State in response to a query by another Member State.

A detailed description of LCA, NCA and Central Index is provided further in the ICD.

2.2 Distribution Principles

The bulk of information remains in the Member States. When a LCA/NCA has got information about a ship, it just informs the central index about it through a “notification” message. The system will display that the competent authority that provided the data (identified as data provider) possesses a certain type of information on a certain ship.

In common with standard messages for ship position and destination, the system will display the name of the ship, the position transmitted, the port of destination and the ETA (Estimated Time of Arrival).

When an authority (e.g. in another Member State) wishes to display more detailed information, the following occur:

- The competent authority (identified as data requester) sends a “request” message to his NCA, who forwards it to the central index;
- The central index forwards the request to the NCA of the Member State where the requested information resides, which, in turn, forwards it to the end entity that owns the information;
- The competent authority (data provider) that owns the information then answers with the information that is transmitted back to the requestor;

There can be variations: some Member States may decide to collect within an NCA the information that is produced by their LCAs. In these Member States, the target NCA can answer the request without involving the respective LCAs.

2.2.1 Physical flows

Following International, European and National regulations ships are required to notify important information to the coastal or port authorities.

In accordance with the European requirements, ships shall report to the competent authorities:

- Notification prior to entry into ports of the Member States (Article 4 of the Directive 2002/59/EC)
- Notification of dangerous or polluting goods on board ships (Hazmat - Article 13 of the Directive 2002/59/EC)
- AIS (Automatic Identification System) and VTS (Vessel Traffic Service) Ship reports

Following the international, European Union and national regulations, Member States administrations have to capture a large amount of information on vessels within their coastal waters and distribute this to other Member States along the intended route of the vessel.

Member States shall notify in a **specified time** to the E.I.S:

- Port Notifications
- Hazmat Notifications
- Ship reports AIS and VTS

- Messages emitted by their operational services following events at sea (Search and Rescue report, Pollution report, and Deficiency report...)

The figure 2/1 shows the general principle of distribution in SafeSeaNet according with the flow of information exchanged between shore to shore services.

2.3 Security requirement

The SafeSeaNet system will exchange data relative to the maritime traffic and activity. Due to the sensitivity of the data and with objective to keep their integrity, the system is protected by the implementation of several levels of security.

The security measures are based on four major services:

- Authorisation
The authorisation service ensures that the data access is granted only those who are authorised to see the data. The Central Index manages the authorisation.
- Authentication
Access is granted on the identity of the requestor made on a relaying authentication scheme. It's mean the end-user (LCA) authenticate towards the NCA, and then the NCA forwards the identity of the authenticated end-user to the Central Index and.
- Confidentiality
The confidentiality service ensures that information is not disclosed to unauthorised people when it travels across the system. The confidentiality is guaranteed by the use of Secure Socket Layer (SSL) and 2 ways SSL between the Central Server and the NCAs. The Web protocol HTTP takes the name of HTTP-S when protected with SSL. SafeSeaNet use the IDA Public Key Infrastructure (PKI) to improve the security of transaction. The main function of PKI is to produce a certified public key or Certificate. Only members of an approved Closer User Group have access to the IDA PKI.
- Private Network
The Trans European Services for Telematics between Administrations is a private Wide Area Network accessible to Members States and European Institutions. TESTA can be seen as a secure network split from the Internet.

Detailed information on security measures is provided further in the Interface Control Document.

2.4 Definition:

For the purpose of the system, unless expressly provided otherwise:

- a) *Person on board* means every person alive on board, without any consideration of function or age.

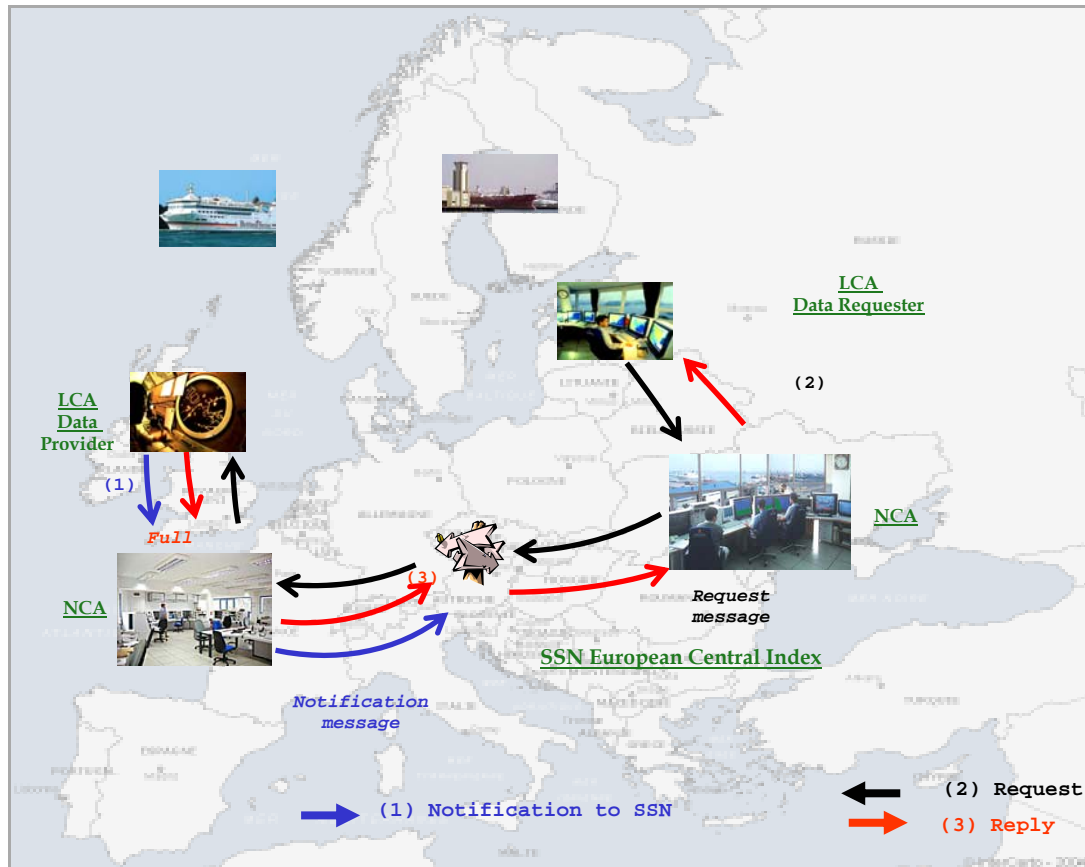


Figure 2/1 Distribution principle

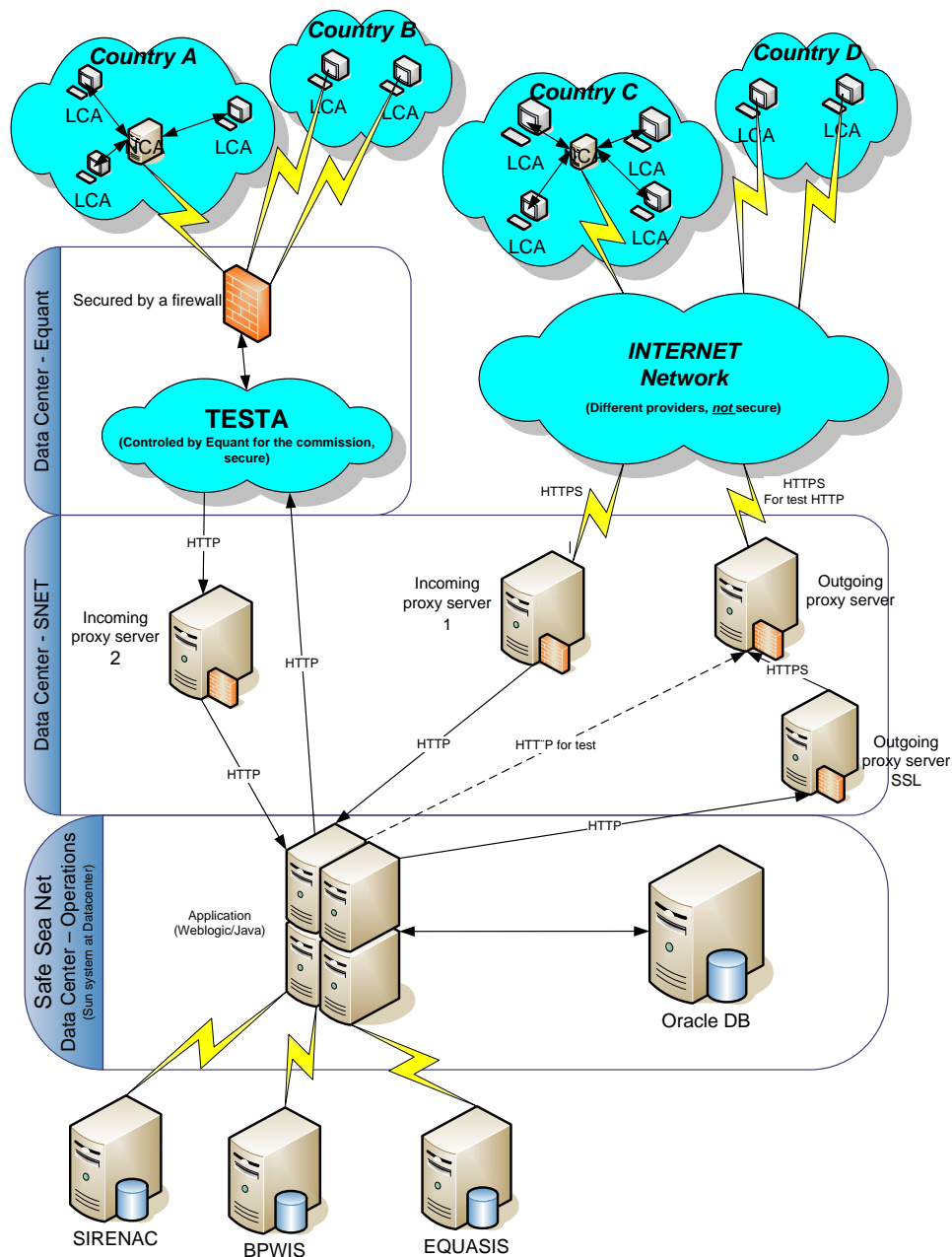


Fig.2/2.General Architecture

3 SAFESEANET PARTICIPANTS

3.1 Parties involved

Parties involved in the SafeSeaNet system are:

- The Members States of the European Union and associated Member State
- The European Union institution

3.1.1 Members State Stakeholders

The Members States are involved in the system through different participants:

- Member States authorities:
 - National Competent Authority (NCA): Body designated by Member States responsible of the management of the system at national level. It co-ordinates all required action with objective to comply with the specification described in the Interface Control Document.

The NCA is the only national authority in contact with the European Union Institutions for the matters related to SafeSeaNet as such it takes part to the management and the development of the system at EU level by participating to periodical review. NCA is also responsible to designate his associated Local Competent authorities and deliver and maintain their access right to the SafeSeaNet network.

NCA could be involved or not for handling and exchanging the SafeSeaNet messages related to the maritime safety and the traffic-monitoring directive.
 - Local Competent Authority (LCA): the authorities and organisations designated by Member States to receive and transmit information pursuant to Directive 2002/59EC.

The LCA are all the local stakeholders involved in the handling of maritime information. The NCA will designate at which level LCA's participate in the SSN network e.g. Port authorities, Coastal Stations, Vessel Traffic Service, shore-based installation responsible for a mandatory reporting system approved by the IMO, or bodies responsible for co-ordinating search and rescue operations...
- Member States network organisation:

At national level circulation of information between authorities could be organised in different way. In SafeSeaNet system two different situations could occur:

 - Single point of contact (SPOC): When a member States organise all the SafeSeaNet transfer of data through a single National Contact Point (NCP). This NCP is the national system in charge of handling and exchanging the SafeSeaNet messages with the European Index Server. The NCP communication system should be available on a 24h a day basis, 7 days a week.

