Faculty of Science and Technology

MASTER'S THESIS

Study program/ Specialization: **Computer Science**	**Spring semester, 2012** **Open access**
Writer: **Maria Akbulatova**	…… **(Writer's signature)**

Faculty supervisor:
Prof. Dr. Chunming Rong (UIS)
External supervisor:
Dr. Matthias Winkler (SAP Research Dresden)

Title of thesis:

The Container Risk Evaluation Concept

Credits (ECTS): 30

Key words: Secure supply chain, risk evaluation	**Pages: ……101……** **Stavanger, 13th of June, 2012**

ABSTRACT OF THE THESIS

The Container Risk Evaluation Concept

by

Maria Akbulatova

Faculty of Science and Technology

University of Stavanger, Norway, 2012

Research Advisors:

Prof. Dr. Chunming Rong, Dr. Matthias Winkler

The international supply chain brings a wide range of threats: including the smuggling of illegal goods and substances, and the tampering with sea containers in order to hide nuclear, chemical or other weapons in them. Moreover with the introduction of House Resolution 1 (or "100% scanning law") marine ports may face a problem of increased workload and unacceptable bottle-necks in their work flow as a result of scanning of every container.

To improve the security of supply chains, there is a need to assess potential risks. The purpose of this study was to develop a concept for risk evaluation of sea containers bound for the USA and EU. The risk assessment should be efficient, cost effective and not cause big delays in work of marine ports.

The investigation was conducted on how logistical data which is provided to customs authorities by all supply chain participants as well as different container inspection technologies (e.g. x-ray) can help to enhance the security of an international supply chain. The main research questions which were addressed in the project are:

- which exact information is needed for container risk evaluation;
- how this information can be evaluated;
- how to integrate the risk evaluation process into the supply chain.

As a result of the Master's project a semi-automatic evaluation approach as an alternative to the "100% scanning law" was suggested. A prototype supporting the evaluation of security relevant container and supply chain data was developed for the evaluation of the concept. The developed concept together with the prototype reduces the need for a container scan and introduces a possible green lane scenario, enhances security through additional security related information and supports customs/border personnel during the evaluation of container security risks.

Acknowledgments

First I would like to express my deep and sincere gratitude to my supervisor from SAP Research Center in Dresden, Dr. Matthias Winkler, who supported me throughout my thesis from the very beginning. I appreciate his guidance, supervision and the excellent atmosphere for research he provided. Without him this thesis would not have been completed or written.

I gratefully acknowledge my supervisors from the University of Stavanger, Prof. Dr. Cunming Rong and Dr. Tomasz Wiktor Wlodarczyk for their advice and guidance.

I also would like to thank Gareth Alwyn Rowlands who, as a good friend, was always willing to help and give his best suggestions.

Finally, I wish to thank all my colleagues at SAP Research Center in Dresden. They were always supporting and encouraging me with their best wishes.

Maria Akbulatova

University of Stavanger, Norway
June, 2012

Dedicated to my parents.

I dedicate this thesis to my parents who supported me each step through my life.

Contents

List of Tables

List of Figures

Chapter 1

Introduction

In today's World there is a great need to be socially and environmentally responsible, as well as anticipate and, where possible, mitigate security risks in advance. One of the challenges for governments and logistical companies is to solve the problem of balance between increasing the security in international trade, especially in containerized traffic, and reducing administrative burden and time delay in international supply chain. A supply chain is a framework of organizations, activities, information and technologies involved in the transportation of a product from manufacturer to customer. An international supply chain involves multiple enterprises and organizations (including customs authorities) which work together to deliver a product from one country to another. The international supply chain brings a wide range of threats: including the smuggling of illegal goods and substances, and the tampering with sea containers in order to hide nuclear, chemical or other weapons in them. From a risk assessment point of view the most hazardous threat is transportation of nuclear weapon, as the consequences from an explosion will have a devastating impact. Securing an international supply chain is very complicated process and includes many entities: infrastructure, facilities, carriers, people, cargo and information exchange. Several legislations were initiated with the goal of securing supply chains. Examples are the US National Strategy For Global Supply Chain Security **(1)** and the "100% scanning" law **(2)**.

