SEVENTH FRAMEWORK PROGRAMME

SST–2007–TREN–1 - SST.2007.2.2.4. Maritime and logistics co-ordination platform

SKEMA Coordination Action

"Sustainable Knowledge Platform for the European Maritime and Logistics Industry"

Deliverable: D2.3.1.4 PRACTICALITIES OF USING SSN AND SAFETY / SECURITY SUPPORT SYSTEMS IN LATVIA.

WP No 2 – SKEMA Consolidation Studies
Task 2.3 European Capabilities for Safety and Security
Sub Task 2.3.1.4 – Practicalities of Using SSN and Safety / Security Support Systems in Latvia
Responsible Partner: MAL
Contributing Partners:
WP Leader: VTT
Planned Submission Date: 1st June 2010
Actual Submission Date: 12th April 2010
Distribution Group: Consortium
Dissemination Level: PU (Public)
Contract No. 218565
Project Start Date: 16th June 2008 **End Date:** 15th May 2011
Co-ordinator: Athens University of Economics and Business

Document summary information

Version	Authors	Description	Date
1.0	Belinskis E., Cernovs H., Gailis A., Sedovs K.	D2.3.1.4 for quality review to VTT	30/11/08
2.0	Belinskis E., Cernovs H., Gailis A., Sedovs K.	D2.3.1.4 for quality review to VTT	13/02/09
2.1	Belinskis E., Cernovs H., Gailis A., Sedovs K.		27/06/09
3.0	Belinskis E., Cernovs H., Gailis A., Sedovs K.		12/04/10

Quality Control

	Who	Date
Checked by Task and WP Leader		
Checked by Peer Review		
Checked by Quality Manager	Antti Permala	
Approved by Project Manager	Takis Katsoulakos	

1 Table of Contents

No.	Content	Page
1	Table of contents	2
2	List of abbreviations	3
3	Introduction	4
4	Objectives	4
5	Goals	5
6	Key areas	5
7	Target Stakeholders	5
8	International requirements regarding maritime information exchange	6
9	National requirements related to shipping security	10
10	SafeSeaNet system	12
11	Concept of the national SSN system	23
12	ISPS data exchange	33
13	Off-line module – way to access the SSN for non-authorized users	43
14	Conclusion	48
15	References	49

2 List of abbreviations

AIS	Automatic Identification System
ARCC	Aeronautical Rescue Coordination Centre
DSC	Digital Selective Calling
EIS	European Index Server
EMSA	European Maritime Safety Agency
EU	European Union
IAMSAR Manual	International Aeronautical and Maritime Search and Rescue Manual
IMO	International Maritime Organization
IMM	International Maritime Mobile
ITU	International Telecommunication Union
ISPS	International Ship and Port Facility Security Code
GMDSS	Global Maritime Distress and Safety System
MARPOL	Maritime Pollution Convention
MAS	Maritime Assistance Service
MRCC	Maritime Rescue Coordination Centre
MRS	Mandatory Reporting System
MSI	Maritime Safety Information
SSAS	Shipping Security Alerting System
Single Window	The concept of the ship reporting process where all information is made available within one window
SOLAS	Safety of Life at Sea Convention
SSN	Shipping-related information exchange system SafeSeaNet
UN	United Nations
LOCODE	UN/CEFACT Location codes
VTS	Vessel Traffic Service
XML	Extensible Markup language

3 Introduction

The prevention of accidents at sea and marine pollution is an essential component of the European Union's transport policy. Since 1993, over 15 proposed Directives or Regulations were initated concerning passenger vessels' safety, prevention of pollution and port state control requirements for seafarers. Their implementation encompasses also the collection and dissemination of maritime data which is the main task of the SafeSeaNet. Since 2002, Member States and the European Commission have been working together to develop a practical solution for the exchange of information concerningship safety records, cargo and port destinations.

This document will discuss the information relating to the cargo and shipping vessel and transfer of these details between the port of departure, the ship and the destination port. A comparison will be made between requirements in European and Latvia with the aim of providing a single form for all authorities. The need for a single window system will be outlined for faster and more efficient transfer of goods, and tracking of other materials.

4 Objectives

- Directive 2002/59/EC of 27 June 2002 is aimed at establishing a vessel traffic monitoring and information system in Europe. To achieve these objectives, the European Commission initiated the development of the infrastructure network, SafeSeaNet (SSN).
- Information contained in the SafeSeaNet system, and mandated by the safety and security at sea legislation, is often similar or even identical to information requested by other information systems. To avoid unnecessary duplication, the Latvian national SSN system was created collate information for each of the maritime authorities.

5 Goals

The exchange of information is often made difficult for a number of reasons: institutions, like port authorities, use different approaches to collate, store and transfer data; IT systems are incompatible with each other; and information is transmitted by different means (fax, tel, email).

The goals of this study are to provide:

- a general view of SSN basics and development capabilities based on experience in Latvia;

- a concise view of SSN as a tool for shipping security information flow amalgamation, plans for its development, and legislative requirements based on the Latvian experience.

6 Key areas

- Related international and national legislation;
- Shipping security-related information:
  - AIS
  - ISPS
  - SSN
- National SafeSeaNet system architecture:
  - NCA
  - LCA
  - Users
- „Single window" concept solution for the national SSN;
- Recommendations for improvement.

7 Target Stakeholders

Maritime safety requires coalescence of data exchange between the vessels and maritime authorities for adequate information about the real time situation. The main players in this process include:

- Policy makers;
- Ship and port operators;
- Authorities related to the shipping safety and security;
- Ship masters.

8 International requirements regarding maritime information exchange

In order to organize maritime data exchange, the European Maritime Safety Agency (EMSA) developed a European maritime data exchange infrastructure named SafeSeaNet. SafeSeaNet is a European Platform for Member States' maritime authorities and is a network solution based on the concept of distributed databases.

Approach

EU member states are obliged to establish national electronic data exchange systems for shipping security. These systems shall be created as a part of the joint SafeSeaNet (SSN) concept. Oher maritime data exchange systems are simultaneously requesting similar information for integration into national SSN systems.

Also, ports do not obtain a lot of additional benefits from the SafeSeaNet as they already may obtain all necessary information from other sources. Furthermore, ports are core elements in the SafeSeaNet system and new requirements for the system also mean additional investments.

According to Directive 2002/59, Member States were required to complete their SafeSeaNet (SSN) national systems and interlink them for exchange of five basic messages (Port, Hazmat, Ship, Security and Alert notifications) by the end of 2008. Implementation of the SSN began in 2002, and the technical specifications remained unchanged until 2009 in order to give the necessary time to all Member States to comply with the requirements of the first SSN version. Only a few Member States were not able to provide this data exchange within the SSN by the end of 2008. This was clearly shown in monthly reports released by the EMSA and made available for analysis by the Commission and Member States. These reports are available on the EMSA homepage as well as being distributed regularly to the National Competent Authorities. For example, such comments as follows were provided by the EMSA in August, 2008:

- Out of the twenty-four coastal countries, eighteen have successfully completed their tests and eighteen are already participating and exchanging messages (two using only the web interface).

- Iceland, Ireland, Latvia and the UK have joined SSN in the second quarter of 2008.

- In April 2008, Italy ceased communication with SSN due to technical problems.

- Bulgaria, Estonia, Greece and Romania were recently visited by EMSA experts who provided them with support concerning the acceleration of SSN implementation. Estonia and Romania have signed the contracts; Greece is currently drafting technical specifications, while

Bulgaria is awaiting approval of the financial resources. All these Member States confirmed their participation in SSN by the end of 2008[1].

According to the definition: "SafeSeaNet means the Community maritime information exchange system developed by the Commission in cooperation with the Member States to ensure the implementation of Community legislation…". The following requirements to the system are prescribed:

- Member States shall establish and maintain national SafeSeaNet systems allowing the exchange of maritime information among authorities at national level, under the responsibility of a National Competent Authority (NCA);

- Member States shall enable the receipt and exchange of information related to maritime safety, port and maritime security, marine environment and the efficiency of maritime traffic and maritime transport;

- National SafeSeaNet systems shall enable the inter-connection of all National Competent Authorities (NCAs) - (ports, coastal stations and others) and shall be able to be accessed by the identified shipping actors (ship owners, agents, masters, shippers and others) when authorized to do so. Member States (dedicated NCAs) should ensure the national co-ordination of data users and data providers, the establishment and maintenance of the necessary national IT infrastructure, and the procedures as described in the "Interface and Functionalities Control Document" referred to in paragraph 2.3;

- Systems shall use standards from the industry and have the ability to interact with public and private systems used to create, provide or receive the information within SafeSeaNet. The functionality of the national systems shall be developed in such a way as to enable the data providers, including masters, owners, agents, operators, shippers and relevant authorities, to submit the information only once.

[1] SafeSeaNet implementation Second quarterly (April, May and June 08). Lisbon, 09 July 2008 Ref: C.2.1/Ops/QR2/2008

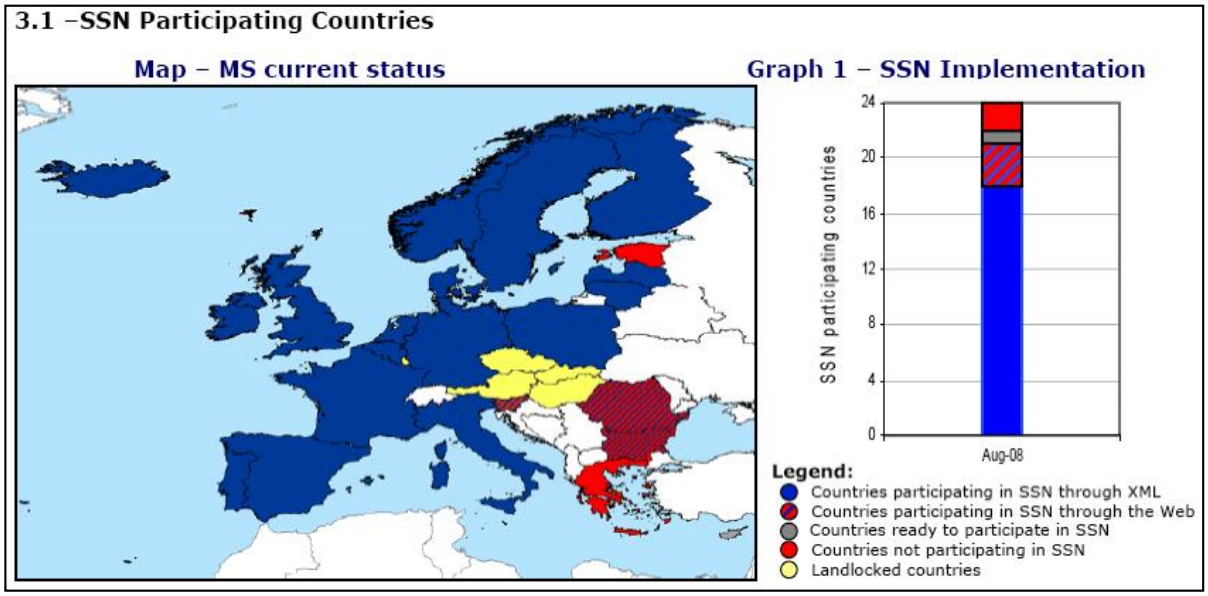

Figure 1. SSN implementation on August, 2008[2]

The main target for Directive 2002/59/EC is to establish a vessel traffic monitoring and information system in the Community *"with a view to enhancing the safety and efficiency of maritime traffic, improving the response of authorities to incidents, accidents or potentially dangerous situations at sea, including search and rescue operations, and contributing to a better prevention and detection of pollution by ship".*

Based on this, the major SSN objectives are:

- Development of a European Platform for Maritime Data Exchange among the EU maritime administrations;

- Setting-up a network between all of the EU maritime Member States for their cooperation in preventing maritime pollution and accidents at sea;

- Creating this network taking into account common technologies and standards such as XML and Internet/TESTA networks;

- Providing the flexibility to deal with future technological developments.