In this case each National Competent authority must preferably provide a NCP single address (URL) for sending and receiving XML messages. This single address provided for every NCP application will be used by the central SafeSeaNet system to send XML messages (requests and responses) to the point of contact.

- Multiple point of contact (MPOC): When there is no national network concentrating the information to a National Contact Point, the national authorities decided to work with multiple points of contacts connected to the Local Competent Authorities.

Whatever national system is defined, it is the responsibility of the Member State to manage and guarantee that the data requested by SafeSeaNet is always available. The management of the one-to-many relationship remains the responsibility of the Member State.

3.1.2 European Union Institutions

- The European Union Institutions are involved in the system through:
 - The Commission (DG TREN): On the basis of its legal obligation under Directive 2002/59/EC, the Commission represented by DG TREN assume the political responsibility for the SafeSeaNet system.
 - EMSA: Established by Regulation 1406/2002 of the European Parliament and of the Council of 27th June, EMSA assume the operational responsibility of SafeSeaNet system such as general monitoring of the European Index Server. EMSA also co-ordinate the participation of the Members State to the system, and is in charge to edit the statistics.
- European Union network:
 - The European Index Server (EIS): hosted for the time being by the Informatics Directorate of the Commission (Luxembourg), the EIS is composed of the Central Index, the European Database (yellow pages) and a Web Server (http/https protocol). The EIS is able to locate and retrieve in a Member State the information required by another Member State and forward it to the requesting Member State.

3.2 Agreement of the parties

- Member States agreement

Each Member State should implement and maintain all necessary equipment, communication interface and access complying with the requirement described within the Interface Control Document and accepted by all participants to the system.

Each Member State should designate and update as necessary the list of National Competent Authority in charge to assume the overall responsibility of the proper functioning of the system at national level.

Each Member State should exchange information with the participants of the system in accordance with the specification described at section 4 of the Interface Control Document.
- European Union Institutions

European Union Institutions should undertake all actions regarding the management and the maintenance of the European Index Server as defined at section 3.1.2 of the Interface Control Document for maintaining the SafeSeaNet system operational and compliant with the procedures and specifications as described within the ICD.

4 SAFESSEANET FUNCTIONS

SafeSeaNet provide to participants the capability for exchanging information available in a Member State and retrieve information exchanged within a predefined area.

For that SafeSeaNet provide the function of Notification of data and the function of Request of data. When a participant acts for notifying the system, it plays the role of Data Provider. When it acts for requesting the system, it is a Data Requester.

4.1 Definition of a Data Provider

A "*Data Provider*" is an LCA as described at section 3.1.1 or a National Competent Authority owning some information about vessels or incidents, and making it available to end user by sending notifications to SafeSeaNet and responding to requests for detailed information.

4.1.1 Responsibility of a "Data Provider"

The responsibility of a "Data Provider" is twofold. It must:

- Send in accordance with a specified time as described at section 5 of the Interface Control Document, the notification to SafeSeaNet EIS about vessels and incidents, indicating that it owns some detailed information about these notifications, which is made available on request. The Data provider should properly validate the information notified to the EIS in order to guarantee their conformity.
- Respond in accordance with a specified time as describe at section 5 within the Interface Control Document to SafeSeaNet requests for detailed information about notifications.

4.1.2 SafeSeaNet Supplied Interfaces for Data Provider

SafeSeaNet provides two different interfaces to enable Data Provider to exchange messages with the central SafeSeaNet system:

- the default browser-based web interface,
- The XML message-based interface.

4.1.3 Data Provider capabilities

Data provider sends by Internet a notification to SafeSeaNet, indicating that it owns information available for other participants.

The distribution of information stored by the Data provider can be done by three different ways depending on its capabilities for providing the detailed content of the notification:

- data provider does not have any application server nor web server (Database) to serve detailed information:
If a LCA request the information stored by that Data Provider, SafeSeaNet will merely send back in the response to the *data requester*, the "data provider" contact details (contact person name, phone, fax and email as defined in the central SafeSeaNet configuration database or supplied in the notification message).

This procedure should only be applied by small entities (Port, coastal station) not equipped with their own database.

- data provider has a local (national) web server where it may store documents (pdf, doc, format):
Corresponding to the information the data provider owns (Port, ship, Hazmat, Alert/Incident notification), SafeSeaNet Central Index Server will fetch the document

from the web server and send it back, Base64-encoded, in the response to the *data requester* (note that the URL of the document must have been given in the notification message).

- Data provider has implemented the SafeSeaNet XML messages specifications. SafeSeaNet will ask the *data provider* to send back the detailed information in XML format. SafeSeaNet will then send the XML response to the *data requester*.

4.2 Definition of a Data Requester

A “data requester” is a LCA [as described at section 3.1.1 or a National Competent Authority](#) asking SafeSeaNet to get information about a port, a vessel or incidents in an area. This information is based on previous notifications sent by a “data providers”.

4.2.1 Responsibility of a “Data Requester”

A data requester should only request data in regard with his normal duty or relevant to a specific event where it has been involved.

When a “data requester” request detailed information about a notification, SafeSeaNet will ask the corresponding “data provider” to get the detailed information and send it back within a specified timing to the “data requester”.

4.2.2 SafeSeaNet Supplied Interfaces for *Data Requester*

SafeSeaNet provides two different interfaces to enable Data Requester to exchange messages with the central SafeSeaNet system:

- the default browser-based web interface,

In terms of data requester needs, the default browser-based web interface provides *data requesters* with a rich interface for getting detailed information about any of the sent notifications (provided they have been granted access to) right out-of-the-box, i.e. without implementing anything. Obviously, such browser-based web interface implies user interaction in terms of keying in information and reading displayed information, and, therefore, cannot be used to communicate automatically and programmatically with the SafeSeaNet system

- The XML message-based interface.

The XML message-based interface supplied by SafeSeaNet enables automated communication between a NCA application and the SafeSeaNet system. The XML message-based interface consists of a set of XML messages fulfilling the needs of both *data requester* and *data provider*.

5 MESSAGING PROCEDURE

5.1 Presentation

There are four different types of messages exchanged within SafeSeaNet;

- Notification,** sent from Member State when they have any information to share
- Request,** sent from Member State when they need information
- Receipt,** confirmation sent from SafeSeaNet
- Response,** sent from Member State when they are asked to do so

5.2 Notification

SafeSeaNet provide notification message hereafter described. All messages are adapted to different situation as detailed at Table 5/1 – Notification Messages Description.

Up to now, 8 different messages has been approved by the Member States. For each individual message, different fields containing the information are linked.

Some fields are common for all the defined messages.

- ✓ *Ship name*
- ✓ *IMO number*
- ✓ *Call sign*
- ✓ *MMSI number*

The link between the information messages and the fields identified for each message is detailed below at Table 5/2.

Type	Message	Description
Generic Notification	Port	Used to notify SafeSeaNet that a given vessel is bound for a particular port with an estimated time of arrival and with a number of persons aboard. Note that the destination port can be 'unknown' (then canceling a previous port notification).
	Ship	Used to notify SafeSeaNet about a ship's voyage and cargo information. A ship notification is essentially based on Mandatory ship Reporting System or AIS message.
	Hazmat	Used to notify SafeSeaNet that a given vessel carries dangerous goods and that the sender owns some detailed information about these dangerous goods
	Security	Used to notify SafeSeaNet that the sender holds some security information about a given vessel.
Alert Notification	Ship Identified	Used to notify SafeSeaNet that the sender holds some information about specific incidents like SITREP, POLREP, Waste, lost/found containers. An alert can be linked or not to a particular vessel.
	Ship Not identified	Used to notify SafeSeaNet that the sender holds some information about specific incidents like SITREP, POLREP, Waste, lost/found containers. An alert can be linked or not to a particular vessel.
E-mail notification	Send E-mail	Used to send message of notification when appropriate, and support the system information (system status change).

Table 5/1 – Notification Messages Description

5.2.1

PORT NOTIFICATION

General procedure

When a Port (LCA) receive from a ship's operator, agent or master the mandatory notification of ship for entry into port, the Port (LCA) should forward in a specified timing as indicated hereafter a "Port Notification" message to SafeSeaNet Index Server.

When a Port (LCA) receives from a ship's operator, agent or master an updated Port notification message where the new E.T.A. or/and E.T.D. has changed by 2 hours or more from the previous notification, the Port (LCA) should sends in a specified timing a revised Port Notification message to SafeSeaNet Index Server

Port of destination change

In case the Port of destination change during the voyage of the ship, the initial port of destination when informed of the change should forward a Port Notification message to SafeSeaNet Index Server with the revised "Port of destination" or if necessary set to Unknown.

Multi port of destination

Ship berthing in multi consecutive ports for a short period of time must notify every port of destination. Taking into account the delay of transmission, the message of port notification may reach SafeSeaNet Index Server not in chronological order. The chronological order will be reconstituted with the available information of Estimated Time of Arrival (ETA) by the SSN CES. The SafeSeaNet interface will retain the last [five] Port Notification messages for managing the chronological arrangement.

Message Timing Requirement

A Port (LCA) receiving a port notification from a ship agent/operator should notify the SafeSeaNet Index Server within 15 minutes if the Port (LCA) is using the XML interface or 60 minutes if the Port (LCA) is using the Web interface.

The SafeSeaNet Index Server should reply a message of acknowledgement within one minute after having received the message.

Communication requirement

In case of communication fail after five attempts, the sender of the message should inform the recipient by any available mean (tel., fax).

In case of SafeSeaNet Index Server receiving a corrupted message, a message of error should be forwarded to the sender.

5.2.2 SHIP NOTIFICATION

General procedure

A LCA (as described at section 3.1.1) should send a ship notification message for a mandatory ship entering and leaving its area of competence. The maximum elapsed time between two messages should not exceed 2 hours, otherwise an intermediate ship notification message should be send.

When the time within a VTS area is less than one hour, a single message should be send.

The LCA should verify the ship is complying with the mandatory reporting requirement and correct the port notification details contained in the SafeSeaNet Index Server as appropriate.

Message Timing requirement

A LCA collecting a ship notification from a ship entering its area of competence should forward a [Ship](#) Notification message to SafeSeaNet Index Server within 15 minutes if the LCA is using the XML interface or 60 minutes if the LCA is using the Web interface.

The SafeSeaNet Index Server should reply a message of acknowledgement within one minute after having received the message.

Communication requirement

In case of communication failed after five attempts, the sender of the message should inform the recipient by any available mean (tel., fax).

In case of SafeSeaNet Index Server receives a corrupted message, a message of error should be forwarded to the sender. A corrected message should be readdressed as soon as possible.

5.2.3 HAZMAT NOTIFICATION

General procedure

When a LCA receive from the operator, agent or master of a ship the notification of dangerous or polluting goods carried on board, the LCA should forward in a specified time a Hazmat Notification message to SafeSeaNet Index Server.

Hazmat message Detail

The “Hazmat Notification details” document should be provided by the LCA on request and accessible by authorised participants.

The address where the “Cargo Manifest” document is accessible should be provided by the LCA on request and accessible by authorised participants.

Timing requirement

A LCA receiving a “Hazmat Notification from the operator, agent or master of a ship should forward a “Hazmat Notification” message to SafeSeaNet Index Server within 15 minutes if the LCA is using the XML interface or 60 minutes if the LCA is using the Web interface.