My Mater Thesis work is a part of the ECSIT (Increase of container security by applying contactless inspections in port terminals, German - Erhöhung der Containersicherheit durch berührungslose Inspektion im Hafenterminal) project. The project goal is the development of infrastructure that allows the capture of relevant information needed for the security evaluation of containers and the improvement of supply chain management visibility and security. This infrastructure should support

container scanning and information exchange between participants of the secure supply chain and provide integration with the Port Community System, scanning infrastructure, customs authorities and customers. The project analyses security risk and requirements of end-users, legislation (European Union and American), possible inspection technologies and how they can be embedded into the terminal's environment. The long term goal of the project is to increase container security through development of innovative technologies, such as container scanning, and analysis of their integration potential with existing harbor operations and processes.

Everyday Customs Authorities process a huge amount of data in order to analyze whether cargo possess a certain risk or not. Only in 2001, U.S. Customs processed more than 214,000 vessels and 5.7 million sea containers **(3)**. The data provided to U.S. authorities can contain information about compliance history of the company-importer, its financial solvency, security measures taken to eliminate the possibility of smuggling, unauthorized access to cargo units and tampering with cargo. As a result of the "100% scanning" law, U.S. authorities will have to evaluate also x-ray images and scan for radio activity. The information comes to U.S. authorities from different companies, systems and in different forms. Based on this information U. S. authorities need to make the right decision about potential security risks posed by of containers quickly and at low cost.

The problem which I highlight in my Master Thesis is the fact that it is not clear which exact information needed by the customs authorities for their security evaluations, nor is it clear how the customs authorities will evaluate the risk of containers based on this information. As an example, it is unclear how container scan images evaluation can be integrated into border processing; the issue became important especially after the endorsement of the "100% scanning" law.

The goal of this Master's Thesis is the development of a concept for a security risk evaluation process needed when deciding if a container may cross the border or not. The development of the concept includes assumptions on security data needed by the customs authority and the understanding of which parts of the process can be automated and which part must be conducted manually.

Also as part of this Master Thesis, a prototype for the partial implementation of the concept was developed. The prototype helped evaluate the concept.

In my Master's Thesis research I use an approach which includes:

- Research on the current situation in secure supply chain management for understanding the project context, including: existing technical solutions for supply chain management; current legal regulations for importing cargo into the United States and Europe; current and finished projects for cargo security (i.e. projects which concern only the technical part of container security such as e-seals or CSDs infrastructure as well as integration projects aimed to improve supply chain visibility and security).
- Development of a concept for data integration and container security risk evaluation using results from background research, this includes assumptions on:
    - data which the customs authority will need to make decisions about cargo (e.g. C-TPAT/AEO certificate, x-ray of the container);
    - how the customs authorities process data and how they make decisions if data is sufficient for release of cargo into a country or not.
- Development of a prototype for the application as enhancement to an existing SAP solution
- Evaluation of the concept

In Chapter 2 "Background Information and Related Work" I outline the most important international security regulations which affect international cargo transportation. In the same chapter I also describe related projects and discuss how far my work builds upon the latest systems already in use. In Chapter 3 "The Concept" I present my concept for semi -automatic risk assessment. In Chapter 4 "Description of the Tool" I describe on high level the prototype for risk evaluation tool which was developed for evaluation of the concept. I conclude this paper with Chapter 5 "Evaluation" and Chapter 6 "Summary and Future Work" where I describe evaluation of the concept based on use-case, discuss the results and outlook the future work.

Chapter 2

Background Information and Related Work

In this chapter I give a brief overview of the ECSIT project in order to outline the motivation for creating Container Risk Evaluation Tool. Moreover, I present an overview of the international sea freight security regulations. The purpose of my research on sea freight legislation is to understand which security criteria can be used for container risk evaluation and which information is critical for displaying and analyzing in Container Risk Evaluation Tool developed within the project. I also present my research on current and finished projects aimed to improve the visibility and security of the supply chain which is necessary in order to analyze how far my work enhanced the current state of the art. I finish the chapter by discussing existing SAP solutions which can be used as a base for development of Container Risk Evaluation Tool.

2.1 The ECSIT Project

The ECSIT project was initiated as a response to the U.S. "100% scanning" law, or House Resolution 1 (H.R. 1), which was adopted by Congress in July 2007. The law is an implementation of the National Commission on Terrorist Attacks Upon the United States Recommendations, also known as the "9/11 Commission Recommendations", which were set up on November 27, 2002 (Public Law 107-306, November 27, 2002). In Section 1701 – "Container scanning and seals" of the Act of 110th Congress of the United States, January 4, 2007 it states: "A container that was loaded on a vessel in a foreign port shall not enter the United States (either directly or via a foreign port) unless the container was scanned by nonintrusive imaging equipment and radiation detection equipment at a foreign port before it was loaded on a vessel." **(4)**.