SafeSeaNet-related documents name the following basic requirements for the system's interoperability:

- Availability 24 hours/day, 365 days/year;

[2] SSN monthly report, August 2008. EMSA.

- Flexibility - a platform shall be ready for the new requirements coming from EC legislation, new types of messages, new members in the network, etc.

- Security - for communications and data confidentiality;

- Independence - from the national information handling systems.

In accordance with the related publications, SafeSeaNet users are divided into 3 levels[3]:

• Local Competent Authorities (LCA): port authorities, coastal stations, institutions;• National Competent Authority (NCA): national point of contact and the administrative institution;

• Central European (index) server – system „cross point", hosted by the Informatics Directorate of the Commission until May 2009 and by the EMSA afterwards.

The main capabilities of the SSN project aims to provide:

a) Situation awareness - SAR authorities share information with other Member State SAR authorities;

b) Early warning – relevant authorities are informed about approaching vessels;

c) Target tracking –delivery of information about a specific vessel between the maritime monitoring centres;

d) Semi-automatic ship reporting - ship agents or masters can send a report. Within the integrated EU network it will then be automatically distributed to other Member States;

f) Risk assessment - data analysis for traffic planning;

g) Incident investigation - investigations of collisions, groundings, pollutions, etc.

Exchange of information is based on the following scheme: a ship approaching territorial waters of an EU state or leaving the harbour must send certain information to the national SSN server for the subsequent information exchange within the EU.

[3] SSN ICD, Version 1, Article 2.2.

9 National requirements related to shipping security

The Republic of Latvia has introduced several national regulations to ensure compliance with EU regulations on shipping safety, for example:

- The latest adjustments to the Law on ports of the Republic of Latvia[4],

- Regulation Nr.199 "Procedure for control of dangerous and hazardous cargo in ports"[5] of the Cabinet of Ministers (related to requirements of EU Directive 2978/94/EC),

- Regulation Nr.592 "Order of reports of dangerous and hazardous cargo"[6] of the Cabinet of Ministers (related to requirements of EU Directive 2002/59/EC);

- Regulation Nr.747 "Registration of ship passengers"[7] of the Cabinet of Ministers (related to requirements of EU Directive 98/41/EC);

- Regulation Nr.373 "Supervision of Classification societies"[8] of the Cabinet of Ministers;

- Regulation Nr.248 "Regulation on fishing vessel safety" of the Cabinet of Ministers.

This legislation was introduced based on international regulations and EU practices, and was aimed at regulating organizations involved in shipping safety business. Besides this, there was also specific legislation created for implementing SafeSeaNet.

1) Article 36 of the Maritime Administration and Marine Safety[9] law states that ships entering waters of Latvia or leaving the Latvian port with dangerous and hazardous cargo onboard must report to Latvian authorities before leaving the last port of call (for incoming port calls) as well as prior to leaving the Latvian port (for outgoing port calls).

2) Article 7 (4) of the Maritime Administration and Marine Safety law stipulates a responsibility for the Latvian Coast Guard Service to ensure transfer of data on vessel traffic and other relevant information,,and system functioning in compliance with EU requirements.

3) Article 17 of Regulation Nr.826 "Exchange of Data in EU system" of the Cabinet of Ministers (03.10.2006) states:

---

[4] Law on ports: Republic of Latvia law: 22.06.1994., *Latvijas Vēstnesis*,12.07.1994. nr. 80;

[5] Procedure of control of dangerous and hazardous cargo in ports: Cabinet of Ministers 14.03.2006. regulation Nr.199, *Latvijas Vēstnesis,* nr. 47 (3415), 22.03.2006.

[6] Order of reports of dangerous and hazardous cargo: Cabinet of Ministers 09.08.2005. regulation Nr.592, *Latvijas Vēstnesis,* nr. 126 (3284), 11.08.2005.

[7] Registration of Passangers: Cabinet of Ministers 23.12.2003 regulation nr. 747, *Latvijas Vēstnesis,* 183 (2948) 30.12.2003.

[8] Supervision of Classification societies: Cabinet of Ministers 09.05.2006 regulation nr.373, *Latvijas Vēstnesis*, 168 (2743), 19.11.2002.)

[9] Maritime Administration and Marine Safety Law -- with amendments, *Latvijas Vēstnesis*, 19.11.2002

- The Latvian national competent institution in the framework of the EU SafeSeaNet system is the Latvian Coast Guard Service MRCC Riga;
- The responsibility of the Latvian Coast Guard Service is to ensure proper functioning of the national SafeSeaNet system according to directive 2002/59/EC;
- The Latvian Coast Guard Service is responsible to provide access to a national system for LCAs;

4) Article 18 of Regulation Nr.826 of the Cabinet of Ministers prescribes that MRCC Riga creates and maintains infrastructure to ensure data transmission, reception, and transformation among the systems, and ensures compatibility between the national and EU systems.

The Maritime Administration and Marine Safety Law of the Republic of Latvia applies on all ships in the Latvian Ship Register regardless of berthing place, foreign ships in the waters of jurisdiction of Latvia, and all other subjects relating to shipping safety[10]. The Law also prescribes the state institutions responsible for executing maritime administrative functions such as: Ministry of Transportation, Hydrographic Service of Maritime Administration of Latvia, Latvian Coast Guard Service, Marine Environmental Protection Authority and Latvian Port authorities[11]. One of these functions, according to Article 5(6), Article 7(1) and Article 9 of the Law, is supervision of shipping regulations in waters under the jurisdiction of the Republic of Latvia. Therefore, the national legislation of Latvia provides a legal basis to meet EU requirements related to shipping monitoring.

[10] Maritime Administration and Marine Safety Law (with amendments), *Latvijas Vēstnesis*, 19.11.2002, Article 2.

[11] Maritime Administration and Marine Safety Law (with amendments), *Latvijas Vēstnesis*, 19.11.2002, Article 4.

10 SafeSeaNet system

Directive 2002/59/EC (27.07.2002) stipulates that the Member States shall introduce and maintain an electronic shipping control and monitoring information exchange system (SSN), which is compliant with the directive standards[12], by 31.12.2008. This was also one of the tasks for the Latvian Coast Guard Service for 2007-2008.

As stated in the interoperability requirements, one of the conditions for the successful introduction of the system is the compatibility to EIS, certified by the EMSA. The Latvian SSN system has received such certification on 16.04.2008 and since 01.06.2008 is connected to the EMSA EIS server. With this, the first phase of introducing the national SafeSeaNet system was completed - the basic system according to EU regulations was introduced.

As planned, through the use of SafeSeaNet the EU maritime authorities will be able to improve overall control of shipping, monitoring vessels in ports and producing statistics for EMSA, Member States and the European Commission. However, at the same time, information contained in the EU SafeSeaNet system and mandated by the control and safety at sea legislation is similar or even identical to information requested by other systems and authorities. The Latvian SSN system will thus be developed to exchange information of interest with other maritime authorities such as SAR services, environmental protection agencies, Customs, Border Guards and Police, etc.

SafeSeaNet requires the system to receive and forward information to the Index server with the following notifications on:

- Port;
- Hazmat;
- Ship (MRS and AIS);
- Alert situations (Waste, POLREP, SITREP, Lost-Found containers, others);
- Security.

All these notifications have generic data (IMO, MMSI, Call Sign and Name) and additional information where required. For example, the Waste Notifications (a part of the Alert Notifications) shall contain information requested in one of the following Articles of Directive 2002/59/EC: Article 4; Article 13; Article 9; Article 16 and Article 4 of Regulation 725/2004.

[12] Amended proposal for a Directive of the European Parliament and the Concil on enhancing port security, Brisele: 28.05.2004, http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=CELEX:52004PC0393:LV:NOT

To analyse these requested capabilities the following is concluded:

Port (Pre-Arrival) Notification

In accordance with the SSN XML Messaging Reference Guide[13], the Ship Notification XML message is sent by the Member State to SafeSeaNet in order to notify SafeSeaNet that a given vessel is bound to a particular port with an estimated time of arrival and a number of persons onboard. The message shall contain the following information:

1) Header (Version; TestId; MsRefId; Creation time; From:; To:) – reference information to accompany the message;
2) Body:
    - Vessel Identification:
        - (IMO, MMSI, Call sign, Vessel name);
    - Voyage Information:
        - (Next port of Call, ETA, ETD, Total persons onboard)

The main purpose of the Port (or pre-arrival) Notification is to inform the port about the vessel's visit within an acceptable timeframe. Information shall be provided by the ship (agent, master or operator) 24 hours prior to entering the harbour (there are a few exceptions to this rule). To compare the information on the SSN Port Notification and the FAL forms (here - General Declaration), the following distinctions can be noted:

Table 1. Capabilities of the Latvian SSN system – Port Notification

	FAL General Declaration (FAL Form 1)	SSN Port Notification
Reporting regime	24 hours prior to entering the port (with some exemptions)	24 hours prior to entering the port (with some exemptions)
Information provider	Ship (agent, master, operator)	Ship (agent, master, operator)
Information content	Contains the data requested in the FAL Form 1 (General Declaration)	Contains the short notice of the ship's visit
Information distribution	Is distributed to the port authorities, as a hard copy mainly.	Is distributed electronically, via the SSN system.

[13] SafeSeaNet XML Messaging Reference Guide (V. 1.6.4.), Section 3.3.

Information availability	Information is available for the addresses within ports mainly.	Information is available for authorized SSN users within EU.
Storage and archiving of the information	Shall require an additional fee for the storage and archiving of information (e.g. „Port Net")	Information is stored automatically, by the system.

The Latvian national SSN system presently has limited capabilities for receiving all the information contained in the FAL Form 1. Some parts of the Form, which are not requested by the ISPS Code, are not activated. The reception of information requested by the SSN (Port Notification) is supported fully.

Ship Reporting Systems – Mandatory Reporting System (MRS), or automatic data transfer from the national Automatic Identification System (AIS)

The SSN XML Messaging Reference Guide (V. 1.6.4., Section 3.3.), explains that a Ship Notification XML message is sent by a Member State to SafeSeaNet with details on the vessel's voyage and cargo. Ship notification is initially captured via MRS or an AIS signal. The message contains the following information:

3) Header (Version; TestId; MsRefId; Creation time; From; To:) – reference information for relating to the message;
4) Body (selected from MRS Notification or AIS Notification);
    - MRS Notification:
        - Vessel Identification (IMO, MMSI, Call sign, Vessel name)
        - Voyage Information (Next Port of call, ETA, Total persons onboard);
        - Ship position (Lat., Long.)
        - Notification details (two possibilities: Contact details or Url);
            - Url Details (Hazmat information is stored as a document and presents a link to the document. Standardized document types are used: DOC, DOT, RTF, HTM, HTML, PDF, TXT, HML)
            - Contact Details (indicates a Contact containing a Hazmat information on shore):
                - Includes (Last name, First Name, LoCode (port of location of Contact), Phone, Fax, E-mail.)