The SafeSeaNet Index Server should reply a message of acknowledgement within one minute after having received the message.

Communication requirement

In case of communication fail after five tentative, the sender of the message should inform the recipient by any available mean (tel., fax).

In case SafeSeaNet Index Server receives a message corrupted, a message of error should be forwarded to the sender. A corrected message should be readdressed as soon as possible.

5.2.4 ALERT NOTIFICATION

Ship identified – Ship not Identified

General procedure

A LCA (as described at section 3.1) who originate a message of Alert (SITREP, POLREP, Waste, Lost/found Containers, Others) should send an Alert Notification message to SafeSeaNet Index Server. In certain circumstance, the information may not be linked to a ship (Ship identified – Ship not Identified).

Timing requirement

A LCA generating a message of Alert should forward a “Alert notification” message to SafeSeaNet Index Server within 15 minutes if the LCA is using the XML interface or 30 minutes if the LCA is using the Web interface.

The SafeSeaNet Index Server should reply a message of acknowledgement within one minute after having received the message.

Communication requirement

In case of communication failed after five attempts, the sender of the message should inform the recipient by any available mean (tel., fax).

In case of SafeSeaNet Index Server receives a corrupted message, a message of error should be forwarded to the sender. A corrected message should be readdressed as soon as possible.

5.2.5 SEND E-MAIL NOTIFICATION

General procedure

The application provides the capability for sending an e-mail to a SafeSeaNet recipient. It support the system information set up for the information of all actors on the current system status.

5.2.6 Temporary Measures

Number of person on board

According to the Directive 2002/59EC annex I, there is an obligation to transmit the total persons on board to SafeSeaNet. However, in the particular case where in violation with the Directive, the notification sent by the operator, agent or master does not contain the number of persons on board then, the default value ‘99999’ may be temporary used.

The responsible authority shall take all appropriate measure to obtain the missing information in order to complete the notification sent to SafeSeaNet with the updated total persons on board.

Bound for port Leaving From port	Message	Member State	Out Member State
Member State	Port notification	ETA = port of destination ETD = port of destination	ETA N.A. ETD N.A.
	Hazmat	ETA = port of destination ETD = port of departure	ETA = port of destination ETD = port of departure
Out Member State	Port notification	ETA = port of destination ETD = port of destination	ETA N.A. ETD N.A.
	Hazmat	ETA = port of destination ETD = N.A.	ETA N.A. ETD N.A..

N.A.: Not Applicable

Table 5/2. – Voyage Information Notification

Table 5/3 – List of Notified Data

	<i>Field name</i>	<i>PN</i>	<i>MRS</i>	<i>AIS</i>	<i>HAZ</i>	<i>WAS</i>	<i>INC</i>	<i>PSC</i>	<i>SEC</i>
Static information	Ship name	PN	MRS	AIS	HAZ	WAS	INC	PSC	(SEC)
	IMO number	PN	MRS	AIS	HAZ	WAS	INC	PSC	(SEC)
	Call sign	PN	MRS	AIS	HAZ	WAS	INC		(SEC)
	MMSI number	PN	MRS	AIS	HAZ		INC		(SEC)
	Flag					WAS		PSC	
	Date of construction							PSC	
	Dead-weight tonnage							PSC	
	Configuration (SH, SBT, DH)							PSC	
	Length and beam			AIS					
	Ship's draught			AIS					
	Type of ship			AIS					
	Location of position-fixing antenna			AIS					
Voyage Information	Previous port of call					WAS			
	Next port of call					WAS			
	Port of departure						INC		
	Port of destination	PN	MRS	AIS	HAZ		INC		
	Route plan			AIS					
	ETA	PN	MRS	AIS	HAZ	WAS			
	ETD from current port of call				HAZ	WAS			
	Planned duration of call							PSC	
	Planned operations at port of destination (loading...)							PSC	
	Planned operations survey inspections							PSC	
Persons on Board	Total number of persons aboard	PN	MRS		HAZ		INC		
Dynamic information	Ship's position		MRS	AIS			INC		
	Position time stamp			AIS					
	Date and time		MRS						
	COG		MRS	AIS					

Cargo information	SOG	MRS	AIS					
	Heading		AIS					
	Navigational status	MRS	AIS					
	Rate of Turn		AIS					
	DG on board (Y/N)	MRS						
	If DG, IMO class and quantity	MRS						
	Type of hazardous cargo (DG-HS-MP)		AIS					
	Technical names of DPG			HAZ				
	UN numbers of DPG			HAZ				
	IMO hazard classes (IMDG, BC, IBC , IGC Codes or Marpol Annex I)			HAZ				
	INF Ship class			HAZ				
	Quantities of DPG			HAZ				
	Location on board of DPG			HAZ				
	Identification number of cargo transport units (if not tanks)			HAZ				
Cargo info	Address from which detailed information on the cargo may be obtained	MRS		HAZ		INC		
	Characteristics and estimated quantity of bunker	MRS						
Waste information	Last port where ship generated waste was delivered				WAS			
	Last date when ship generated waste was delivered				WAS			
	Are you delivering all, some or none of your waste into port reception facilities				WAS			
	Type and amount of waste and residues to be delivered and/or remaining on board				WAS			
	Percentage of maximum storage capacity				WAS			
Security	Valid Ship Security Certificate : Y/N							SEC
	Name of issuing authority							SEC
	Current Security level							SEC
	Security level in previous ports							SEC
	Special/additional security measures							SEC

	Confirmation maintenance ship security procedures							SEC
	Other practical security related information							SEC
Incident information	Details of incident or accident					INC		

The 8 messages are defined as follows:

PN	Port Notification
MRS	Ship Reporting System
AIS	Automatic Identification System
HAZ	Hazmat Message
WAS	Waste Notification
PSC	Port State Control
INC	Incident Reports
SEC	Security Notification

5.3 Request

SafeSeaNet provides the Request message described hereafter, these may be adapted to different situation as detailed at Table 5/3 – Request Messages Description.

Request Function	Type Information	Description
Ship	Latest notification	Used to obtain detailed notification about a given ship. Upon receiving such request, SafeSeaNet display the latest available notification, ordered by type and date.
	Voyage history	Used to obtain detailed ETA, next port of call, AIS message about a given ship. Upon receiving such request, SafeSeaNet display the latest available information, ordered by date.
	Incident history	Used to obtain detailed incident about a given ship. Upon receiving such request, SafeSeaNet display the latest available incident, ordered by type and date of notification.
Port	Latest ETA notification	Used to obtain latest ETA notification about a given port associated to a NCA. Access to the information is restricted.
Area*	Identified ships	SITRE P POLRE P Waste Lost/fo und contain ers Other
	Not Identified Ships	
	SIRENAC BPWIS EQUASIS	Used to get a direct access to SIRENAC, Baltic Port Waste Information System or EQUASIS databases.

Table 5/4 - Requests messages description

* Only implemented on the Web Interface

5.3.1

SHIP REQUEST

General procedure

The Ship Request is sent by a Local Competent Authority (as described at section 3.1.1) to SafeSeaNet EIS in order to request the latest;

- ship notification (Port notification, Hazmat, MRS, Security)
- voyage history,
- Incident history details about a given vessel.

The Ship Response message is the response sent by SafeSeaNet Index Server to the Local Competent Authority requesting the latest ship notification details for a given vessel.

Timing requirement

A Local Competent Authority sending a Ship Request message should received the “Ship Response” message within 15 minutes. When the 15 minutes period is exceeded, SafeSeaNet EIS sends a “Ship Response” message to the data requester with the address of the LCA (phone, fax) where the Ship Notification data are available.

A Local Competent Authority receiving from SafeSeaNet Index Server a “Ship Request” message should provide a response to SafeSeaNet Index Server within 10 minutes.

Communication requirement

In case of communication failed after five attempts, the sender of the message should inform the recipient by any available mean (tel., fax).

In case of SafeSeaNet Index Server receives a corrupted message, a message of error should be forwarded to the sender. A corrected message should be readdressed as soon as possible.

5.3.2 PORT REQUEST

General procedure

The Port Request message is sent by a Local Competent Authority (port, VTS, MRCC, etc...) to SafeSeaNet Index Server in order to request the latest port notification details about a given vessel.

The Port Response message is the response sent by SafeSeaNet Index Server to the Local Competent Authority requesting the latest port notification details for a given vessel.

Timing requirement

A Local Competent Authority sending a Port Request message should received the “Port Response” message within 15 minutes. When the 15 minutes period is exceeded, SafeSeaNet central server sends a “Port Response” message to the data requester with the address of the LCA (phone, fax) where the Port Notification data are available.

~~A Local Competent Authority receiving from SafeSeaNet Index Server a “Port Request” message should provide a response to SafeSeaNet Index Server within 10 minutes.~~

Communication requirement

In case of communication failed after five attempts, the sender of the message should inform the recipient by any available mean (tel., fax).

In case of SafeSeaNet Index Server receives a corrupted message, a message of error should be forwarded to the sender. A corrected message should be readdressed as soon as possible.

5.3.3 AREA SEARCH

General procedure

The “Area Search” request provide an overview of all messages transmitted in a given geographical area (Atlantic, North Sea and Channel, Mediterranean West and East part)

A LCA could consult all messages exchanged within a delimited area as detailed in

Table 5/4 - Area Search Access**Timing requirement**

A Local Competent Authority requesting an Area Search consultation should received the "Area Search" information within 5 minutes.

Communication requirement

In case of communication failed after five attempts, the sender of the message should inform the recipient by any available mean (tel., fax).

In case of SafeSeaNet Index Server receives a corrupted message, a message of error should be forwarded to the sender. A corrected message should be readdressed as soon as possible.

Geographical Area	Access Rights
Baltic	Finland, Sweden, Germany, Denmark, Poland, Lithuania, Latvia, Estonia.
North Sea and Channel	Sweden, Denmark, Norway, UK, Germany, Netherlands, Belgium, France
Atlantic	UK, Ireland, France, Spain, Portugal
Western Mediterranean Sea	Spain, France, Italy, Malta.
Eastern Mediterranean Sea	Italy, Greece, Cyprus, Malta
European Union	All Member States

Table 5/5 - Area Search Access**5.3.4 SIRENAC, BPWIS, EQUASYS****General procedure**

SafeSeaNet provide a direct access to the selected database.



Fig. 5/3 - Geographical sorting

5.4 Receipt

5.4.1 Process

General procedure

The goal of the message Receipt is twofold:

- It must be sent by SafeSeaNet as the confirmation message (indicating whether the notification message has been successfully validated and processed, or not) to every notification message received from the Member States.
- When a received response is not well formatted (not XML compliant) or not valid (not compliant to corresponding XSD), this message receipt must be sent to the response's sender to indicate an *InvalidFormat* error.

Timing requirement

A Receipt message should be sent within 1 minute after the reception of the notification message.

Communication requirement

In case of communication failed after five attempts, the sender of the message should inform the recipient by any available mean (tel., fax).

In case of SafeSeaNet Index Server receives a corrupted message, a message of error should be forwarded to the sender. A corrected message should be readdressed as soon as possible.

6 SAFESANET SYSTEM INFORMATION AND TEST

6.1 System information

A configuration management system [will be implemented](#) with the objective to distribute standard messages within the SafeSeaNet network in relation to the operational status of the system. It will concern planned changes of software version, modification of communication interface, modification of communication specification, etc...

All messages exchanged in this framework between NCA and EIS should be sent by the SSN email facility and copied by fax.

6.2 System Status Change

System status changes are the result of System element and System function failures, scheduled maintenance, integration or testing of new System elements. All change of System Status that would impact the working of the SafeSeaNet system will be notified to the participants.