One of the technical challenges for the ECSIT project is the development of new inspection technology for x-ray and radioactivity integration into harbor procedure, and

evaluation how far that can enhance container security. Another challenge is the integration of imaging methods for cargo scanning into harbor processes and operations. The Container Terminal Bremerhaven in Germany, the fourth largest container port in Europe and the largest one in terms of number of containers sent to the US in Europe is chosen as a use-case for demonstration of integration of different components developed within the ECSIT project. The project team from the SAP Research is developing IT system which will support collaboration of different stakeholders in transport process and harbor procedures.
As part of the ECSIT project I have developed a semi-automatic approach for container risk assessment, which can be executed e.g. by customs and border control personnel.

2.2 Legislation

A single international container shipment is affected by various laws of different countries and is the responsibility of numerous governmental and nongovernmental entities. During transportation the container is subject to business, transportation, taxation, customs and security laws, regulations and international agreements. In the Master's Thesis the focus is given to security regulations of sea freight containers, perhaps the most "rapidly developing and largely unsettled area of the law" **(5)**. Further in this section I will outline the most important international security regulations for sea freight, such as the European Authorized Economic Operators (AEO) program, American C-TPAT certification, the International Ship and Port Facility Security (ISPS) Code among others.

2.2.1 Authorized Economic Operators (AEO) program

AEO is a partnership between companies and customs authorities described by Word Customs Organization's (WCO's) SAFE Framework of Standards. The SAFE Framework of Standards is a set of worldwide security standards for secure international trade which focus on three elements: the availability of reliable data, the promotion of open standards for new security technologies, as well as mutual recognition of security standards and trade partnership programs. The approach used in SAFE standards based

on Customs to Customs and Customs to Business cooperation; later is implemented through AEO program. The program was launched in January 2008. More than 1700 European companies were authorized by November 2009 **(6)**.

Almost all participants of a supply chain can apply for Authorized Economic Operator Status: including manufacturers, exporters, freight forwarders, warehouse keepers, customs agents, carriers, and importers. The AEO Membership List - a database of economic operators holding a valid AEO certificate - can be accessed freely in the official website of the European Commission **(7)**. The possession of AEO status provides several benefits to its owner:

- Fewer physical and document-based controls (applied from January 1, 2008)
- Priority treatment of consignments if selected for control (applied from January 1, 2008)
- Choice of the place for controls if it leads to the shorter delay or less costs for the AEO (applied from January 1, 2008)
- Easier admittance to customs simplifications (applied from January 1, 2008)
- Reduced data set for summary declarations (applied from July 1, 2009)
- Notification of the place for further physical control prior to the arrival/departure of the goods (applied from July 1, 2009)
- Improved relationship with customs authorities
- Recognized as a secure and safe business partner
- Mutual recognition of Authorized Economic Operators.

According to **(8)** the criteria for granting the status of Authorized Economic Operator include:

- an appropriate record of compliance with customs requirements,
- a satisfactory system of managing commercial and, transport records, - which allow appropriate customs controls,
- proven financial solvency,
- where applicable, appropriate security and safety standards.

Security and safety standards are listed in Commission Regulation (EC) No 1192/2008 of 17 November 2008 **(9)**. In general there are requirements for external boundaries

(walls, fences, etc.), access control for premises, security process for goods transportation and security screening on prospective and current employees.

The application for AEO should be submitted to the relevant customs office. There is no expiry date on authorization. AEO status can be subject to review in case of major changes to the relevant Community legislation or indication that the relevant conditions are no longer being met by the AEO.

At present AEO or similar programs have been introduced in:

- the United States, under the name of C-TRAT
- all 27 Member States of the European Union (From May 2008 to February 2009, relevant monitoring carried out in all 27 Member States confirmed the uniform implementation of the AEO in all of those Member States **(10)**)
- New Zealand, under the name of Secure Export Scheme (SES)
- Singapore, under the name of Secure Trade Partnership (STP).

2.2.2 C-TPAT Certification

C-TPAT is a voluntary government-business initiative for building cooperative relationships to protect U.S. borders against terrorism. It was a response from U.S. Customs and Border Protection (CBP), one of the Department of Homeland Security's components, to the events of September, 11. Currently there are more than 10.000 companies participating in C-TPAT **(11)**. Such companies as U.S. Importers, U.S. Customs Brokers, Third Party Logistics (3PL) Providers, Marine Port Authorities & Terminal Operators, etc. are eligible to participate in C-TPAT.