- AIS Notification - information captured directly from the AIS signal consists of:
  - Vessel Identification (IMO, MMSI, Call sign, Vessel name)
  - Voyage Information (Next Port of call, ETA, SOG, COG, Navigational status);
  - Ship position (Lat., Long., Timestamp)

A choice of two possible responses is permitted: AIS or MRS Notification. MRS Notification provides information on the vessels' movement and Cargo, while AIS only provides information on the vessels' movement. The message creation procedure is also different. The AIS message is fully automated (data mainly taken directly from the AIS). The creation of the MRS messages includes some additional activities (i.e. establishment of the MRS reporting lines, creation of the automated (or manual) reporting tools).

The Latvian national SSN system contains a tool to automatically add the coastal AIS into SSN. This information is taken from the geographical position taking into consideration the lack of registered MRS lines within the waters of jurisdiction.

Hazmat Notifications

In accordance to SSN XML Messaging Reference Guide (V. 1.6.4., Section 3.3.), a Hazmat Notification XML message is sent by the Member State to SafeSeaNet to notify SafeSeaNet of dangerous goods on a given vessel and that more detailed information on the goods is available upon request. The message contains the following information:

5) Header (Version; TestId; MsRefId; Creation time; From:; To:) – information provided for the message management within system mainly;

6) Body (Vessel Identification: IMO, MMSI, Call sign, Vessel name);

7) Voyage Information (Next Port of call; ETA; ETD (port of loading Hazmat); Total persons onboard);

8) Hazmat Notification Details (two possibilities are requested: Contact details or URL);

   - URL Details (Hazmat information is stored as a document with a link to the document. Standard document types include DOC, DOT, RTF, HTM, HTML, PDF, TXT, HML)

   - Contact Details (indicates a Contact containing Hazmat information on shore):

        - Includes: Last name, First Name, LoCode (port of location of Contact), Phone, Fax, E-mail.)

9) Cargo Manifest Details (two possibilities are requested: Contact details or URL);

    - URL Details (Cargo Manifest is stored as a document on a server with a link to the document. Standard document types include DOC, DOT, RTF, HTM, HTML, PDF, TXT, HML)

    - Contact Details (Contact containing Hazmat information on shore):

        - Includes: Last name, First Name, LoCode (port of location of Contact), Phone, Fax, E-mail.)

There are two operating principles for Hazmat information exchange in the SSN:

- to report the Hazmat onboard a vessel when leaving the port of a Member State with a planned route to the port or through the waters of another Member State;

- to report the Hazmat onboard the vessel if requesting to port in a Member State when the port of departure is outside the boundaries of the EU.

The reporting procedure also varies for these two situations. In the first situation the authority (port, competent authority) reports the vessel leaving their port of responsibility. In the second situation, report details are based on information received by the institution from the vessel (agent, master, operator).

Differences and problems should be noted:

- In the first of these two situations, information is provided to all Member States prior to the vessel entering their waters (iaw SSN organization – at the time of departure or earlier).

- In the second situation, information is sent into SSN (i.e. all the Member States will be informed through SSN) at least 24 hours prior to the vessel entering the port of call,. A few days may pass after the Hazmat has crossed the boundaries of the EU (and waters of some Member States) without any notifications being sent to Member States.

For example: Vessel X underway from South America with Hazmat onboard. If vessel X has a port call in Ventspils (Latvia), the first information concerning the cargo (as well as Hazmat) will be entered into SSN at least 24 hours prior to the arrival. In practice the ship will be somewere close to

Denmark and the Hazmat has crossed the waters of jurisdiction (depending on the route) of France, Great Britain, Germany, the Netherlands, Denmark etc. without prior notification.

This problem can be solved by creating MRS (Mandatory Reporting System) reporting lines around the boundaries of the EU, or (and it could be more usable) changing the content of AIS reporting systems. An additional line can be added specifying onboard Hazmat. The financial and operational aspects should be calculated but this solution could affect not only EU needs but also the maritime community itself as well.

The Latvian national SSN system supports both reporting capabilities – to report and receive Hazmat onboard the vessels entering or departing ports in Latvia.

Waste Notifications

An"Incident report" and is created to notify SSN users of non-compliance with waste delivery requirements. In accordance with the SSN XML Messaging Reference Guide (V. 1.6.4., Section 3.3.), the Waste Notification XML message is sent by a Member State to SSN to notify SSN that that Member State holds information regarding this incident. The main information providers are port institutions. This message contains the following information:

- Header (Version; TestId; MsRefId; Notification time; From:; To:) – information related to the message management within the system mainly;
- Body (Incident Type and Vessel Identification);
    - Incident:
        - Type: WASTE;
    - Vessel Identification (if vessel identified):
        - IMO, MMSI, Call sign, Vessel name;
    - Contact Identification (if Vessel is not identified)
        - Includes: Maritime Authority, LoCode (port of location of Authority), Phone, Fax, E-mail;
- Incident details (reporting form or URL)
    - URL details
        - Indicates that an Incident Report is stored as a document on the server and presents a link to the document. Standard document types include DOC, DOT, RTF, HTM, HTML, PDF, TXT and HML.
    - Contact details

- Includes: Last name, First Name, LoCode (port of location of Contact), Phone, Fax, E-mail.

This type of report could be created as a "one-way" communication tool – where information from a vessel is provided to Member States – or as a „dedicated way" communication tool – where the vessel can select those to receive the information. The new SSN version supports both capabilities.

The national SSN system of Latvia provides a "two-means" reporting capability. The same "Waste Data" reporting form can be used to provide "Waste Declaration" (based on pre-arrival waste declaration form) on the vessel's arrival (provided by the agent, master or operator), and also provide a "Waste Notification" (based on the SSN Waste Notification form) in the case of non-compliance with a waste delivery requirement on the time of departure or later (shall be provided by the port authorities or relevant state authorities).

Reports are verified by the Latvian SSN NCA duty personnel upon reception, and depending on the type of information (Waste Notification or Waste Declaration), the report will be sent to the SSN or automatically stored in the national system's database for an internal use. Capabilities of the national SSN system to provide both report types by a single tool are shown in Table 2.

Table 2. Capabilities of the Latvian SSN system - Waste Notification

Information requested	SSN Waste Notification (iaw SSN requirements) Provided in case of incidents	Waste Declaration (iaw FAL requirements) Provided on ship arrival
Header		
Version	Created by the system	
MsRefId	Created by the system	
Sending time	Provided by the system	Provided by the system
From	Reporting authority	Reporting authority
To	Reporting authority	Reporting authority
Body		
Type	Waste Notification	Waste Declaration
Vessel Identification: IMO, MMSI, Call sign, Vessel name	Reporting authority	Reporting authority
Contact Ident.: Maritime Authority, LoCode (port of	Reporting authority, if vessel	

location), Phone, Fax, E-mail.	not identified	
Incident or Report Details:		
Details (report form)	Reporting authority if chosen	Reporting authority if chosen
Details: URL (attached file)	Reporting authority if chosen	Reporting authority if chosen
Contact: First Name, Family name, phone, fax, e-mail	Reporting authority if chosen	Reporting authority if chosen

Port State Control Notification

This is a distinction in the national SSN system of Latvia. SafeSeaNet publications do not request this type of information and these reporting fields are created under the form

"Additional information" consists of the following three requests:

- Date (dd, mm, yyyy) of last Port State Control inspection;
- Date (dd, mm, yyyy) of the last expanded PSC inspection within region Paris MoU;
- Place (LoCode) of the last expanded PSC inspection within region Paris MoU.

Note: Information shall be provided to the Port State Control and applies to the following types of vessels only: Passenger; Bulk carrier; Chemical tanker; Gas carrier; Oil tanker. Information shall be provided only upon request.

Incident Reports

The general principles of these reporting capabilities and structure are provided in the topic „Waste Notifications". In accordance with SSN XML Messaging Reference Guide (V. 1.6.4., Section 3.3.), the Waste Notification XML message is sent by a Member State to SafeSeaNet to notify SafeSeaNet that the Member State maritime authorities hold information on an incident. The following incident reports can be provided: SITREP, POLREP, WASTE, Lost/Found Containers, Others.

The national SSN system of Latvia fully supports all the capabilities requested by the SSN specifications. These capabilities can also be easily expanded to notify all necessary warnings in the national system, such as abandoned vessel, illegal passengers, contagious diseases, and other.

Security notifications

Security Notification XML messages are sent by a Member State to SafeSeaNet to notify SafeSeaNet that the Member State owns security information about a given vessel[14]. The following notice is added: "The Security message was initially in the list of SSN messages but after launching a discussion to reviewing the content of the security message and harmonize it with the decisions of the MARSEC Committee, some Member States expressed concerns about the inclusion of the security message into SSN. The COSS Committee discussed the issue but no final decision has been made for inclusion of the security message into SSN". The message could contain the following information:

- Header (Version; TestId; MsRefId; Distribution time; From:; To:) – reference information for the message;
- Body (Vessel Identification and Notification details: URL or Contact details)
    - Vessel Identification (IMO, MMSI, ship name, call sign)
    - Notification details:
        - URL details (indicates that a Security Report is stored as a document on the server and presents a link to the document. Standard document types include DOC, DOT, RTF, HTM, HTML, PDF, TXT, HML).
        - Contact details (First Name, Last Name, Phone, Fax, E-mail)

The national SSN system of Latvia is created as a "dual purpose" tool and provides the ability for users to exchange SSN and ISPS data using with the same tool. As the SSN Security Notification contains the same data as requested by the ISPS Code, notification is automatically created by the system. Additionally, the system contains mechanisms for automated data verification. For example: the system verifies the security level of the ship (iaw ISPS report/SSN Security report), the security level of the planned station or terminal (iaw security level prescribed by the state authorities) and the security levels of the last 3 ports of call (iaw ISPS report). In case of dissimilarity, a notice to the relevant institution will be created and sent by the system.

The main objective for the EU SafeSeaNet is to aid the collection, dissemination and harmonization of exchange of maritime related data. The EU SafeSeaNet network includes many

[14] SSN XML Messaging Reference Guide (V. 1.6.4., Section 3.3.),

authorities across Europe, each with their own IT infrastructure and objectives. Consequently SafeSeaNet has implemented the European Central Index System (EIS) that stores only references to the data locations and not the actual data. It functions as a central hub for all communication between the data requesters and data providers. SafeSeaNet covers EU Member States, Iceland and Norway and involves a number of different authorities per country.

In accordance with EU and related Latvian regulations, persons involved in the operation of the SafeSeaNet system in Latvia are the National Competent Institution (NCA), Local Competent institutions (LCA) and the authorized users.

According to Article 5 of the Regulation Nr.826 (03.10.2006) "Functioning of AIS Coastal Communication Network and Vessel Traffic Monitoring and Data Exchange System" of the Cabinet of Ministers of the Republic of Latvia, the NCA in Latvia is the Latvian Coast Guard Service Maritime Rescue Coordination Centre (MRCC Riga). MRCC Riga develops and, according to the SSN related regulations, maintains the infrastructure ensuring data transmission between national and EU SafeSeaNet systems and provides necessary access for the LCAs and authorized users[15]. Therefore, the NCA is responsible for evaluation of reported information, maintenance of the national database, and the further exchange of information within EU member states.

The (LCAs for the national SafeSeaNet system are:

- Port authorities (including harbour master services);
- Maritime Administration of Latvia (including subordinate institutions);
- State Environmental Protection Service (including subordinate institutions);
- State Border Guard institutions;
- State Revenue Service (including subordinate institutions);
- State Fire and Rescue service (including subordinate institutions);
- Security Police.