6.2.1 SafeSeaNet Changes of Operational Capabilities

Changes of Operational Capabilities resulting from new equipment or new processing which impact the operation of SafeSeaNet System should be notified by the system administrator to the concerned participants. [The system administrator will provide advance notification as early as possible and at least 24 h00 before implementing.](#)

6.2.2 SafeSeaNet System Failure

System Status change resulting from either a failure or outage of a system element or a system function will be reported as soon as possible to the SafeSeaNet participants.

6.2.3 SafeSeaNet 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 NCAs. The responsible NCA should provide advance notification as early as possible before interrupting operations, including a description of the planned arrangements taken, if any.

6.3 System Test

[This section provide basic guidance on principles governing the performance of test which Member States will endeavour to implement for ensuring efficient System operations.](#)

6.3.1 General guidance

[Before entering in exploitation with SafeSeaNet system, a National authority shall perform a test and provide the data, which is specified in the document "test plan" to the SafeSeaNet system manager \(EMSA\).](#)

[The tests verify the system developed by a Member State is able to provide and received messages exchanged between participants in accordance with the agreed documents specification.](#)

6.3.2 Pre test requirement

Prior to commencing the test, the National Competent Authority under which responsibility the test will be conducted shall notify in advance the SafeSeaNet system manager.

6.3.3 Submission of results – Integration

The result of the test shall be documented in a test report. It includes a test cycle reporting drafted by the test manager in accordance with the test plan and the bug report drafted by the test support contractor.

The complete report and the data files (if any) shall be submitted to the SafeSeaNet manager for further evaluation and presentation to the Participants for subsequent review at the closest Member State meeting.

After review of the test report, Member States makes appropriate recommendation.

6.3.4 Tests Plan

A test plan is developed with objectives to recommend and describe the testing strategies to be employed by participants:

- Identify the functional and non-functional requirements as target for testing,
- Recommend and describe the testing strategies s to be employed
- Identify the required resources
- recommend and describe the test organisation
- provide an approach to test and bug reporting
- Present a list of tests scenarios to execute.

7 SYSTEM SPECIFICATIONS

7.1 Communication Interfaces

The SSN system allows the exchange of information about maritime traffic. To this end, it will collect the information available on a ship at a determined moment, as requested by the EU maritime safety legislation, while being compatible with the procedures used by the operational services.

SafeSeaNet provides two different interfaces to help the Members States communicate with the Central Index Server:

- An XML message-based interface
- A default browser-based web interface

7.1.1 XML message based interface

SafeSeaNet provides an XML message-based interface to enable the NCP applications of the Members State to communicate programmatically with the SafeSeaNet system. The XML message-based interface consists of a set of XML messages fulfilling the needs of both data requester and data provider.

7.1.2 Default browser-based web interface

SafeSeaNet provide a default browser web interface to help Members State communicate manually and visually with the central system. It particularly concerns small entities (e.g. small ports) still receiving the maritime data in paper format. It has been suggested that they scan those paper documents in electronic format and upload them on a web server that will be managed at the responsible Member State level.

The browser-based web interface enables an actor to:

- Manually send notifications to SafeSeaNet by filling in web forms,
- Manually request detailed information about notifications and alerts held on the SSN CIS.

7.1.3 Connection to the Central Index

The interconnection between the NCP and the Central Index Server can be made through three different means:

- The National Network if this exists in the country, and if this is already connected to TESTA. This solution is recommended.
- A permanent connection to a TESTA EuroGate with a leased line;
- The Internet.

It is assumed that the connection of the LCAs (as described at section 3.1.1) is made through the Internet or via a local leased line to the NCP.

At national level, it is recommended for a country to implement a dedicated network linking the LCAs to a unique nodal point acting as SPOC.

A detailed description is available within the SafeSeaNet Network and Security guide.

7.1.3.1 TESTA Connection through the National Network

Nearly all Member States have a National Network, which is connected to the European network TESTA. These National Networks interconnect their administrations as well as other national entities.

Security on TESTA is enforced through the implementation of encryption devices within the National Network ensuring the confidentiality of the information exchange.

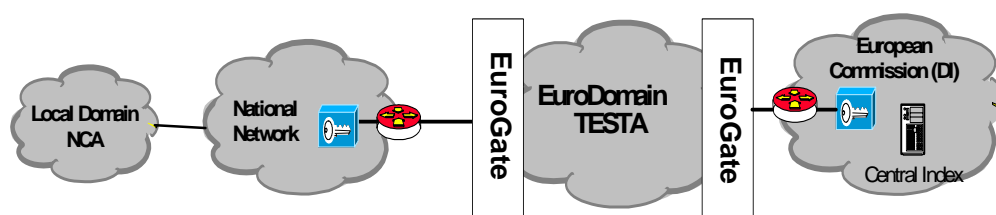


Figure 7/4 – National Network Connection

Sites that are already connected to the National Network are strongly advised to use it for the connection to TESTA. Sites, which are not yet connected to their National Network, but have the possibility to do so, are advised to further implement this interconnection.

7.1.3.2 Permanent Connection Directly to TESTA with a Leased Line

Sites that can't connect to their National Network or prefer not to use such a way of connecting may opt for a direct connection without passing through any intermediate networks. These direct connections are delivered and managed by the contractor of the EuroDomain, Equant. However, Member States are allowed to use their local leased line provider to connect their site to the Eurogate. In this case, the coding device will be put at the Eurogate and the data transiting the leased line will not be coded.

The IDA program is gradually installing encryption boxes at all Local Domain routers connected to TESTA. Priority is given to National Network connections, but directly connected sites will also be equipped if there is a high security requirement. So from a security perspective, this connection type will ensure the data confidentiality between the router of the NCA and the router at the European Commission, giving access to the Central Index Server.

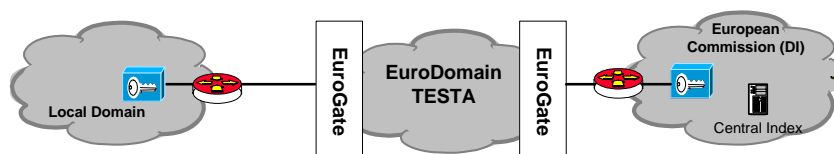


Figure 7/5– Direct Connection

7.1.3.3 Internet Connection

If a Member State chooses for an Internet connection, he has to take a provider that can offer Service Level Agreement fulfilling the conditions of the regulation concerning availability and quality of the service. [A particular attention should be pay to the minimum bandwidth required for satisfying the time specification as described at parag. 7.2.7.](#)

7.1.4 SafeSeaNet Security

7.1.4.1 Security Services

The SafeSeaNet security requirements that must be used by Members State are mainly based on:

- Authorisation
- Authentication,
- Confidentiality.

A description of the organisation of the security is presented at Figure 7/6.

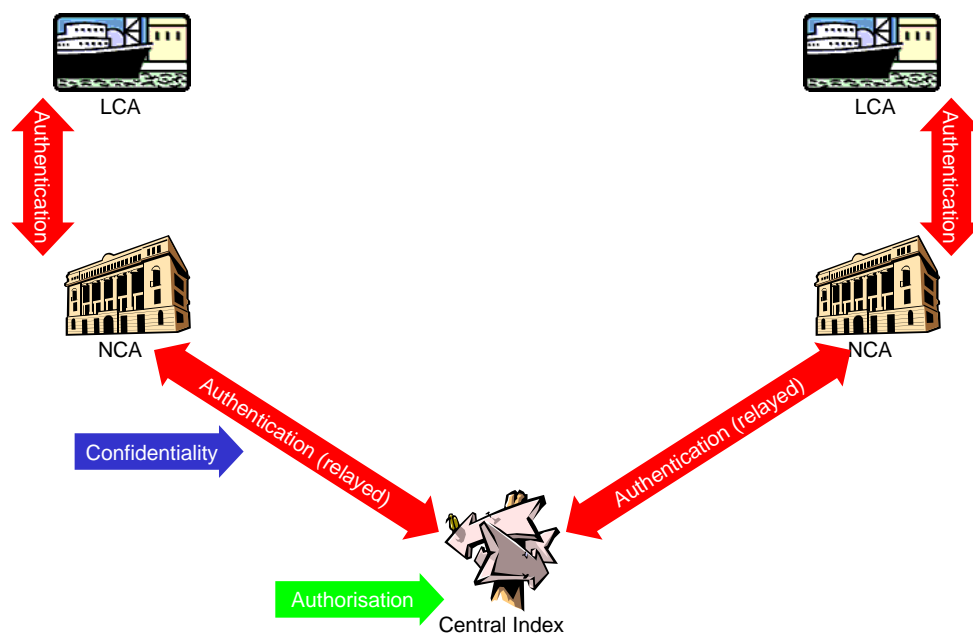


Figure 7/6 - Security Services

7.1.4.2 Authorisation

The most important security service is authorisation. Not all data can be made available to everyone in the system. The authorisation security service ensures that data access is granted only those who are authorised to see the data.

The Central Index manages the authorisation in accordance with the specification agreed by the participants and the roles assigned to each participant (see Table 7/5 Role Code). The current user's access right is summarised in Table 7/6, Users Access Right.

Roles access rights are managed at the system level by the system administrator and can only be modified by a change request submitted by the EMSA.

The NCA Administrator (managing the SSN users in her Member State) may modify these access rights (e.g. removing some access rights) but only within the permitted boundaries of the role, i.e. they may not give more access rights than the default and maximum access rights defined for the role.

The NCAs of the Member States (via their NCA Administrators) will be granted the right to manage their own SSN users for their own Member State using a special web application (administrative interface) provided to them by the central SSN system. Such user management includes adding, editing and removing of SSN users, along with setting their roles and access rights.

7.1.4.3 Authentication

The authentication of transactions exchanged uses the SSL protocol between the NCA and the European Index Server. The SSL protocol is based on the exchange of keys between the NCA and the CIS.

Https (Hypertext Transfer Protocol over Secure Socket Layer or Http over SSL) is a Web protocol that encrypts and decrypts user page requests as well as the pages that are returned by the Web server. Https is really just the use of Secure Socket Layer (SSL) as a sub-layer under the regular Http application layering.

Security solutions using digital certificates rely on PKI cryptography in which each user has a pair of cryptographic keys: one private key that is kept private by the user, and one related public key widely made public.

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

This certified public key can be used to encrypt confidential information to the certificate owner and/or to verify digital signatures generated by the certificate owner.

The certified public key is linked to the private key of the certificate owner in such a way that:

A digital signature is computed from the message and the private key of the signer. It is a small size coded file appended to the signed message. Verification of a digital signature involves the certified public key of the signer. If the check succeeds, the recipient is convinced about its origin and has the guarantee that nothing has been modified in the message since the signature process.

The only way to decrypt a coded message is to use the corresponding private key that is supposed to be known only to the certificate owner.

Digital certificates provide thus solid assurance that a public key actually belongs to the right entity whose identity has been certified by a Certification Authority, a known trusted third party, which controls and confirms the accuracy of the binding between a public key and its legitimate owner.

Digital certificates are the Internet passports that prevent you from disclosing confidential information to unauthorised persons, and/or to deny an impostor's digital signature as authorisation for a critical electronic business transaction.

Procedure to be applied by Member State for implementing such a service is detailed within document SafeSeaNet Network and Security Reference Guide.