Authorized users (with limited access) of the national SafeSeaNet system are:

- Ship masters;
- Owners or operators;
- Agents – according to authorization (agreement between operator or owner of the ship and agent on agent services for the particular ship) requirements;

[15] Regulation Nr.826 (03.10.2006) "Functioning of AIS coastal communication network and Vessel traffic monitoring and data information exchange system" of the Cabinet of Ministers of Republic of Latvia, Article 28.

Actually, users are divided into groups depending on the authorization level. The NCA administrator prescribes authorization rights to each single user. The administrator can also define access rights to particular modules for individual users as well as for user groups.

The system provides the following additional capabilities for users:

- Options for statistical reviews;
- Information about the reporter (UserID, phone, fax, e-mail. Full information, including name and company, available only to the NCA);
- Supervision of system components and operations (servers' operations, status of communication lines, etc.) – for the NCA administrator only;
- Information exchange management tool (status of messages transmission/reception, status of requests, data exchange quality) – for the NCA 24/7 duty personnel.

The number of authorized users (agents) depends on the companies operating in the ports. The number of institutions acting as LCAs remains the same because legislation prescribes the institutions as users of SSN. User statistics are provided in Table 3.[16]

Table 3. Users of the Latvian SSN system.

Users	June 2008	June 2009
Agents	139	152
LCA's officials	63	91
LCAs (institutions)	10	10

In accordance with EU SafeSeaNet regulations, the competent institutions of Member States can request and receive restricted information from national SSN servers via the EIS. This solution is also included in a structure of the Latvian SSN system where LCAs can request information from the EIS. Authorized users can only use a database created by them. This means that the main information providers (vessels) have no permits to use – or have limited access to use – SSN.

This requirement, based on the existing legislation, does not support the proper use of the system's capacities, and changes have been requested at SSN working group meetings in EMSA.

[16] Latvian national SSN system statistics

11 Concept of the national SSN system

In order to comply with EU requirements, one of the tasks for maritime business in Latvia during the years 2007-2008 was the introduction of the national SafeSeaNet component. Additionally, Latvia had to appoint the National Competent Authority, adjust and create regulations on exchange of electronic information and maritime reporting solutions related to SSN. There were two main tasks during implementation of the national SafeSeaNet system: create an information exchange system – to improve maritime transport security and act on accidents, collisions or possible pollution – and minimize organizational inconsistencies. These inconsistencies include:

- Limit the number of users – the EU SSN system is accessible only by defined user groups (EIS,NCA, LCA, POR, PSC, etc.);
- Limit access - information providers (ships, operators, agents) do not have equal access;
- Lack of information in SSN - information requested by the EU does not meet all the needs of the national authorities.

For example: Port X can use data from the standardized SSN PORT Notification for an information purposes, but not for a practical need. This means that information sent to port authorities does not contain a necessary amount of data.

The following analysis is provided for one of the SSN basic elements – Port Notification.

Generally, the SSN Port Notification consists of:

1) General information about the ship (Static data - Ship name, Flag, IMO number, MMSI number).

However, there are no possibilities within SSN to provide additional important information for the users such as a vessel draft, width, length, operator, agent, actual ETA, pilot request, etc. For this, Vessel Traffic Services (VTS) must use alternative sources of information.

2) Voyage data (dynamic data):
    a. Next Port of Call – name of the next port of call (LoCode);
    b. ETA and ETD – estimated arrival and departure times

This is general information only. Often, it is more important to get specific information related to arrivals and departures (necessary for pilot services, pier and towing organization, tugboat operations, general movements in the port, port cost calculations) for port authorities.

3) Persons on board (total number of persons onboard).

Such information could be interesting to other SSN users (Coast Guard, Border Guard, Customs, etc.). However, even for these institutions such an amount of information is not sufficient.

This example demonstrates that the "synthetic" SSN information has no specific meaning: it is informative only and the amount is not sufficient for the institutions involved.

The above-mentioned discrepancies were taken into account in building the Latvian national SSN component to comply with EU SSN requirements and meet needs of national users.

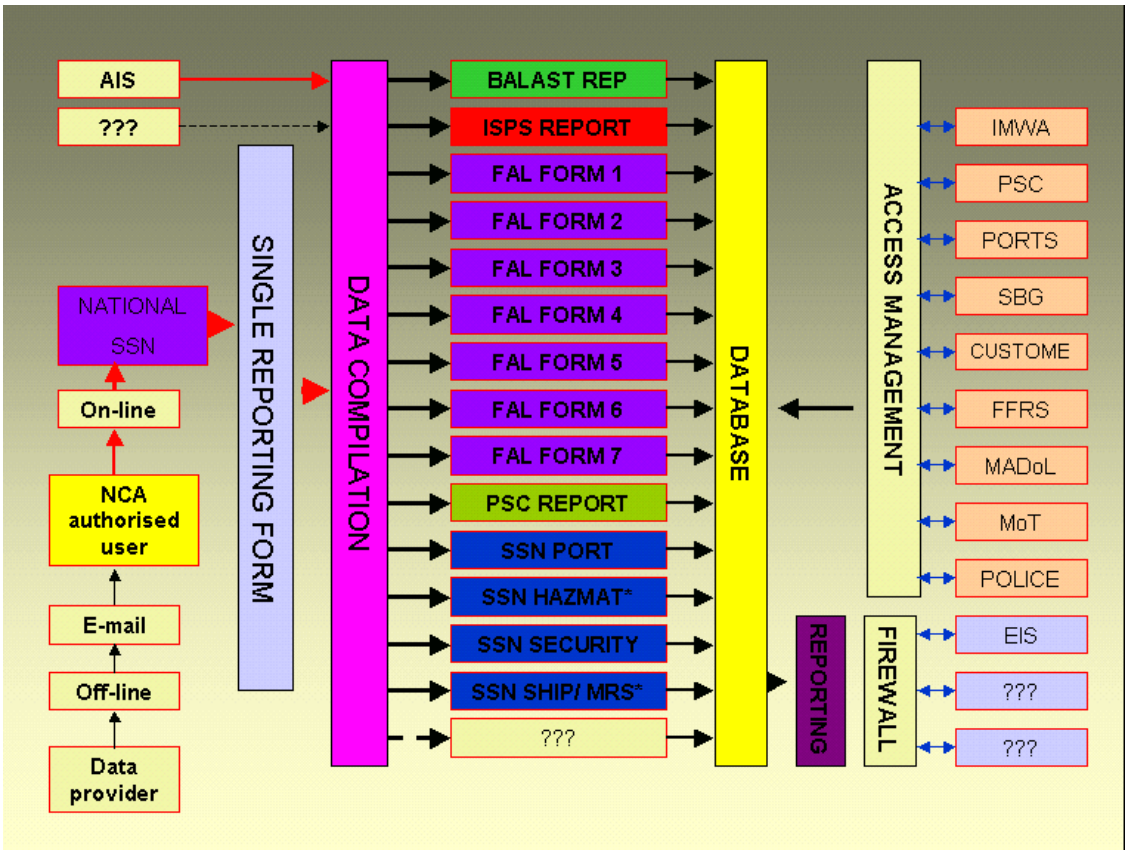

Figure 2. Structure of the national SSN system of Latvia.

The Latvian Coast Guard Service requested a combination of ISPS and SSN reporting tools in one reporting form, i.e. applying a "single window" principle. The system was created as a "dual purpose" tool with the following capabilities:

- Electronic information exchange;
- Common reporting form;
- Sorting, evaluation and preparation of the information;
- Execution of requirements of ISPS Code;
- Execution of requirements of SSN;

The system provides the ability to exchange the following SSN and ISPS data:

1. EU SSN requested information:
    - Port Notification
    - Ship Notification
    - Hazmat Message
    - Waste Notification
    - Port State Control Notification
    - SITREP, POLREP, Lost/Find Containers
    - Security Notification

2. ISPS Code requested information:
    - Ship security certificate data (number, validity, issuing authority);
    - Last 10 ports of call and their security levels;
    - Any security level changes or risks of changes since the last port of call;
    - Next (if known) port of call.
    -

3. Port visit information:
    - Pilot requests - information related to port service;
    - Reason for port calls – information for port, ISPS duty, Customs, Border Guard;
    - Planned station/pier/terminal (if known at the reporting time) – information scheduled for ISPS duty institutions, port, State Border Guard and Customs;
    - Cargo data (including hazardous cargo and materials).

4. Maritime environment protection and sanitary protection related information:
    - Ballast management information - for institutions to ensure environment protection;
    - Presence of contagious diseases onboard (if any) –for sanitary services;
    - Presence of animals onboard (if any) –for sanitary or veterinary services.

5. Management information:
    - Owner/ operator/ agent contacts (phone, fax, e-mail) – for MAS and SAR services;
    - Means of communications (phone, fax, e-mail, other) – for MAS and SAR services.

6. Immigration control information:
    - Crew list (can be added as an attachment, created „person-by person" into the report, or presented as POC information) –for ISPS responsible services, Border Guard, Customs;
    - Passenger list (if available - added as an attachment, created „person-by person" into the report, or presented as POC info.) –for ISPS duty, State Border Guard, Customs.

7. Port State Control related information:

- Last control date and location;
- Next mandatory control date;
- Next delayed control date (if any).

This information is for the Maritime Administration services and is provided upon request.

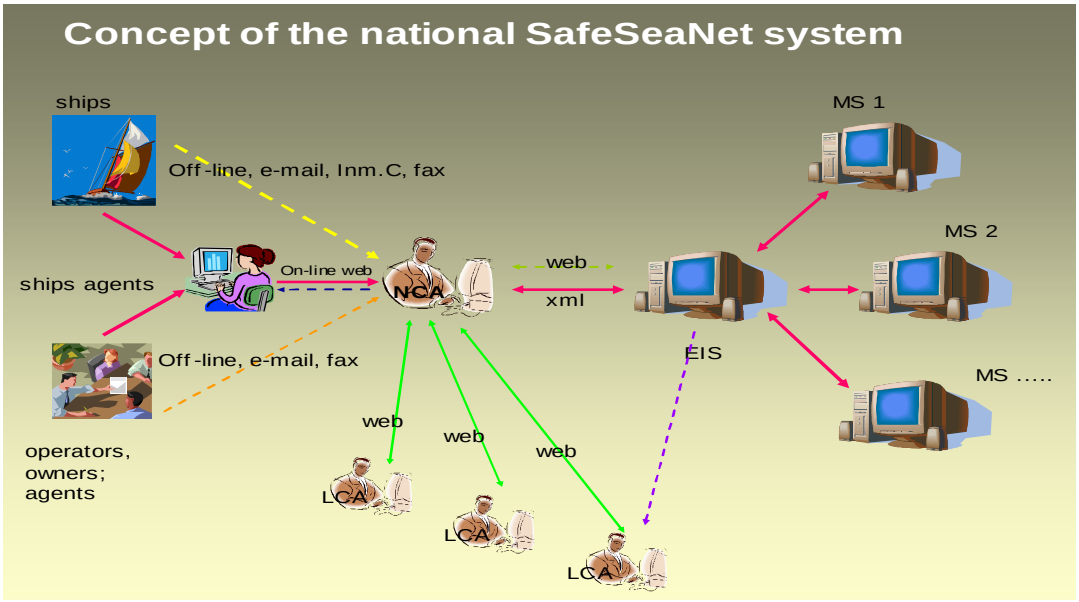

Figure 3. Concept of the national SSN system in Latvia.