7.1.4.4 Confidentiality

The confidentiality service ensures that information is not disclosed to unauthorised people when it travels across the system. The confidentiality will be guaranteed by the use of Https Web protocol.(see figure 7/7 Security Measures)

Between the national web server and the Central SafeSeaNet system which is hosted at the EC premises the Secure Socket Layer (SSL) is used as standard solution. The implementation of SSL at the DI follows a set of strict rules. These rules ensure that the implementation is standard, but it also brings some limitations, such as to end the SSL tunnel at the reverse proxy of the DI for the incoming traffic. Simple SSL will be used for the incoming traffic to the Central Index. Updates and queries to the Central Index generate incoming traffic.

There is no restriction for the outgoing traffic. 2-way SSL will be used here; on the condition that the NCA accepts this method and that this traffic is not blocked at the entry point of the NCA (e.g. by firewall, reverse proxy).

SSL supports digital certificates. The IDA PKI will be used here to produce the NCA's certificate. There will be one IDA certificate for the Central Index for the SSL tunnel of the incoming traffic, and there will be one IDA certificate for each NCP connected to the Central Index for the 2-way SSL tunnel of the outgoing traffic.

Between the NCA/NCP and the End-user, it is recommended to use at least one-way SSL. This means that there are 2 SSL "tunnels" in the path between the end-user and the central index: one between the end-user and the NCA, another one between the NCA and the central index.

The end-user authenticates towards the NCA (who has a list of authorised end-users in his country) and the NCA forwards the identity of the authenticated end-user in the payload sent to the Central Index.

This payload is protected by another SSL tunnel: this means that the chain of trust between the end-user and the central index is maintained.

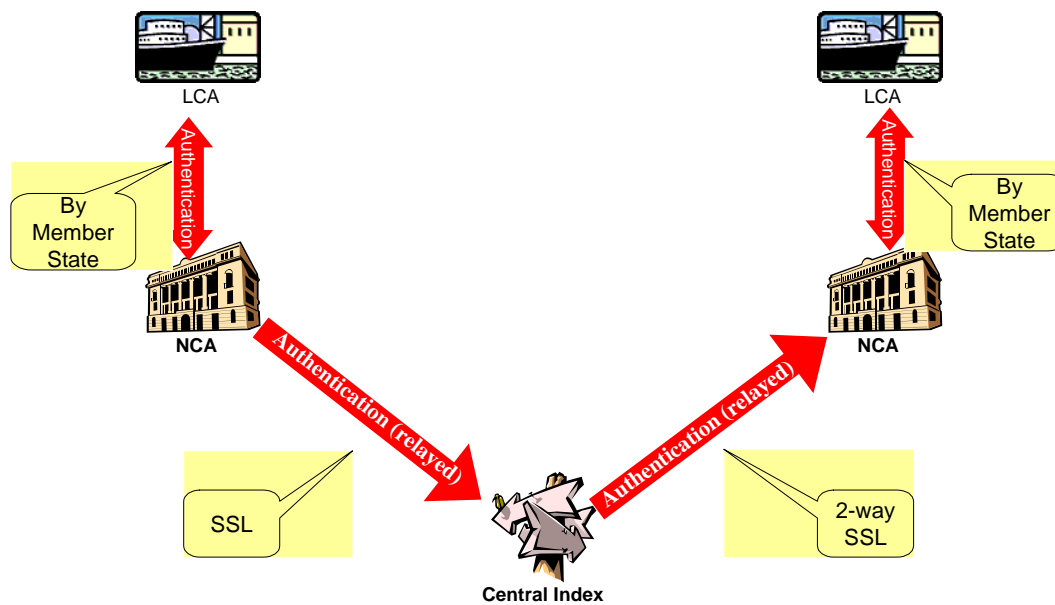


Figure 7/7 - Security Measures

Role Code	Description
POR	Used to identify a Port Authority
CST	Used to identify a Coastal Station
PSC	Used to identify a Port State Control
NCA	Used to identify a National Competent Authority
EMSA	Only used to identify the SSN Administrator (not used by Member States)
OTH	Used to identify anything that's not in the above roles

Table 7/6 - Role Code

Table 7/7 - Users Access Right

	Send Notifications (Web/XML)										Information Requests (Web/XML)										Information Requests (Web only)				
											Notification Details										Ship Search				Port Search
	Port	Ship	Hazmat	Security	Alert					Port	Ship	Hazmat	Security	Alert					Latest Notif.	Voyage	Cargo Manifest	Latest Incidents			
Roles					SITREP	POLREP	Waste	L/F Containers	Others		MRS	AIS			SITREP	POLREP	Waste	L/F Containers	Others						
POR	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y ¹	Y ¹	Y ¹	Y ¹	Y ³	N	N	Y	N	N	Y ¹	Y ¹	Y ¹	Y	Y ¹	
CST	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y ³	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y/N	
PSC	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	
NCA	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	
EMSA	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	
OTH	N ²	N ²	N ²	N ²	N ²	N ²	N ²	N ²	N ²	Y	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	

¹ If the Port Authority is the next port of call

² The granting of an access right would have to be decided on a case by case basis, depending notably on the relevance of the information for the authority or body concerned, and taking protection of confidentiality.

³ To be confirmed (such authorities may have not yet been defined).

Others : could be represented by : Customs, Schengen,

7.2 Operational System Requirements

7.2.1 Overview

The SafeSeaNet system is an important electronic network established between Members States in order to facilitate the implementation of EC maritime safety legislation.

To be effective it 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); and
- e. Accountability (tracking of messages in the system).
- f. Security (confidentiality and authenticity).

To achieve these objectives, the SafeSeaNet system must comply with certain standards. The standards contained in this section provide a framework for the functions of the NCP and the Central Index Server including the transmission of message, performance levels and operating procedures.

Participants that meet specified standards of performance are commissioned to operate within the SafeSeaNet system.

7.2.2 Scope

This specification describes the minimal operational, functional and performance requirements of SafeSeaNet system. This specification also describes the additional requirements to be met by the national administrations and systems connected to SafeSeaNet.

7.2.3. General Operations

The basic operational objective of SafeSeaNet system is to set up an electronic network between the maritime administrations.

Each Member State shall be responsible for establishing procedures for the distribution of messages, system information within its own national area.

A national competent authority shall notify the SafeSeaNet Index Server for information to other participants,

A national competent authority shall respond to direct requests for information from other participants,

A national competent authority shall be capable of counting for all messages, received or transferred through its system.

7.2 3.1 monitoring of national authority

A national competent authority (NCA or MPOC) shall monitor the following System elements in its national area.

A national competent authority (NCA or MPOC) shall monitor the performance of the communication system within its service area to determine degradation of its operational capability.

A national competent authority(NCA or MPOC) shall monitor the local competent authorities (LCA) communication link. The LCAs communication link may be actively monitored (i.e., sending

periodic test messages), or passively monitored (e.g., monitoring the time delay between the forecast message at the LCA and the reception of the message at the NCA, or the LCA/NCA message transfer time).

A national competent authority (NCA or MPOC) shall monitor its own operation to ensure availability and to avoid distributing unreliable or corrupted message.

A national competent authority (NCA or MPOC) shall immediately notify the SafeSeaNet system if it is unable to receive, process, and transmit data according to ICD specifications.

Any detected defects that might affect the SafeSeaNet system shall immediately be reported in accordance with ICD documents section 6.1 (SafeSeaNet System Information), and backup procedures shall be implemented, as appropriate.

7.2.4 Availability of the system

Once SafeSeaNet System has been declared operational, system management shall maintain the system in operation 24 hours a day, seven days a week and personnel shall be available to satisfy the operational and performance requirements documented within the Interface Control Document.

Once a member State has been declared operational, it shall maintain the notified NCP in operation 24 hours a day, seven days a week and personnel shall be available to satisfy the operational and performance requirements documented within the Interface Control Document.

7.2.5 Communication

A national competent authority (NCA or MPOC) shall maintain communication links with the local competent authorities according to operational requirements.

A national competent authority (NCA or MPOC) shall only use communication networks identified in ICD section 7.1 for communications with SafeSeaNet.

A national competent authority (NCA or MPOC) shall maintain communication links with the SafeSeaNet Index Server for the distribution of message and System information as shown in ICD section 5.

A national competent authority shall establish appropriate arrangements with all the local competent authorities in its national area regarding the communication networks to be used for the distribution of message.

A national competent authority (NCA or MPOC) shall implement communication links consistent with the standards and protocols contained in the ICD and annexed documents.

7.2.6. System timing and performance

7.2.6.1 LCA Co-ordination

The national systems connected to SafeSeaNet shall be able to receive and process all messages from its associated LCA.

7.2.6.2 Message Formats

The national systems connected to SafeSeaNet should communicate in any format with the associated local competent authorities.

The national systems connected to SafeSeaNet shall employ only formats specified in ICD document for communications with SafeSeaNet Index Server.

The national systems connected to SafeSeaNet shall be able to interface with XML and Default browser-web communication networks and change the message format, as appropriate (e.g., receive input message from associated the local competent authorities and convert in XML format for transmission to SafeSeaNet Index Server).

7.2.6.3 Backup Provisions

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 affected element must be capable of informing other participants in the SafeSeaNet System network using status messages as defined in the Interface Control Document section 6.1.

7.2.6.4 Information Archival and Retrieval (see Portuguese comment)

The national systems connected to SafeSeaNet shall be able to archive and retrieve all messages and any messages transmitted or received during a defined time frame. The national systems connected to SafeSeaNet shall then be capable of transmitting again the appropriate information to that issued the request.

A national competent authority shall be able to retrieve message using any of the following parameters:

- a. Message Unique Identifier as specified within the XML Messaging Reference guide,
- b. IMO number, MMSI, call sign,
- c. Geographical area,
- d. Locode.

A national competent authority may implement other retrieval modes as determined by national needs.

SafeSeaNet Index Server shall be able to retrieve a message using any of the following parameters:

- a. Message Unique Identifier as specified within the XML Messaging Reference guide,
- b. Starting time/ending time of the search,
- c. Type of message (Notification, Request, etc..),
- d. Message source or destination,
- e. IMO number, MMSI,
- f. Locode.

7.2.7 Performance 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 requirement.

7.2.7.1 Availability

The SafeSeaNet Index Server and shall be available to perform its functions [99%] of the time over a period of one year.

The interruption of service shall not exceed a maximum period of [8 hours].

7.2.7.2. Communication Links

The SafeSeaNet Index Server and NCAs shall implement procedures to ensure that the communication network specifications within the Interface Control Document are met.

The national systems connected to SafeSeaNet shall be supported by data communication links and networks that allow them to transfer notification messages to SafeSeaNet Index Server within [1 minute, 99% of the time]

The ratio of messages lost or corrupted in message transfer between NCA/SafeSeaNet Index Server shall be less than [0.1%.]

A communication network with SafeSeaNet Index Server shall be available 99% of time 365 days a year, 24 hours a day.

The interruption of service shall not exceed a maximum period of [8 hours].

7.2.7.3 Additional Timing Requirements

The national systems connected to SafeSeaNet shall be designed to allow for the following timing requirements:

- [60] Minutes to start up backup procedures,
- [15] Minutes to forward retrieved information to the requesting authority.

7.2.7.4 Message Processing Capacity

The SafeSeaNet Index Server shall be capable of receiving and processing from national systems connected to SafeSeaNet the number of messages as determined by a forecast of the volume of message traffic. The forecast shall take into account:

- a. the actual and forecast volumes of regional maritime traffic,
- b. the actual and forecast volumes of the global maritime traffic,
- c. the message distribution procedures outlined in the "ICD document.

7.2.7.5 Processing Time

SafeSeaNet processing time is the time elapsed between the receipt of message at SafeSeaNet Index Server measured at the incoming point (reverse proxy server) and the transfer of the response to the ad hoc recipient measured at the outgoing point (proxy server) . SafeSeaNet shall process all messages and provide a reply message within [1 minute 99% of the time.]