Information in each of the existing FAL[17] reporting forms is partially duplicated. The national SSN system sought to decrease repetitive information, but maintain the "dual purpose" of the system (SSN plus ISPS). IMO Recommended Practice also was taken into account. The following tables (Tables 1-9) compare the 4 main reports:

General Declaration:

Note: IMO FAL Recommended Practice, Article 2.2.2, states that in the General Declaration public authorities should not require more than the following information (column „IMO FAL recommended"):

[17] IMO Convention on Facilitation of International Maritime Traffic

Table 4. Comparison of FAL "General Declaration" and Latvian SSN "Vessel & Voyage"

No.	IMO FAL recommended	National SSN of Latvia, "Vessel & Voyage"
1	Name and description of the ship	Name/ Type/ IMO No./ MMSI No./Int.Call
2	Nationality of ship	Flag
3	Particulars regarding registry	Classification society/ Registered owner
4	Particulars regarding tonnage	GT
5	Name of master	Name of master
6	Name and address of ship agent	Name, address, tel, e-mail of ship agent/ operator
		Name, address, phone and e-mail of ship owner
7	Brief description of cargo	*Not requested*
8	Number of crew	Number of crew
9	Number of passengers	Number of passengers
10	Brief particulars of voyage	List of previous 10 ports (LoCodes), Port of call /Port of departure in Latvia (LoCode)/ Next destination after Latvia (LoCode).
11	Date, time of arrival or departure	ETA port in Latvia/ ETD last port in Latvia
12	Port of arrival or departure	*Requested in position 10*
13	Position of ship in the port	Berth or terminal number

Cargo Declaration:

Note: IMO FAL Recommended practice, Article 2.3.1, says: "In the Cargo Declaration, public authorities should not require more than the following information (see column „IMO FAL recommended" in Tables 5 and 6):

Table 5: Cargo declaration (on arrival)

No.	IMO FAL recommended	National SSN of Latvia
1	Name and nationality of the ship	*Already provided ("Vessel & Voyage", Table 4)*
2	Name of master	*Already provided ("Vessel & Voyage", Table 4)*
3	Port arrived from	*Already provided ("Vessel & Voyage", Table 4)*
4	Port where report is made	*Not requested*
5	Container identification; marks and numbers; number and kind of packages; quantity and description of the goods	Requested to provide a Cargo manifest as an attachment or to provide POC information on the reporting form "Vessel&Voyage"
6	Transport document numbers for cargo to be discharged at the port in question	Already requested in pos.5.
7	Ports at which cargo remaining on	Port of loading/unloading – as part of the form

	board will be discharged	„Cargo manifest" and „Hazmat Cargo"
8	Original ports of shipment in respect of goods shipped under multimodal transport documents or through bills of loading.	Already requested in pos.5.

Table 6. Cargo Declaration (on departure)

No.	IMO FAL recommended	National SSN of Latvia
1	Name and nationality of the ship	*Already provided ("Vessel & Voyage", Table 4)*
2	Name of master	*Already provided ("Vessel & Voyage", Table 4)*
3	Port of destination	*Already provided ("Vessel & Voyage", Table 4)*
4	In respect of goods loaded at the port in question: container identification; marks and numbers; number and kind of packages; quantity and description of the goods	Requested to provide a Cargo manifest as an attachment or to provide POC information on See reporting form "Vessel & Voyage"
5	Transport document numbers for cargo loaded at the port in question	Requested to provide a Cargo manifest as an attachment or to provide POC information to the reporting form "Vessel & Voyage"

Crew list

Note: According to [FAL-Crew (FALC)], public authorities shall not require more than the following information (see column „IMO FAL recommended" in Table 7):

Table 7. Crew list

No.	IMO FAL recommended	National SSN of Latvia
1	Name and nationality of the ship	*Already provided in Table 4, as Ship data*
2	Family name	Family name
3	Given names	Given names
4	Nationality	Nationality
5	Rank or rating	Rank
6	Date and place of birth	Date of birth
		Gender
7	Nature and number of identity document	Number of identity document
8	Port and date of arrival	*Already provided ("Vessel & Voyage", Table 4)*
9	Arriving from	*Already provided ("Vessel & Voyage", Table 4)*

Note: Information (Crew list) in the Latvian SSN system can be provided directly into the report („person-by-persons") or as an attachment to the "Vessel & Voyage".

Passenger list:

Note: Recommended EDI format for the passenger list - PAXLST (Passenger List Message), which states that in the passenger list, public authorities should not require more than the following information (see column „IMO FAL recommended" in Table 8):

Table 8. Passenger list

No.	IMO FAL recommended	National SSN of Latvia
1	Name and nationality of the ship	*Already provided ("Vessel & Voyage", Table 4)*
2	Family name	Family name
3	Given names	Given names
4	Nationality	Nationality
5	Date of birth	Date of birth
6	Place of birth	*Not requested*
7		Gender
8	Port of embarkation	*Not requested*
9	Port of disembarkation	*Not requested*
10	Port and date of the arrival of the ship	*Already provided ("Vessel & Voyage", Table 4)*
11	Arriving from	*Already provided ("Vessel & Voyage", Table 4)*

Note: Information (Passenger list) from the Latvian SSN system can be included in the report (principle „person-by-person") or as an attachment to the table "Vessel & Voyage".

Waste report

Note: Directive 2002/59/EC requests that the report shall include items shown in the column „2002/59/EC recommended" (see Table 9):

Table 9. Waste report

No.	2002/59/EC recommended	National SSN of Latvia
1	Destination port	*Already provided ("Vessel & Voyage", Table 4)*
2	Name, call sign IMO ship indentification nr (where appropriate)	*Already provided "Vessel & Voyage", Table 4)*
3	Flag State	*Already provided ("Vessel & Voyage", Table 4)*
4	Estimated time of arrival (ETA)	*Already provided ("Vessel & Voyage", Table 4)*

5	Estimated time of departure (ETD)	*Already provided ("Vessel & Voyage", Table 4)*
6	Previous port of call	*Aleady provided ("Vessel & Voyage", Table 4)*
7	Next port of call	*Already provided ("Vessel & Voyage", Table 4)*
8	Last port and date when ship-generated waste was delivered	Requested to provide a Waste declaration as an attachment to the "Vessel & Voyage" or present a POC containing the information.
9	If waste is delivered, details of waste	

Summary:

Duplication of information is mostly solved as shown in the Tables above. The system generates separate reports on the basis of provided information. Recipients of information are informed about:

1) Complete ship voyage data for longer time periods (including the last ten ports of call);

2) Presence of the ship security certificate (fields – „Security Certificate Number" and „Issuing Authority"), certificate validity (fields „Date of Issue" and „Date of Validity") and ship ISPS security level (fields „Current security level" and „List of 10 previous ports");

3) Ship plans (tasks) related to the visit (fields – „Next port of Call"), time of arrival (field "ETA"), planned station (field „Berth/terminal Nr."), planned operations (field „Reason for port Call") and time of departure (field "ETD");

4) Persons onboard (fields: „Crew" and „Passengers – if exist"), „Total Persons Onboard" (system calculates automatically) and the general information about the persons onboard (tables „Crew list" and „Passenger list");

5) Possibility or risks of diseases and other quarantines (fields „Contagious diseases" and „ Animals onboard" – Yes/No);

6) Illegal immigrants or refugees (fields „Stowaways onboard" – Yes/No);

7) Presence of cargo including hazardous cargo or materials (fields „Cargo manifest" and „Hazmat Cargo". This information can be input directly into the report form, attached as an attachment or presented as POC information);

8) Waste and water management information (field „Waste report". Information can be input directly into the report form, attached as an attachment or presented as POC information).

Some fields have “drop-down” menus to facilitate entering information. Reporting tables include notices with an explanation for each field (mandatory, optional, shall be filled on request only). The system automatically creates the necessary reports (i.e. those required by an existing legislation), and transmission of these reports to the people specified in the table.

Warnings and announcements in the national system shall be provided by the NCAs and LCAs:

- Coordination center - SITREP, POLREP, warnings about drifting objects affecting shipping safety, other warnings;

- Port authorities – WASTE Alerts, announcements about the dangerous cargo on the departing ships (HAZMAT), other warnings;

- Maritime administration - results of the port state inspections and other warnings;

LCAs and authorized users can request access rights to enter the system from the NCA. In practice, the “on-line” module user’s access request shall be provided according to instructions; therefore, reduction of the risk of inaccurate operation is ensured.

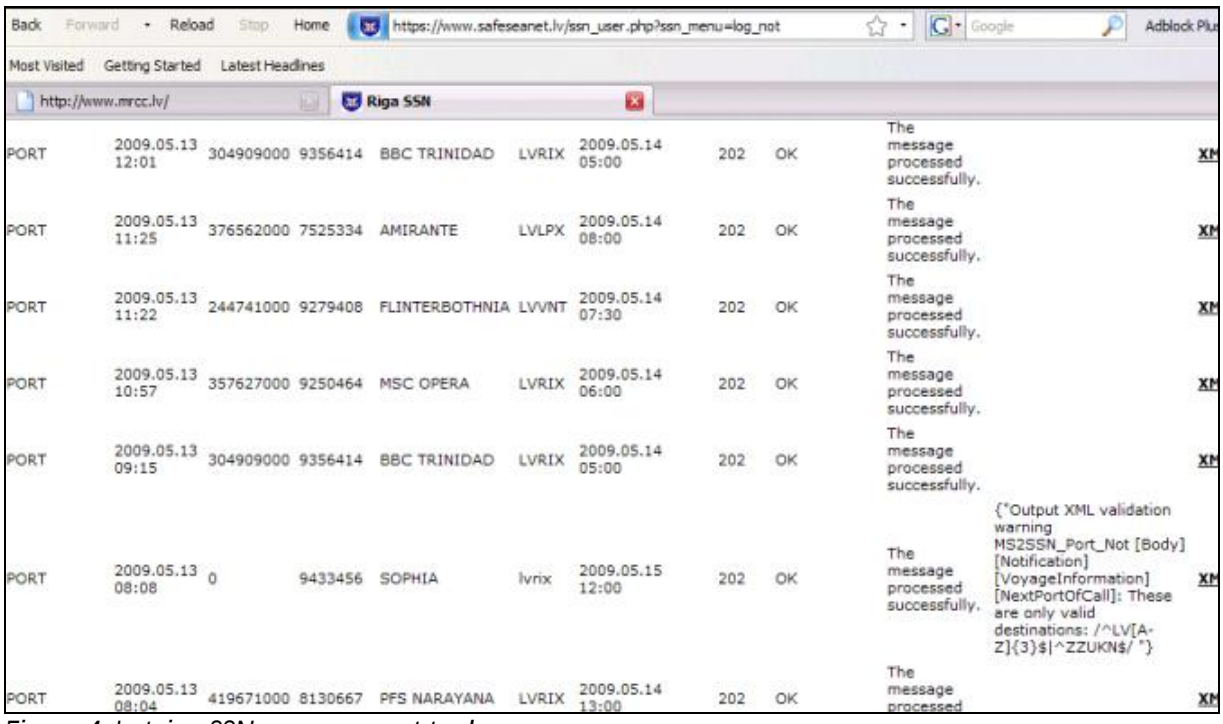

Figure 4. Latvian SSN management tool.