The interruption of service shall not exceed a maximum period of;

- [for critical incident (system down) 1.5 hours during on line period and 4 hours during off-line period,
-]. For urgent incident (system limited) 8 hours

7.2.7.6 Access to Archived Information

The national systems connected to SafeSeaNet shall archive messages for at least [30 days].

The national systems connected to SafeSeaNet shall respond to requests for archived data and messages from other NCAs within [60 minutes].

The national systems connected to SafeSeaNet shall respond to requests for messages covering the preceding 48-hour period within [30 minutes].

The actual information received will be stored by the NCP for a period of [TBD]

The Central Index Server will store the information during the same period as defined for the NCP, through a database storing the notification messages during the agreed period.

8 STATISTICS

8.1 Edition of statistics

to be developed

8.2 Statistical uses

The data handled by SafeSeaNet are extremely valuable and can potentially be used for a number of statistical applications.

The main user of these statistics would probably be the European Maritime Safety Agency. However, the Commission and the Member States may also be interested in directly receiving statistics concerning their country, a specific region or the whole EU.

The development of statistical functions in SafeSeaNet could even facilitate further the implementation of specific requirements. For instance, under the Paris MOU rules, as well as the requirements of Directive 95/21/EC, Member States have to inspect 25% of individual vessels calling to their ports, which mean that they must count all port entries and retain only individual vessels. If SafeSeaNet would be provided with all port entries data, it could calculate automatically the number of individual vessels and, in advance, the 25% number of ships to be inspected for each Member State.

**ANNEXES
TO THE
INTERFACE CONTROL DOCUMENT**

ANNEX A	MEMBER STATE COMPETENT AUTHORITIES REFERENCE
ANNEX B	NATIONAL CONTACT AUTHORITY (NCA)
ANNEX C	LOCAL COMPETENT AUTHORITY (LCA)
ANNEX D	STATUS OF PARTICIPANTS
ANNEX E/1	DEFAULT BROWSER-BASED WEB INTERFACE DOCUMENTS FOR NOTIFICATION
ANNEX E/2	SHIP (MRS) INFORMATION
ANNEX E/3	HAZMAT INFORMATION
ANNEX E/4	SECURITY INFORMATION
ANNEX E/5	INTERNATIOAL SITREP Format
ANNEX E/6	POLREP FORMAT
ANNEX E/7	LOST/FOUND CONTAINERS REPORT
ANNEX E/8	WASTE ALERT NOTIFICATION
ANNEX F	TYPES OF MESSAGES

ANNEX A – MEMBER STATE AUTHORITY REFERENCE

Member state	Country code	Office Name	Postal Address	Phone Facsimile	Email
Belgium	BE				
Cyprus	CY				
Denmark	DK				
Estonia	EE				
Finland	FI				
France	FR	Direction des Affaires Maritimes et des gens de mer – S/D sécurité maritime	3 place de Fontenoy 75007 Paris 07 SP	Tel : 33 1 44 49 85 20 Fax :	
Germany	DE				
Greece	GR				
Ireland	IE				
Iceland	IS				
Italy	IT				
Latvia	LV				
Lithuania	LT				
Malta	MT				
Netherlands	NL				
Norway	NO				
Poland	PL				
Portugal	PT	IPTM - Institute for Ports and Shipping (Head-Office)	Instituto Portuário e dos Transportes Marítimos Edifício Vasco da Gama, Rua General Gomes Araújo 1399-05 Lisboa - PORTUGAL	+351-21 391 4500 +351-21 391 4600	imarpor@mail.telepac.pt jose.cruz@imarpor.pt paulo.bispo@imarpor.pt
Slovenia	SI				
Slovakia	SK				
Sweden	SE				
United Kingdom	GB				
Spain	ES				

ANNEX B – NATIONAL COMPETENT AUTHORITY (NCA)

COUNTRY NAME	NAME OF NCA	LOC ODE	MAILING ADDRESS	EMAIL ADDRESS	TEL FACSIMILE	URL https://
Belgium	Flemish Maritime Administration		Flemish Maritime Administration VTS Radarcentrale Westelijke Dam B- 8380 Zeebrugge Belgium			
Germany			Maritimes Lagezentrum des Havariekommandos Am Alten Hafen 2, 27472 Cuxhaven Germany			
Denmark						
France						
Greece	Hellenic Ministry of Mercantile Marine		Directorate of Information and Innovative Technologies 18 MERARHIAS st. 18535 PIRAEUS GREECE			
Ireland	Department of Communications, Marine and Natural Resources					
Italy	Italian Coast Guard		Maritime Rescue Coordination Center – National VTS Center Viale dell'Arte 16, 00144 Rome Italy			
Netherlands	Koninklijke Marine Kustwachtcentrum Zeeland Seaports Groningen Seaports		Rijkszee en Marinehaven 1, Gebouw MHKC Port Authority of Port Authority of Delfzijl/Eemshaven Noordersingel 1 P.O Box 20004 9930 PA Delfzijl Municipality			

COUNTRY NAME	NAME OF NCA	LOC ODE	MAILING ADRESS	EMAIL ADDRESS	TEL FACSIMILE	URL https://
Norway	Port of Rotterdam		World Port Center Wilhelminakade 909 /3072 AP Rotterdam – Municipality			
	Port of Amsterdam		Port authority of Ijmuiden, Beverwijk, Zaanstad and Amsterdam De Ruyterkade 7 1013 AA Amsterdam Municipality			
	Port of Scheveningen		(Municipality) Visafslagweg 1 2583 DM Den Haag			
	Netherlands Shipping Inspectorates		-Gravenweg 665 3065 SC Rotterdam Governmental authority			
Portugal	IPTM - Institute for Ports and Shipping (Head-Office)	PTN CA	Instituto Portuário e dos Transportes Marítimos Edifício Vasco da Gama, Rua General Gomes Araújo 1399-05 Lisboa PORTUGAL	imarpor@mail.telepac.pt jose.cruz@imarpor.pt paulo.bispo@imarpor.pt	+351-21 391 4500 Fax: +351-21 391 4600	http://ssn.imar por.pt
Sweden	Swedish Maritime Administrations Planning and Regulations		Slottstsgatan 82, SE-601 78 Norrköping, Sweden			
United Kingdom	Maritime and Coastguard Agency		Spring Place, 105 Commercial Road, Southampton, SO15 1EG			

COUNTRY NAME	NAME OF NCA	LOC ODE	MAILING ADRESS	EMAIL ADDRESS	TEL FACSIMILE	URL https://
-------------------------	--------------------	--------------------	-----------------------	--------------------------	--------------------------	-------------------------

Finland

Spain

ANNEX C – LOCAL COMPETENT AUTHORITY (LCA)

Country name	LCA	Locode	Role	Mailing adress	email address	URL	tel/fax
Belgium							
Germany	Fachstelle für Verkehrstechniken Bundesanstalt für Wasserbau Kisters AG Oldenburg			Herr Werner Brunet Weinbergstraße 11- 13 56070 Koblenz Herr Dr. Ralph Neuhaus Am Ehrenberg 8- 98693 Ilmenau Herr Thomas Mühlhausen Bollmannsweg 8 26125 Oldenburg	wbrunet@fmt.wsv.de Ralph.Neuhaus@baw.de Thomas.Muehlhausen@kisters.de		49-261/9819-2031 49-3677/669-2426 49-441/93602-19
	Havariekommando" Verkehrzentrale Cuxhaven						
Denmark							
France							
Greece							
Ireland							
Italy							
Netherlands	Port of Rotterdam Port of Amsterdam Groningen Seaports Zeeland Seaports Port of Den Helder Port of Moerdijk Port of Harlingen Port of Dordrecht Port of Scheveningen Netherlands Coastguard Shipping Inspectorate	NLRTM NLAMS NLDZL NLVLI NLDHR NLMOE NLHAR NLDOR NLSCE NLDHR NLRTM	POR POR POR POR POR POR POR POR POR NCA/C ST PSC				
Norway							
Portugal	Port State Control	PTPSC	PSC	Instituto Português e dos Transportes Marítimos Edifício Vasco da Gama, Rua General Gomes Araújo 1399-05 Lisboa	imarpor@mail.telepac.pt	ssn.imarpor.pt	+351-213914500 +351-213914600
	Port of Viana do Castelo	PTVDC	POR	Instituto Português e dos Transportes Marítimos–Delegação dos Portos do Norte Porto Comercial	ipn@ipnorte.pt	ssn.imarpor.pt	+351 - 258359500 +351 - 258359550

ANNEX C – LOCAL COMPETENT AUTHORITY (LCA)							
Country name	LCA	Locode	Role	Mailing adress	email address	URL	tel/fax
				4900-056 Darque			
	Port of Leixões	PTLEI	POR	Administração dos Portos do Douro e Leixões, S.A. Avenida da Liberdade 4451-851Leça da Palmeira	correio@apdl.pt	ssn.apdl.pt	+351 - 229990700 +351 - 229955062
	Port of Aveiro	PTAVE	POR	Administração do Porto de Aveiro, S.A. Edifício 9 - Forte da Barra, 3830-565 Gafanha da Nazaré	geral@portodeaveiro.pt	www.portodeaveiro.pt	+351 - 234393300 +351 - 234393399
	Port of Figueira da Foz	PTFDF	POR	Instituto Portuário e dos Transportes Marítimos – Delegação dos Portos do Centro Avenida de Espanha, 3080 Figueira da Foz	geral.ffoz@imarpor.pt	ssn.imarpor.pt	+351- 233402910 +351- 233402920
	Port of Lisbon	PTLIS	POR	Administração do Porto de Lisboa, S.A. R. da Junqueira, 94 1349-026 Lisboa	admin.junqueira@porto-de-lisboa.pt	ssn.porto-de-lisboa.pt	351- 213611000 +351- 213611005
	Port of Setúbal	PTSET	POR	Administração dos Portos de Setúbal e Sesimbra, S.A. Praça da República 2904-508 Setúbal	geral@portodesetubal.pt	safeseanet.portodesetubal.pt	+351- 265542000 +351- 265230992
	Port of Sines	PTSIN	POR	Administração do Porto de Sines, S.A. Apartado 16 7520-953 Sines	geral@portodesines.pt	sicp.portodesines.pt/virtualentity	+351- 269860600 +351- 269860690
	Port of the Portimão	PTPRM	POR	Instituto Portuário e dos Transportes Marítimos – Delegação dos Portos do Sul Cais do Comércio e Turismo, 8500 Portimão	geral.portimao@imarpor.pt	ssn.imarpor.pt	+351- 282450200 +351- 282450230
	Port of Faro	PTFAO	POR	Instituto Portuário e dos Transportes Marítimos – Delegação dos Portos do Sul	geral.faro@imarpor.pt	ssn.imarpor.pt	+351- 289860600 +351- 289860666

ANNEX C – LOCAL COMPETENT AUTHORITY (LCA)