Conditions of the system foresee that in cases of repeated submission failure, the submitter (LCA or authorized user) shall inform the recipient (NCA) and submit information by using other means of communication (phone, fax, e-mail). These conditions allow the exchange of information in

all circumstances, even for persons who cannot use the "on-line" environment. All submitted information is immediately accessible by the responsible institutions. For example, port services, upon receiving information about hazardous cargo, can proceed to take all the necessary security measures.

When developing the national SSN system, special attention is given to information integrity and security. If a ship (or agent) has provided false or incorrect information then sanctions can be applied according to national legislation. Futhermore, the system software will not allow submission of incomplete or controversial information. The system acts as a filter for the data, and performs verification in fields including (but not limited to):

- The ship data (MMSI/ IMO/ Call sign/ Flag) correspondence;
- Correspondence of entered data and the ship register data;
- Correspondence of the ship security level and the terminal security level;
- Other.

The statistics provided by NCA Latvia indicates system usage has increased since the improvements made by the NCA, Table 10.

Table 10. Increase in different types of notifications with time.

	SHIP Notification	PORT Notification	HAZMAT Notification	SECURITY Notification
June, 2008	78297	84	-	80
September, 2008	97705	394	8	386
December, 2008	99602	644	7	640
January, 2009	105915	641	6	637
March, 2009	95612	691	28	689

Benefits noted

1. "Single point of contact" solution: data can be provided to one, single point of contact.

2. "Single Window" solution: usage of a single reporting form with added automated capabilities can decrease the work load for the shipping agencies and ship crews.

3. Effective user management: authorised access for national users ("On-line" module) and guaranteed access for non-authorised users ("Off-line" module) expands the system efficiency. 4. Data quality control: established data verification, usage of LoCodes instead of port names, and automated data validation function (for example: "now" ≤ ETA < ETD) increase the validity of information provided.

5. Alternatives on reporting (for some reports): variety of reporting capabilities such as direct-filling the report, attaching an earlier prepared form to the report, or presenting just a POC containing such information onshore, serve to decrease work loads.

12 ISPS data exchange

The second capability required by the international legislation is exchange of the information between coastal states and ships as per ISPS Code. As previously noted, the SSN Security Notification is under discussion and is not a basic element of the SSN. Article 9 (2.9) of the SOLAS Convention contains the requirement for ships to report (ISPS report) 24 hours before entering a port.

At the same time, a common reporting procedure is not provided. To comply with the requirement, a new reporting form has been proposed entitled „Ship pre-arrival security information form for all ships prior to entry into the port of an EU Member State (SOLAS Regulation XI-2/9 and Article 6.3 of Regulation (EC) No. 725/2004)"[18], expected as FAL Form 8 "Security Declaration".

Security must be ensured not on ships and in ports for international shipping, but also for ships used for local shipping, particularly passenger ships. ISPS Code part "B" regulates that Member States shall:

- Establish high security ports and alternate actions based on security evaluations to ensure the appropriate level of security;
- Control ships wishing to enter any port of the Community, regardless of route and flag.

National legislation of Latvia clearly defines institutions responsible for shipping security as well as compliance of their activities with national and international maritime legislation. The responsible institution for control of the ISPS Code requirements in Latvia is Ship and Port Security Inspection of

[18] Proposal for a Directive of the European Parliament and of the Council on reporting formalities for ships arriving in and/or departing from ports of the Member States of the Community and repealing Directive 2002/6/EC, Annex III, 26 January 2009

the Maritime Administration of Latvia. The main tasks and functions for this institution are delegated by the legislation and they are: to be the responsible institution for maintaining the ISPS Code, and implementation of the Regulation Nr.725/2004/EC "Ship and Port facility security" and Directive 2005/65/EC "Increasing security of ports". Furthermore, Ship and Port Security Inspection is responsible for the evaluation of the port and port facility security, approval of the security plans of ships under the Latvian flag, port and port facilities, performing security inspections on the ships and port facilities, handing out security certificates for the ports and port facilities, handing out the shipping safety certificates, certification of the classification societies, and approval of the training programs for security personnel[19].

Regulation Nr.682 "Division of functions of ship, port, port facility, and shipping company security"[20] from the Cabinet of Ministers, Republic of Latvia prescribes the division of the security functions among the Ministry of Defense, Ministry of Internal Affairs, and Ministry of Transportation according to international and national legislations. The Regulation is based on the requirements of Directive 2005/65/EC (26.10.2005) for increasing security of ships, ports and ports facilities and ensuring exchange of information among these aforementioned institutions.

Article 44 of the Maritime Administration and Marine Safety Law of the Republic of Latvia states the right of the Latvian Coast Guard Service to control shipping in compliance with national and international legislation in the waters of jurisdiction of the Republic of Latvia, and inspect and detain the ships according to requirements of the UN Convention on Law of the Sea, 1982. Regulation Nr.508 "Ship control, inspection and detain order" of the Cabinet of Ministers states the mechanisms for the Latvian Coast Guard Service to control, inspect and detain the ships, except foreign military ships and non-commercial service ships owned by the State[21]. Latvian Coast Guard Service MRCC Riga has been tasked to act as a National Competent Institution according to Article 6 of Regulation Nr.725/2004 (31.03.2004) "Increasing ship and port facility security". MRCC Riga also has the right to request ISPS related information from ships and shipping companies (shipping security certificate data)[22] according to Article 7 (1.b) of the Regulation Nr.725/2004, to ensure that a specific ship and port facility has a valid security plan, and control the communication of ship and

[19] Ship and Port security inspection main tasks and functions, http://www.jurasadministracija.lv/index.php?pid=03428

[20] Division of functions of ship, port, port facility, and shipping company security. Cabinet of Ministers regulation Nr. 682, *Latvijas Vēstnesis*, 22.08.2006

[21] Ship control, inspection and detain order: Cabinet of Ministers regulation Nr.508, *Latvijas Vēstnesis*, 01.06.2004, Article 1

[22] Annex 8 (E.B.).

port facility plans[23]. If MRCC Riga realizes that a ship does not meet the security criteria, control measures can be taken. The MRCC Riga, according to Article 11 of the Regulation Nr.725/2004, will inform the ship and the Inspection about the action taken. The Coordination center has rights, according to Regulation Nr.725/2004 (Annex 1 Article 9 (2.5.3)), to request the Latvian Naval Forces, State Border Guard or Ship and Port Security Inspection to board such a non-conforming ship in the territorial waters of the Republic of Latvia, as well as inform the ship and the State Security Police of the necessity of such an inspection[24].

In accordance with international legislation, each country must designate a competent institution responsible for coordination of shipping safety actions on a national level[25]. To ensure and perform functions to increase ship and port facilities security[26], MRCC Riga is authorized to request the following information from ships with the intent to enter a port:

- Validity of security certificate and the issuing authority;
- Ship security level (at the moment of the request);
- Security levels of last ten ports of call;
- Particular or additional security measures taken in last ten ports of call or cooperations with other ships;
- Safety procedures or security levels in cooperation with other ships or in last ten ports of call;
- Information relating to security but not part of the ship security plan.

MRCC Riga can request any ship or shipping company to verify information, analyze reported information, apply necessary security procedures[27], and control/complete procedures[28], such as:

- Request information at least 24 hours before entering a port, or
- Request information no later than departure of the ship from the last port of call if the voyage is less than 24 hours, or
- Request information when the next port of call is known if it was not known before or changed during the voyage.

---

[23] Annex 7 (E.B.).

[24] Ship security alarm network: Cabinet of Ministers Regulation nr.683, *Latvijas Vēstnesis*, 22.08.2006

[25] Article2 (3) of Regulation Nr.682 (22.08.2006)of Cabinet of Ministers

[26] SOLAS Convention, Chapter XI-2 (Special measures to enhance maritime security), Regulation 9 (Control and compliance measures), Regulation Nr.682 (22.08.2006) of Cabinet of Ministers, Annex 2(4)

[27] Regulation (EK) Nr. 725/2004 (31.03.2004), Article 6(1)

[28] Regulation Nr. 725/2004 (31.03.2004), Article 6 (2)

These regulations do not apply to warships, military transport ships, ships less than 500bt, ships not using mechanical propulsion, simple construction wooden ships, fishing vessels and non-commercial ships[29].

MRCC Riga is tasked to control all the operations at sea by using all the available means and resources and shall prepare and submit reports regarding security-related incidents.

[Note: a security-related incident is any suspicious action(s) that might affect the ship, other ships, port or port facility security, or occurrence of collisions of ships[30].]

To fulfil these tasks, the following activities shall be performed:

- Receipt of shipping safety information on a continuous basis[31];
- Controlling how the shipping companies comply with security regulations and request necessary shipping safety information from these companies[32];
- Requesting shipping safety information from ships (shipping companies), including ships (companies) with exceptional status if the decision is based on security issues in a particular situation[33];
- Verify the security information, i.e.:
    - does the particular ship or port facility use an approved security plan,
    - does the ship's security level match with the security level of the port facility[34];
- Request that security information is reported iaw forms provided on the MRCC webpage;
- Inform a ship, port or port facility to increase the security level if:
    - The ship or port facility does not have a security plan, or
    - Security plans of the ship and port facility do not match;
- Exchange shipping safety and security information with appropriate institutions[35].

In the case of a recognized nonconformity, MRCC Riga shall assess the need to perform a ship inspection and inform the ship and appropriate institutions of their decision. In addition, MRCC shall

[29] Regulation (EK) Nr. 725/2004, Article 3(7)

[30] Regulation (EK) Nr. 725/2004, Article 6(3)

[31] Regulation Nr.682 of the Cabinet of Ministers, Article 2 (5)

[32] Regulation 725/2004/EC, Article 7 (3).

[33] Regulation 725/2004/EC, Article 7 (5).

[34] Regulation Nr.682 of the Cabinet of Ministers, part 2, Article 8

[35] Regulation Nr.682 of the Cabinet of Ministers, part 2, Article 9

establish and maintain a stable communication with the ship in case suspicions arise that the provided information does not correspond with security regulations[36].

As the National Competent institution, the MRCC Riga shall ensure that the ship with the intent to enter the port reports, in accordance with the ISPS Code:

- Ship security certificate validity;
- Security level of ship at the time of operation;
- Security level of ship in last ten ports of call;
- Information on specific or additional security measures in last ten ports of call;
- Ship security procedures during any operations;
- Any other practical information not included in the security plan.

In the case of inconsistencies being observed, MRCC Riga shall[37]:

- Request the ship to correct the inconsistency in security information;
- Request the ship to proceed to a certain place in territorial or internal waters of the State;
- Apply restrictions on the ship to enter the port;
- Inform the ship, company (agent) and port about the decision made by the appropriate institution regarding a particular vessel:
- Prohibit the ship from entering the port;
- Banish the ship from the port;
- Recommend the inspection of the ship;

Remark: such decisions are made only in cases when the authorities have serious reason to believe that the ship is directly endangring the safety of persons, ships or any other property and there are no other means to mitigate such danger. Before executing such actions, it is mandatory to inform the ship's captain of the decision. Upon receiving this information, the captain may decline to enter the port. In these cases the restrictions are not applied.

As the National Point of Contact within the SSAS system, MRCC Riga must ensure security procedures, exchange of SSAS information, and receipt and relay of distress signals[38].

MRCC Riga provides consultation for any ship flying the Latvian flag as well as for ships in territorial waters of Latvia, and acts as a point of contact with the following consultative functions:

- how to change or delay the planned voyage;
- how to stay on course or proceed to a particular target;

---

[36] Regulation (EK) Nr. 725/2004, part 2, Annex 1, Article 9

[37] Regulation (EK) Nr. 725/2004, Annex 1, Article 9 (2)

[38] Regulation Nr.682 of the Cabinet of Ministers, Article 13

- availability of personnel or devices to mitigate the risk of an accident;
- coordination of voyage, including entering or leaving the port;
- how to request a patrol boat or aircraft for escort.

At the moment, a united system for ISPS information exchange and a united database do not exist in the EU. States are executing the exchange of such information according to national regulations. Article 7 of the Regulation Nr.682 of the Cabinet of Ministers states that the security information (ISPS report) is submitted via the reporting form presented on the MRCC Riga webpage. This solution is created for the users without direct access to the SSN "On-line" module, or who are experiencing any technical problems using the SSN system. In practice it is a simple Excel form which can be filled out and sent to an agent of or directly to the NCA by fax or e-mail. Integration of data into SSN will be performed by the recipient manually. Such a reporting tool is based on the situations dictated by real life – not all reporters have direct access capabilities or rights.

Through establishment of the national SSN system, the ISPS report can also be entered directly into the system: the ship, operator or owner submits the information independently by using the electronic form presented on the MRCC Riga webpage or authorizes the agent in port to provide such information.

Information may be submitted "on-line" or "off-line", as presented on the MRCC webpage.

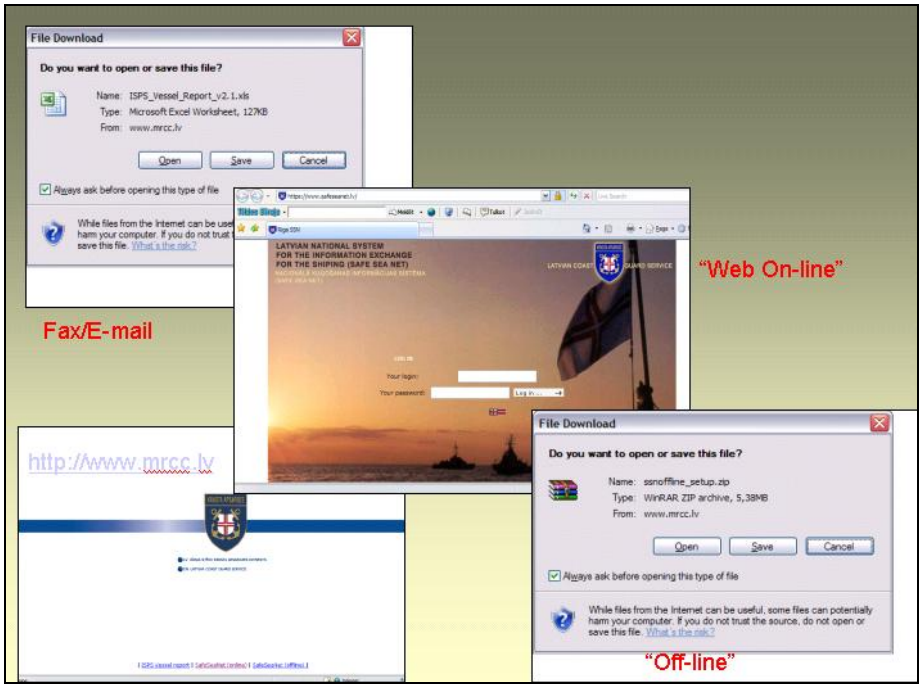

Figure 5. Reporting solutions.

As mentioned previously, one of the specific features of the Latvian SSN system is the capability to provide a detailed ISPS report and SSN required information electronically using the same table. Such a reporting solution was created in 2007 and also fully supports the requirements of IMO's new

proposed Security Declaration form[39]. A comparison of different forms is shown in Table 11. Empty fields imply that information is not requested/provided.

Table 11. Information requested in different reporting systems.

	SSN Security Notification form	FAL 1 (General Declaration) form	Proposed (Security Declaration) form	Latvian SSN system ISPS Reporting form
Information requested				
Identification data	IMO Number	IMO number	IMO number	IMO number
	MMSI Number			MMSI number
	Ship name	Ship name	Name of ship	Name of ship
	Call sign	Call sign	Call sign	Call sign
		Certificate of registry (port, date, number)	Port of registry	
		Flag state of ship	Flag State	Flag
			Type of ship	Type of ship
Comms. Data			Inmarsat call numbers (if available)	Inmarsat number (if exists)
				Ship phone/fax (if exists)
				Ship e-mail (if exists)
Technical data		Gross tonnage	Gross tonnage	Gross tonnage
		Net tonnage		
Management data		Owner/ operator	Name of Company and company identification number	Owner (Name, phone, fax, e-mail)
		Last port of call		Previous port of call
Voyage related data	*Information is provided in PORT Notification*	Port of arrival	Port of arrival	Port of call in Latvia
		Position of ship in the port (berth/ station)	Port facility of arrival (if known)	Berth/ Facility No.
		Port of departure		Port of departure in Latvia
		Subsequent port of call		Next port of call (if known) after port in Latvia

[39] Proposal for a Directive of the European Parliament and of the Council on reporting formalities for ships arriving in and/or departing from ports of the Member States of the Community and repealing Directive 2002/6/EC, Annex III, January 26, 2009

	Information is provided in PORT Notification	ETA	Expected date and time of arrival of the ship in port (ETA)	ETA
	Information is provided in PORT Notification	ETD		ETD
			Primary purpose of call	Reason for port call
ISPS Code and ship security related information			Does the ship have a valid International Ship Security Certificate (ISSC)? YES/ NO	International Ship Security Certificate number
			IISSC	
			Issued by (name of Administration or RSO)	Issuing Authority
				Issuing date
			Expiry date (dd/mm/yyyy)	Validity date
			Does the ship have an approved SSP on board? YES/ NO	
			Security Level at which the ship is currently operating?	Current ship's security level
	Information is provided in Ship Notification		Location of ship at the time this report is made	*Shall be reported only on request*
		Brief particulars of the voyage: previous port of call and subsequent port of call	List the last ten calls at port facilities in chronological order (most recent call first):	List of the 10 last ports of call
			No.	No.
			Date from (dd/mm/yyyy)	Date (dd.mm.yyyy) of departure
			Date to (dd/mm/yyyy)	
			Port	UN LoCode
			Country	
			UNLOCODE (if available)	
			Port facility	
			Security Level	Security level

	Any special or additional security measures YES/NO		Did the ship take any special or additional security measures, beyond those in the approved SSP? YES/ NO	Any special or additional security measures YES/NO/Comments
			If the answer is YES, indicate below the special or additional security measures taken by the ship.	
ISPS Code and ship security related information			List the ship-to-ship activities, in chronological order (most recent first), which were carried out during the last ten calls at port facilities listed above. Expand table below or continue on separate page if necessary – insert total number of ship-to-ship activities:	Any ship-to-ship activities/interference since the last port of call:
			Were the ship security procedures specified in the approved SSP maintained during each of these ship-to-ship activities? YES/ NO	
			If NO, provide details of the security measures applied in lieu in the final column below.	
			Nr.	Nr.
	Date		Date from (dd/mm/yyyy)	Date
			Date to (dd/mm/yyyy)	
	Position		Location or Longitude and Latitude	Position
	Activities		Ship-to-ship activity	Activities
	Security measures taken		Security measures applied in lieu	Security measures taken
Cargo information	*Information is provided in HAZMAT*	Brief description of the cargo	General description of the cargo aboard the	Cargo:

	Notification	Cargo declaration attached: YES/NO	ship	Cargo declaration: Attachment/ Contact
HAZMAT information			Is the ship carrying any dangerous substances as cargo covered by any of Classes 1, 2.1, 2.3, 3, 4.1, 5.1, 6.1, 6.2, 7 or 8 of the IMDG Code? YES/ NO	Dangerous cargo: Yes/ No Hazmat: If YES: Attachment/ Contact
			If YES, confirm Dangerous Goods Manifest (or relevant extract) is attached	
		Ship's stores declaration attached? YES/NO		
		Crew Effects Declaration attached? YES/NO		
		Maritime Declaration on Wealts attached? YES/NO		Contagious diseases YES/NO
Crew data		Number of crew (incl. master)	Confirm a copy of ship's crew list is attached YES/NO	Crew: (number)
		Crew list attached? YES/NO		Crew list: Attachment/ Filled form
Passenger data		Number of passengers	Confirm a copy of the ship's passenger list is attached YES/NO	Passengers: (number)
		Passenger list attached? YES/NO		If YES: Attachment/ Filled form
	Total persons onboard			Total persons onboard (calculated by system)
		Requirements in terms of waste reception facilities		Waste report (attachment / POC)
		Remarks	Is there any security-related matter you wish to report? YES/NO	Any additional comments
			If YES - Provide details:	
Information	*Information is*		Name:	Agent:

provider identity	*provided in PORT Notification*		Contact details (Tel. no.):	Company, name, family name Contact details: Phone, fax, e-mail
Report verification		Name of master	Title or Position (delete as appropriate): Master / SSO / CSO / Ship's agent (as above)	Ship master name
			Name:	
		Signature:	Signature:	
		Date and time	Date/Time/Place of completion of report	Date and time of reporting (created by the system)

Summary:

The following aspects are noted: the ISPS reporting form of the Latvian SSN system contains all the data requested by the FAL General Declaration, the proposed Security Declaration and SSN Security Notification forms. Therefore, the ISPS reporting form can be used as a single tool to provide the full spectrum of the requested information.

13 "Off-line" module – way to access the SSN for non-authorized users

Article 26 of the Regulation Nr.826 of the Cabinet of Ministers states that the master of the ship, operator or owner, by using an access to the system granted by the NCA, must electronically submit ship arrival data according to SOLAS-74 XI-2 (Regulation 9 (2.1) and the EC Directive 2002/59/EC (2002). Personnel on the ship, operator or owner submits the information independently by using an electronic form presented on the MRCC Riga webpage or may authorize the agent in port to provide such information.

Persons submitting the information to the national SSN system are responsible for the accuracy of the information according to requirements of Regulation Nr.826 (Article 25 and 26). Information is submitted via the NCA-granted "on-line" access, or the "SSN off-line" module, which are both presented on the MRCC webpage. Therefore, the Latvian national SSN system has both "on-line" and "off-line" access modules.

1) „On-line" access rights means that the user:

- is registered in the NCA database;
- has provided his/her personal data to the NCA;

- is trained in the use of the system and htaken responsibility for violation of requirements;
- has a password and ID number;
- has an individual account created by the NCA administrator;

2) Off-line access is granted to any potential submitter of information by downloading and installing specific software from the Latvian Coast Guard webpage[40]. In practice, the "off-line" solution can be used by a ship, owner or operator abroad to prepare and then send the report to an authorized user in Latvia for further integration in the "on-line" module. The downloaded "SSN Off-line" software allows the user to prepare reports and convert these into specific XML ZIP format files, which can be attached to an e-mail and sent to an agent or directly to the NCA. These files will be automatically uploaded into the system after validation has been completed by the NCA 24/7 duty service.

The main differences for the two types of access are:

The "On-line" module provides direct access to a user's personal account on the SSN national server, and sllows the preparation of reports directly in a personal account on the server. The "off-line" module is created as "stand alone" software, which can be downloaded from the Latvian Coast Guard webpage and used to create and submit reports without direct connection to the system; the "off-line" user shall link to an "on-line" module via an authorized user (agent, NCA, LCA). This solution ensures the NCA maintain system and data security.