Country name	LCA	Locode	Role	Mailing adress	email address	URL	tel/fax
				Rua Conselheiro Bivar Nº 68, 8000 - 555 Faro			
	Port of Ponta Delgada	PTPDL	POR	Administração dos Portos da Terceira e Graciosa, S.A. Rua Teófilo Braga, n.º 1 9500-247 Ponta Delgada	apsm@apsm.pt	www.apsm.pt	+351- 296285221 +351- 296283390
	Port of Praia da Vitória	PTPVI	POR	Administração dos Portos das Ilhas São Miguel e Santa Maria, S.A. Zona Portuária – Cabo da Praia 9760-571 Praia da Vitória	japah@japah.pt	www.aptg.pt	
	Port of Horta	PTHOR	POR	Administração dos Portos do Triângulo e do Grupo Ocidental, S.A. Av Gago Coutinho e Sacadura Cabral, nº 7 9900-062 Horta	portohorta@mail.telepac.pt	www.aptosa.com	+351- 292208300 +351- 292208315
	Port of Funchal	PTFUN		Administração dos Portos da Região Autónoma da Madeira, AS Av. Sá Carneiro n.3, 4 e 5 9004-518 Funchal	portosdamadeira@apram.pt		+351- 291208600 +351- 291220196
	Port of Caniçal	PTCAN		Administração dos Portos da Região Autónoma da Madeira, AS Av. Sá Carneiro n.3, 4 e 5 9004-518 Funchal	portosdamadeira@apram.pt		+351- 291208600 +351- 291220196
	Port of Porto Santo	Port Authority	PTPOS	Administração dos Portos da Região Autónoma da Madeira, AS Av. Sá Carneiro n.3, 4 e 5 9004-518 Funchal	portosdamadeira@apram.pt		+351- 291208600 +351- 291220196
	Ports of Douro	Port Authority	PTDRO	Instituto Portuário e dos Transportes Marítimos – Delegação Douro Av.Sacadura Cabral, Qta do Paço - Godim 5050-071Peso da Régua	geral.douro@imarpor.pt	ssn.imarpor.pt	+351- 254320020 +351- 254324043

Sweden

ANNEX C – LOCAL COMPETENT AUTHORITY (LCA)

Country name	LCA	Locode	Role	Mailing adress	email address	URL	tel/fax
United Kingdom							
Finland							
Spain							

ANNEX D – STATUS OF PARTICIPANTS

Member State	Status	TESTA	Interface	Comments	National network
Belgium	UT April 2004	TESTA via National Network, TESTA via leased line	Xml		SPOC
Denmark	UT March 2004		Web		TBD
Finland	UT January 2004		Xml		SPOC
France	UT Start 16 Feb. 04		Xml		SPOC
Germany	UT13-16 April 2004		Web		TBD thomas.muehlhausen@kisters.de
Greece	UT March 2004	TESTA via National Network	Web/Xml		SPOC
Ireland	NP				
Italy	postponed		Web		TBD
Netherlands	UT June 2004	TESTA via National Network, Internet	Xml/Web		MOPC Notif in XML format / Request in Web
Norway	UT January 2004	TESTA via National Network			SPOC
Portugal	UT june 2004		Xml		SPOC
Sweden	UT April 2004	TESTA via leased line	Xml		SPOC
United Kingdom	NP			No date	
Spain	NP			No date	
UT: Under test FOC: Full operational capability NP: Non Participant					

ANNEX E/1 - DEFAULT BROWSER-BASED WEB INTERFACE DOCUMENTS
FOR NOTIFICATION

PORT INFORMATION

Vessel identification

IMO Number:

Ship Name:

Call Sign:

MMSI Number:.....

Voyage Information

Next port of call:

Estimated Time of Arrival:

ETD from next port of call:

Total number of persons aboard:

.....

ANNEX E/2 - SHIP (MRS) INFORMATION

Vessel identification

§ IMO Number:

§ MMSI Number:.....

§ Call Sign:

§ Ship Name:

Voyage Information

§ Next port of call:

§ Estimated Time of Arrival:

§ Total number of persons aboard:

§ Reporting date and time:

§ Course over ground (COG):

§ Speed over ground (SOG):

§ Navigational Status:

§ Characteristics and estimated quantity of bunker:

§ Ship position:

o Latitude: Longitude:

Cargo Information

§ Type of cargo:

§ DG on board (Y/N):

§ If DG, IMO class and quantity:

§ Address from which detailed information on the cargo may be obtained:
.....

ANNEX E/3 - HAZMAT INFORMATION

Vessel identification

IMO Number:

MMSI Number:

Call Sign:

Ship Name:

Voyage Information

Next port of call:

Estimated Time of Arrival:

ETD from next port of call:

Total number of persons aboard:

INF ship class:

Cargo Information

DG/PG nr

Technical Name of DG/PG:

UN numbers of DG/PG:

IMO hazard classes (IMDG-IBC-IGC codes):

Gross weight:() Kilo / () Metric tonne

Net weight:() Kilo / () Metric tonne

Location nr of goods: (if not in containers):

Location nr of containers: (if dangerous goods in container)

Cargo transport unit id:

Container location:

Address from which detailed information on the cargo may be obtained:

.....
.....

ANNEX E/4 - SECURITY INFORMATION

Static information

§ IMO Number:

§ Ship Name:

§ Call Sign:

§ MMSI Number:.....

Security

- Valid ship security certificate (Y/N):
- Name of issuing authority:
- Current security level:
- Security level in previous port:
- Special/additional security measures:
- Confirmation maintenance ship security procedures:
- Other practical security related information:

ANNEX E/5 - INTERNATIONAL SITREP Format

TRANSMISSION (Distress/urgency) DATE AND TIME (UTC or Local Date/Time) FROM: (Originating RCC) TO:	
---	--

Item	Title	Description	Example
	SAR SITREP (NUMBER)	To indicate nature of message and completeness of sequence of SITREPs concerning the casualty	SAR SITREP ONE
A.	IDENTITY OF CASUALTY	Name/call sign, flag State	Carbonear/HPHK (US)
B.	POSITION	(Latitude/longitude)	14-20N 064-20W
C.	SITUATION	(Type of message, e.g., distress/urgency; date/time; nature of distress/urgency, e.g., fire, collision, medico)	DISTRESS/23Jul03/AIRCRAFT DITCHING
D.	NUMBER OF PERSONS		4
E.	ASSISTANCE REQUIRED		-
F.	CO-ORDINATING RCC	:	-
G.	DESCRIPTION OF CASUALTY	Physical description, owner/charterer, cargo carried, passage from/to, life-saving equipment carried	CESSNA CITATION III/EXECUTIVE JETS, INC, MIAMI, FL/ ORIGINATOR VERIFIED. AIRCRAFT ON VFR FLIGHT PLAN DEPARTED PORT OF SPAIN TRINIDAD 152100Z EN ROUTE. AGUADILLA, PUERTO RICO/8 PERSON LIFERAFT WITH CANOPY AND SURVIVAL SUPPLIES/FLARES
H.	WEATHER ON SCENE	Wind, sea/swell state, air/sea temperature, visibility, cloud cover/ceiling, barometric pressure	WEATHER ON SCENE UNKNOWN
J.	INITIAL ACTIONS TAKEN	By casualty and RCC	AIRCRAFT ISSUED MAYDAY BROADCAST ON 121.5 MHZ WHICH WAS HEARD BY AIR FRANCE 747. PILOT OF DISTRESS AIRCRAFT GAVE POSITION, STATED BOTH ENGINES FLAMED OUT AND DESCENDING THROUGH 5000 FEET WITH INTENTIONS TO DITCH.
K.	SEARCH AREA	As planned by RCC	NO SEARCH ASSETS AVAILABLE
L.	CO-ORDINATING INSTRUCTIONS	OSC designated, units participating, communications	
M.	FUTURE PLANS		
N.	ADDITIONAL INFORMATION	Include time SAR operation terminated	

ANNEX E/6 - POLREP FORMAT

Address Date time group Identification Serial number	From	To
---	------	----

Part I (POLWARN) is an initial notice (a first information or a warning of a casualty or the presence of oil slicks or harmful substances. This part of the report is numbered from 1 to 5.

Part II (POLINF) is a detailed supplementary report to Part I. This part of the report is numbered from 40 to 60.

Part III (POLFAC) is for requests for assistance from other Contracting Parties, as well as for operational matters in the assistance situation. This part of the report is numbered from 80 to 99.

"BONN AGREEMENT" is for identifying the Agreement in question (other code words "NORDIC" for the Copenhagen Agreement 1971, "BALTIC" for the Helsinki Convention 1974, "DANGER" for the Danish German Joint Maritime Contingency Plan 1982 and "NETHGER" for the Netherlands-German Joint Maritime Contingency Plan 1990). Parts I, II and III can be transmitted all together in one report or separately. Furthermore, single figures from each part can be transmitted separately or combined with figures from the two other parts.

When Part I is used as a warning of a serious threat, the message should be headed with the traffic priority word URGENT

Item	Title	Description	Example
Part I (POLWARN)			
1	DATE AND TIME	The day of the month as well as the time of the day when the incident took place or, if the cause of the pollution is not known, the time of the observation should be stated with 6 numbers. Time should be stated as GMT, for example 091900z (i.e. the 9th of the relevant month at 1900 GMT).	181000z
2	POSITION	Indicates the main position of the incident and longitude in degrees and minutes, and may in addition give the bearing of and the distance from a location known by the receiver	55°33' N - 07°00' E
3	INCIDENT		Tanker collision
4	OUTFLOW	The polluting substance, such as CRUDE OIL, CHLORINE, DINITROL, PHENOL as well as the total quantity in tonnes of the outflow and/or the flow rate, and the risk of further outflow should be mentioned. If there is no pollution, but a threat of pollution, the words NOT YET followed by the substance (for example NOT YET FUEL OIL) should be stated.	Crude oil, estimated 3,000 tonnes
	5 ACKNOWLEDGE	When this number is used, the message (telefax) should be acknowledged as soon as possible by the competent national authority	
Part II (POLINF) "			
40	DATE AND TIME	No. 40 relates to the situation described in numbers 41 to 60 if it varies from number 1.	
41	POSITION AND/OR EXTENT OF POLLUTION ON/ABOVE/ IN THE SEA	Indicates the main position of the pollution in degrees and minutes of latitude and longitude, and may in addition give the distance and bearing of some prominent landmark known to the receiver if other than indicated in number 2. Estimated amount of pollution (eg size of polluted areas, number of tonnes of oil spilled if other than indicated in number 4, or number of containers, drums lost). Indicates length and width of slick given in nautical miles if not indicated in number 2.	The oil is forming a slick 0.5 nautical miles to the South East. Width up to 0.3 nautical miles