Users of this module are usally ships outside the territorial waters of Latvia, and operators, managers or agents, who prepare reports for the Latvian SSN system independently.

Therefore, various problems can be solved:

- Reduction of paper workload for local agents;
- Ensuring more precise submission of the information;
- Guaranteed option for users without direct access rights to submit information to the Latvian SSN system.

Lessons learned

What are the advantages of such a system?

The national SSN system is built to meet the EU requirements and provide necessary information for all national maritime institutions. The Latvian Coast Guard Service has gathered recommendations for additional functions from authorized Latvian SSN users. For example, a recommendation from the Maritime Administration of Latvia was to create the option to find out

[40] http://www/mrcc.lv

whether the ship has ballast water that would lead to contamination if illegally discharged into the Baltic Sea. Responsible institutions also have an interest in monitoring single hull tanker movement in the Baltic Sea. These improvements, with data stored n the SSN database, will lead to less paperwork and improved shipping control.

The "single window" concept is not new in the world. For comparison, a little insight from the Swedish experience of implementing such a concept is provided[41]. A Single Window solution in Swedish Customs was established as a consequence of the computerization starting in 1988. Electronic communication showed great potential for a true Single Window environment; enabling Single Window, assessments to be made in response to volumes, benefits, users and costs. As Swedish Customs is responsible for monitoring all international and national legislation related to border crossing, they provide the logical interface between the business community and other public services. Information is gathered by Swedish Customs on behalf of more than 30 different authorities (import VAT, trade statistics, monitoring of licenses, pets, weapons, etc). These resource is available with different technologies: EDIFACT, Internet and Mobile solutions. Participants include Swedish importers, exporters and brokers, National Board of Taxation, Statistics Sweden, National Board of Agriculture, National Board of Trade, and the European Union.

Statistics show that 94 % of all Customs declarations are annually submitted using a Single Window solution. Results and major benefits reported are: automatic clearance of Customs declarations, release times decreased to 90 seconds, with no requirements for supporting documents; one interface for all information related to international trade; reallocation of resources; improved collection; creation of a level playing field. This example demonstrates the clear advantages of the Single Window solution.

The development of the Latvian National SSN system will continue. Future plans will create a united data submission module for conversion of data also in FAL forms for other shipping databases in Latvia - for example, the Latvian ports' information system "Velkonis".

Problems observed

During the implementation of the national SSN system, the following problems were identified and overcome:

1) "Variety of legislations":

[41] Mats Wicktor. Single Window Development and Implementation. Experience of Sweden. www.unece.org/cefact/single_window/sweden/mats_wicktor.ppt

At the moment different requirements are enforced in the maritime business (for example: IMO FAL; ISPS Code; EC SSN). These requirements have common parts as well as differences which impact the overall information management. A brief example: IMO FAL 1 (General Declaration) requires the signature of the master or authorised person such as an agent; however, this is not requested by SSN. The decision "to use or not" should be made prior to the implementation of common projects, such as "e-Maritime" etc.

2) "Sometimes, the real-life situation does not relate to the theory":

- "Vessels (main information provider) have no permits or limited access to SSN"
- "Users are not aware how to use SSN and advice for ships is not provided by authorities".

For the EU, these problems in general could be solved by changes in the currently proposed Directive 2002/59/EC,. At the national level, problem solving could be done easily with flexibility in the national legislation. International requirements must be taken into account.

3) "Paperwork are still increasing". "From the ship point of view it is common that different authorities request information already provided by the ship".

This is a common complaint from ship's masters and agents. The solution lies in the integration of the reports requested by separate legislation authorities/systems etc.

4) "If each country makes its own versions, it would not provide an efficient system.

It is true especially because the EU currently has no common "reporting face". This problem could be solved by a common decision at an international level. The best approach would be to use internationally-accepted reporting forms, or forms not in contradiction with each other.

5) "Many ships have no internet connection or have limited usage rights to download an execution program (Off-line) or report "On-line""

This is the most serious problem observed and needs a common solution from all the Member States. There are two possible (and for the moment, theoretical) solutions to be evaluated and both require international support:

a) Technical solution – Member States shall ensure the capabilities of the internet access within their territorial waters.

This solution needs financial investments and could not be accepted immediately. Also, some major technical infringements must be taken into account, such as geographical location etc. The Latvian Coast Guard Service has calculated the possibilities of such a solution and the results were quite unsatisfactory – guaranteed access can be provided not more than 8-10 miles from the coast line (or within 1-1.5 hours voyage time to the main Latvian ports) if existing infrastructure is used.

b) Administrative solution – shorter reporting time (changes to Directive 2002/59/EC).

This solution is not asking for a great financial investment,, and the main concept is to change the reporting organization in the SSN and other systems. Reports (usually) must be provided 24 hours

prior to entering the port of call. This is creating communication problems, data validity etc. Changing such requirements of the following (as an example only): "…ships must submit all the reports required by the FAL Convention, ISPS Code and Directive 2002/59/EC at least 1 hour prior to departure from the last port of call…", the problems of communication can be easily solved - by implementing reporting facilities in the ports and connecting them to the common information exchange system such as SSN. In this case, authorities will receive information related to departure and arrival (for the next port of call) at the same time. The international community as well as the next port of call will be informed through the informative tool (in this case - SSN), that a particular ship is going to leave port X at time Y and proceed to the port Z with dangerous cargo XX and total persons YY onboard. This will save institutions time in preparing to monitor the vessel, and the paperwork will be decreased for the mariners as well.

The logical question could be raised – why make the SSN a platform for the national maritime data exchange? The following arguments support the case:

- SSN is a common technical platform for maritime data exchange within the EU;
- It is a stable and accessible solution;
- 24/7 management is guaranteed for the users;
- It is based on common standards;
- System availability for EU requirements is provided;
- Common EU legislation is used as a baseline.

The following aspects should be taken into account to achieve full use of the system capacities:

- To avoid increasing the paperwork workpile, SSN reports should be integrated into an information flow application supporting a full reporting management process;
- Internationally accepted reporting forms must be used;
- Guaranteed access for all users should be provided.

14 Conclusions

Maritime safety often requires the adequate solutions of the data exchange between the vessels and the maritime authorities for adequate information about the real life situation. Such authorities can be National Competent Authorities or Local Competent Authorities, such as port authorities. Currently, there are different electronic forms in the forms . The main challenge is to establish an efficient, cost-effective and harmonized format, and determine how to integrate the compulsory notification into general vessel traffic monitoring.

The national SSN system has only been operational for a short period of time. It is too ealy to comment on the advantages or disadvantages, but some general observations can be made:

1. The Latvian national SSN system fully complies with EU SSN regulations relating to system safety, data exchange order, volume and quality;

2. The Latvian national SSN system combines several mandatory reports in a united information volume. The basis for the system is the so called “single window” concept, utilizing the existing ISPS report form supplemented with EU SSN sections, which are not included in the ISPS form.

3. The main goal of the Latvian national SSN system is to minimize replication of the data - all the information is combined into a single form, and submission is controlled by an automatic report generator function.

4. The Latvian SSN system management is consistent with the international recommendations and international structure:

a) Information is available according to EU requirements and national needs;
b) Submitted and received information is standardised;
c) The use of the “single window” concept reduces the number of reports;
d) Implementation of the “off-line” module decreases the workload of national information submissions and increases the number of potential system users;
e) Latvia has satisfied the international requirements.

15 References

Literature

1. Maritime legislation. Edition by M. Lejnieks and L. Medina, JUMAVA, 1997.

2. Shipping regime in Riga Freeport, http://www.rigasbrivosta.lv/lat/drosiba.asp

3. Ozoliņa I. Criminal jurisdiction rights in international maritime rights,

http://www.ljta.lv/page.php?id=59 (accessed 07.06.2006.)

4. Zeltiņš A. No surprises from Europe. *Marine news* Nr.3/4(10/11), 2005.

5. United Nation Convention on the Law of the Sea 1982, A Comentary. Volume III., Boston, [b.v.], 1995.

6. National SAR Manual [PDF version], York-Town, USA, 1989, Chapter IV.

7. The Ship Security Alert System. Summary of the IMO ISPS Code/SOLAS XI-2/6, http://www.satamatics.com/ssas/ssas_ship_security_alert_system_regulations.htm

8. Amended proposal for a Directive of the European Parliament and the Council on enhancing port security, Brussels: 28.05.2004, http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=CELEX:52004PC0393:LV:NOT

Regulations

1. Convention on the protection of the marine environment of the Baltic Sea area, 1992, http://www.varam.gov.lv/vad/Latviski/Likumd/Likumi/helsinku_konv.htm

2. International Ship and Port Facility Security Code (ISPS Code);

http://www.jurasadministracija.lv/index.php?pid=03421

3. International Convention for the Safety of Life at Sea (SOLAS), 1974, http://www.likumi.lv/doc.php?id=24852

4. Convention on Territorial Sea and Contiguous Zone, 1958, http://www.sam.gov.lv/satmin/content/?cat=109

5. United Nations Convention on the Law of the Sea (UNCLOS), 1982, http://www.sam.gov.lv/satmin/content/?cat=109

6. 1988 UN Convention on Illegal actions to suppress safe navigation

7. Maritime Administration and Marine Safety Law -- with amendments, *Latvijas Vēstnesis*, 19.11.2002

8. National Security Law -- with amendments, *Latvijas Vēstnesis*, 20.12.2000, nr.473/476.

9. National Armed Forces Law -- with amendments, *Latvijas Vēstnesis*, 04.11.99, nr. 388/389;

10. Regulation on use of territorial waters of Latvia and the shipping regime: Regulation Nr.508 (12.07.2005) of Cabinet of Ministers of Republic of Latvia, *Latvijas Vēstnesis,* 111 (3269) 15.07.2005.

11. Order of reports of dangerous and hazardous cargo: Regulation Nr. 592 (09.08.2005) of the Cabinet of Ministers of Republic of Latvia, *Latvijas Vēstnesis,* nr. 126 (3284), 11.08.2005.

12. Regulation on Latvian ship radio and navigational equipment safety requirements: Regulation nr. 144 of the Cabinet of Ministers of Republic of Latvia, *Latvijas Vēstnesis,* 100 (2865), 04.07.2003.

13. Port State control order: Regulation nr.197 (14.03.2006.) of the Cabinet of Ministers of Republic of Latvia, *Latvijas Vēstnesis*, nr.168 (2743).

14. Regulation on ship, port and port facility security: Regulation Nr.128 (15.02.2005.) of the Cabinet of Ministers of Republic of Latvia, *Latvijas Vēstnesis,* nr. 38 (3196), 04.03.2005.

15. Order of coastal network AIS data use for shipping safety and traffic organization: Regulation nr. 826 (10.10.2006) of the Cabinet of Ministers of Republic of Latvia, *Latvijas Vēstnesis*, nr. 161 (3529),

16. Supervision of Classification societies: Regulation nr.373 (19.11.2002.) of the Cabinet of Ministers of Republic of Latvia, *Latvijas Vēstnesis*, 168 (2743),

17. Ship security alarm network: Regulation nr.683 of the Cabinet of Ministers of Republic of Latvia, *Latvijas Vēstnesis*, (22.08.2006)

18. Latvian Coast Guard MAS plan – 2006: Instruction, not published.

19. Instruction on evaluation of enterprises performing ship safety equipment maintenance and inspection: Latvian Maritime Administration instruction, http://www.lja.lv .