42	CHARACTERISTICS OF POLLUTION	Gives type of pollution, eg type of oil with viscosity and pour point, packaged or bulk chemical, sewage. For chemicals proper name or United Nations number if known should be given. Appearance, eg liquid, floating solid, liquid oil, semi-liquid sludge, tarry lumps, weathered oil, Discolouration of sea, visible vapour should also be given as well as any markings on drums, containers	Venezuela crude. Viscosity 3.780 Cs at 37.8°C. Rather viscous
43	SOURCE AND CAUSE OF POLLUTION	Indicates the source of pollution eg from vessel or other undertaking. If from vessel, it should be notified whether the pollution is a result of a deliberate discharge or casualty. If the latter, a brief description should be given. Where possible name, type, size, call sign, nationality and port of registration of polluting vessel should be mentioned. If vessel is proceeding on its way, course, speed and destination should be indicated.	Danish tanker ESSO BALTICA of Copenhagen 22,000 GRT call sign xxxx, in collision with Norwegian bulk carrier AGNEDAL of Stavanger, 30,000 GRT, call sign yyy. Two tanks damaged in ESSO BALTICA. No damage to the AGNEDAL
44	WIND DIRECTION AND SPEED	Indicates wind direction and speed in degrees and in m/sec. The direction always indicates from where the wind is blowing.	270 - 10m/sec
45	CURRENT DIRECTION AND SPEED AND/OR TIDE	Indicates current direction and speed in degrees and knots and tenths of knots. The direction always indicates the direction in which the current is flowing.	180 - 0.3 knots
46	SEA STATE AND VISIBILITY	Sea state indicates the wave height in metres. Visibility should be indicated in nautical miles.	Wave height 2m. 10 nautical miles
47	DRIFT OF POLLUTION	Indicates drift course and speed of pollution in degrees and knots or tenths of knots. In cases of air pollution (gas cloud), drift speed should be indicated in m/sec	135 - 0.4 knots
48	FORECAST OF LIKELY EFFECT OF POLLUTION AND ZONES AFFECTED	Results of mathematical models could indicate eg. arrival on beach with estimated timing.	Could reach the island of Sylt, FRG or further south, NL on the 23rd of this month
49	IDENTITY OF OBSERVER/ REPORTER - IDENTITY OF SHIPS ON SCENE	Identifies who has reported the incident. If it is a ship, name, home port, flag and call sign must be given. Ships on-scene could also be indicated under this item by name, home port, flag and call sign, especially if the polluter cannot be identified and the spill is considered to be of recent origin.	Agnedal, number 43 refers
50	ACTION TAKEN.	Mentions action taken for the disposal of the pollution	2 Danish strike-teams with high mechanical capacity on route to the area
51	PHOTOGRAPHS OR SAMPLES	Indicates if photographs or samples from the pollution have been taken. Contact numbers (including telephone, telefax and telex numbers as appropriate) of the sampling authority should be given.	51 Oil samples have been taken. Telex 64471 SOK DK
52	NAMES OF OTHER STATES AND ORGANISATIONS INFORMED		52 FRG
53 - 59	SPARE FOR ANY OTHER RELEVANT INFORMATION:	eg results of sample or photographic analysis, results of inspections or surveyors, statements of ship's personnel	53 DANGER PLAN is activated
60	ACKNOWLEDGE	When this number is used, the telex/telefax should be acknowledged as soon as possible by the competent national authority	

Part III (POLFAC)

80	DATE AND TIME	No. 80 is related to the situation described below, if it varies from numbers 1 and/or 40.	
81	REQUEST FOR ASSISTANCE	Type and amount of assistance required in form of: - specified equipment - specified equipment with trained personnel - complete strike teams - personnel with special expertise with indication of country requested	81 FRG is requested for 2 strike teams with high mechanical pick-up capacity
82	COST	Information on cost of delivered assistance to be notified to requesting country.	82 FRG is requested for an approximate cost rate per day of assistance rendered
83	PRE-ARRANGEMENTS FOR THE DELIVERY OF ASSISTANCE	Information concerning customs clearance, access to territorial waters in the requesting country.	83 FRG units will be allowed to enter Danish territorial waters for combating purposes or Danish harbours for logistics informing SOSC beforehand
84	TO WHERE ASSISTANCE SHOULD BE RENDERED AND HOW	Information concerning the delivery of the assistance, eg rendez-vous at sea with information on frequencies to be used, call sign and name of Supreme On-Scene Commander of the requesting country or land-based authorities with contact numbers (including telephone, telefax and telex numbers as appropriate) and contact persons.	84 Rendez-vous 57°30' N - 07°00' E. Report on VHF channels 16 and 67. SOSC, Lieutenant Commander Hansen in GUNNAR SEIDENFADEN, call sign OWAJ
85	NAMES OF OTHER STATES AND ORGANISATIONS	Only to be filled in if not covered by number 81, eg if further assistance is later needed by other States	
86	CHANGE OF COMMAND.	When a substantial part of an oil pollution or serious threat of oil pollution moves or has moved into the zone of another Contracting Party, the country which has exercised the supreme command or the operation may request the other party to take over the supreme command	
87	EXCHANGE OF INFORMATION	When a mutual agreement has been reached between two parties on a change of supreme command, the country transferring the supreme command should give a report on all relevant information pertaining to the operation to the country taking over the command.	
88 - 98	SPARE FOR ANY OTHER RELEVANT REQUIREMENTS OR INSTRUCTIONS		
99	ACKNOWLEDGE	When this number is used, the message (telefax) should be acknowledged as soon as possible by the competent national authority.	
	ADDRESS WHERE CARGO INFORMATION CAN BE FOUND		

ANNEX E/7 - LOST/FOUND CONTAINERS (*) REPORT

(*) includes other packaged goods

Item	Title	Description	Example
1	Type of report	A. Loss (ship having lost a or several containers/packages goods) B. Observation (ship noting the presence of containers/packages goods drifting at sea)	
2	SHIP'S IDENTITY	IMO Number/Name/Call Sign/MMSI Number	
3	LAST PRESUMED POSITION OF CONTAINER LOST/LAST SEEN POSITION OF CONTAINERS	Last seen position of container at sea, or last position of ship when the container has presumably been lost	
4	NUMBER OF CONTAINERS		
5	TYPE OF GOODS IN CONTAINERS	DG/PG : Y/N IMO/UN/IMDG Code Number	
	DESCRIPTION OF CONTAINERS	Description of containers: dimension, color, marks, numbers, condition	
	CARGO LEAKING ?	Yes/No/Not visible Description of Pollution	
	WIND DIRECTION AND SPEED	Indicates wind direction and speed in degrees and in m/sec. The direction always indicates from where the wind is blowing.	44 270 - 10m/sec
	CURRENT DIRECTION AND SPEED AND/OR TIDE	Indicates current direction and speed in degrees and knots and tenths of knots. The direction always indicates the direction in which the current is flowing.	45 180 - 0.3 knots
	SEA STATE AND VISIBILITY	Sea state indicates the wave height in metres. Visibility should be indicated in nautical miles.	46 Wave height 2m. 10 nautical miles
	DRIFT OF CONTAINERS	Indicates drift course and speed of pollution in degrees and knots or tenths of knots. In cases of air pollution (gas cloud), drift speed should be indicated in m/sec	47 135 - 0.4 knots
	ADDRESS WHERE CARGO INFORMATION CAN BE FOUND		

ANNEX E/8 - WASTE ALERT NOTIFICATION

(Ship leaving port without having delivered its waste)

Static information

IMO Number:

Ship Name:

Call Sign:

MMSI Number:.....

Description of non-compliance with waste delivery requirements:

.....
...
.....
...
.....
...
Please indicate at least: name of port where waste-delivery was due, time/date where ship left port and reasons why ship should be inspected in next port and any other relevant information

Inspection data (if any):

■ Name and co-ordinates of inspection authority:

.....
■ Deficiencies found during inspection:

.....
■ Action taken:

Authorities notified:

Next port of call:

Other authorities:

ANNEX F – MESSAGES DESCRIPTION

Type of message	Origin	Name	Content	Timing requirement	More XML messaging reference guide
Receipt	Sent by SafeSeaNet to every notification message received from the Member States.	Receipt	Notification message has been successfully validated and processed, (or not) to every notification message received from the Member States. A received response is not well formatted (not XML compliant) or not valid (not compliant to corresponding XSD), this message receipt must be sent to the response's sender to indicate an <i>Invalid Format</i> error.	1min	Section 3.2
Notification	sent from Member State when they have any information to share	Port	Used to notify SafeSeaNet that a given vessel is bound for a particular port with an estimated time of arrival and with a number of persons aboard. Note that the destination port can be 'unknown' (then canceling a previous port notification).	15 min (XML) or 60 min	Section 3.3
		Ship	Used to notify SafeSeaNet about a ship's voyage and cargo information. A ship notification is essentially based on MRS or AIS message.	15 min (XML) or 60 min	Section 3.3
		Hazmat	Used to notify SafeSeaNet that a given vessel carries dangerous goods and that the sender owns some detailed information about these dangerous goods	15 min (XML) or 60 min	Section 3.3
		Security	Used to notify SafeSeaNet that the sender holds some security information about a given vessel.	Not yet implemented	Section 3.3
		Alert	Used to notify SafeSeaNet that the sender holds some information about specific incidents like SITREP, POLREP, Waste, lost/found containers. An alert can be linked or not to a particular vessel.	15 min (XML) or 30 min	Section 3.3
Request	sent from Member State when they need information	Port request	Sent by a Member State (<i>data requester</i>) to SafeSeaNet in order to request the latest port notification details about a given vessel.	15 min	Section 3.4

		Ship Request	Sent by a Member State (<i>data requester</i>) to SafeSeaNet in order to request the latest ship notification details about a given vessel. Re sent by SafeSeaNet to the Member State owning the Ship notification details (<i>data provider</i>) in order to request the latest Ship notification details about a given vessel.	15 min	Section 3.4
		Hazmat Request	Sent by a Member State (<i>data requester</i>) to SafeSeaNet in order to request the latest Hazmat notification details about a given vessel. Re sent by SafeSeaNet to the Member State owning the Hazmat notification details (<i>data provider</i>) in order to request the latest Hazmat notification details about a given vessel.	15 min	Section 3.4
		Security Request	sent by a Member State (<i>data requester</i>) to SafeSeaNet in order to request the latest Security notification details about a given vessel. Re sent by SafeSeaNet to the Member State owning the Security notification details (<i>data provider</i>) in order to request the latest Security notification details about a given vessel.	Not yet implemented	Section 3.4
		Alert Request	Sent by a Member State (<i>data requester</i>) to SafeSeaNet in order to request the incident notification details about a given incident type. Sent by SafeSeaNet to the Member State owning the incident notification details (<i>data provider</i>) in order to request the incident notification details about a given incident type.	15 min	Section 3.4
	Response	Port Response	Sent by SafeSeaNet central database acting as the data provider to the member state (<i>data requester</i>) requesting the latest port notification details about a given vessel.	10 min	Section 3.4
		Ship Response	sent by the Member State owning the notifications details (<i>data provider</i>) to SafeSeaNet in answer to its request for getting the latest ship notification details about a given vessel. The <i>data provider</i> should return the details of the latest ship notification it owns. <u>Final</u> response sent by SafeSeaNet to a Member State (<i>data requester</i>) requesting the latest ship notification details about a given vessel.	10 min	Section 3.5
		Hazmat Response	Sent by the Member State owning the notifications details (<i>data provider</i>) to SafeSeaNet in answer to its request for getting the latest hazmat notification details about a given vessel.	10 min	Section 3.5
		Security Response	<u>Final</u> response sent by SafeSeaNet to a Member State requesting the latest Hazmat notification details about a given vessel (<i>data requester</i>). sent by the Member State owning the notifications details (<i>data provider</i>) to SafeSeaNet in answer to its request for getting the latest security notification details about a given vessel. final response sent by SafeSeaNet to a Member State requesting the latest security notification details about a given vessel (<i>data requester</i>).	Not yet implemented	Section 3.5

Alert Response

sent by the Member State owning the notifications details (*data provider*) to SafeSeaNet in answer to its request for getting the incident notification details about a given incident type.

10 min

Section 3.5

final message sent by SafeSeaNet to a Member State requesting the incident notification details about a given incident type (*Data requester*).the final

SAFESEANET LIST OF DOCUMENTS

Ref.	Technical documentation	Responsible	Status	Last Issue	Comments
Technical Documents					
V. 1.60	SSN XML Messaging Reference Guide	DG TREN	Available	26 Jul. 04	Reference document
V. 1.10	SSN Network and Security Reference Guide	DG TREN	Available	02 Apr.04	Reference document
TEST Description Documents					
V 1.11	SSN Test Plan	DG TREN	Available	19 Dec..03	Reference document
Operational Documents					
	SSN Interface Control Document	EMSA	TBC		Reference document
V. 1.5	SSN User manual -	DG TREN	Available	22 June .04	Reference document
V 1.0	Procedure and Guideline for the Registration of New Web Server Certificates	DG TREN	Available	14 Sept. 04	Reference document

END of ANNEX

- END OF DOCUMENT -