If a company is C-TPAT certified it can get the following benefits **(12)**:

- A reduced number of CBP inspections;
- Priority for processing for CBP inspections;
- Assignment of a C-TPAT Supply Chain Security Specialist (SCSS) who will work with the company to help the company satisfy C-TPAT criteria;
- Eligibility to attend C-TPAT supply chain security training seminars;
- Access to the C-TPAT Membership List.

Requirements for granting C-TPAT certification differ for each type of a company (U.S. Importers, U.S. Customs Brokers, Third Party Logistics (3PL) Providers and etc.). In general a company should have a business office located and staffed either in the United States or Canada and satisfy certain security criteria for:

- **Container Security** (for example, all loaded containers bound to the U. S. should have a high security seal which must meet or exceed the current PAS ISO 17712 standards for high security seals);
- **Container Inspection** (for example, a seven-point inspection process is recommended for all containers prior to loading with cargo: front wall, left side, right side, floor, etc. Moreover, only designated employees should distribute container seals for integrity purposes);
- **Physical Access Controls** (for example, a company should have an employee identification system, visitors must present photo identification for documentation purposes upon arrival, etc.)
- **Personnel Security** (for example, application information, such as employment history and references must be verified prior to employment)
- **Procedural Security** (for example, arriving cargo should be reconciled against information on the cargo manifest, the cargo should be accurately described, and the weights, labels, marks and piece count indicated and verified, drivers delivering or receiving cargo must be positively identified before cargo is received or released, etc.)
- **Security Training and Threat Awareness** (a threat awareness program should be established in the company);
- **Physical Security** (requirements for fencing, gates and gate houses, parking, building structure, locking devices and key controls, lighting and alarm systems and video surveillance cameras);
- **Information Technology Security** (requirements for password protection and accountability).

As of June 2011 five Mutual Recognition Arrangements have been signed by CBP:

- New Zealand Customs Service's Secure Export Scheme Program;

- Canada Border Services Agency's Partners in Protection Program;
- Jordan Customs Department's Golden List Program;
- Japan Customs and Tariff Bureau's Authorized Economic Operator Program;
- Korean Customs Service's Authorized Economic Operator Program.

CBP is also currently working with the following Customs Administration with the goal of reaching mutual recognition:

- Singapore Customs - Secure Trade Partnership Plus Program;
- European Union – Authorized Economic Operator Program.

2.2.3 Importer Security Filing (ISF) and Additional Carrier Requirements

The Importer Security Filing, also known as the "10+2" initiative, is a Customs and Border Protection (CBP) regulation that requires importers to provide ten data elements to CBP as well as two more data elements from the vessel operating carriers 24 hours prior to loading.

For "U.S.-bound" cargo eight data elements should be provided no later than 24 hours before the cargo is laden aboard a vessel destined for the United States. Those data elements are:

- Importer of Record Number (it can be an Internal Revenue Service (IRS) number, Employer Identification Number (EIN) or Social Security Number (SSN))
- Consignee Number (as with the Importer of Record Number it can be Internal Revenue Service (IRS) number, Employer Identification Number (EIN) or Social Security Number (SSN))
- Seller (Owner) name/address
- Buyer (Owner) name/address
- Ship to Party name/address
- Manufacturer (Supplier) name/address
- Country of Origin (country of manufacture, production, or growth of the article, based upon the import laws, rules and regulations of the United States)

- Commodity Harmonized Tariff Schedule of the United States (HTSUS) number, which is a number for determining tariff classifications for goods imported into the U.S.

Two additional data elements must be submitted as early as possible, but no later than 24 hours prior to the ship's arrival at a U.S. port. These data elements are:

- Container stuffing location;
- Consolidator (Stuffer) name/address.

Two additional carrier requirements are:

- Vessel Stow Plan – no later than 48 hours after departure;
- And Container Status message (CSM) Data – no later than 24 hours after creation.

All data should be submitted electronically via vessel Automated Broker Interface (ABI) – a part of the Automated Commercial System (ACS) which is a system used by the U.S. Customs Service to track, control and process all commercial goods imported into the United States **(13)**. Provided information will be used primarily to identify high-risk containerized cargo aboard vessels, for example vessel stow plan will help identify the specific physical location of dangerous goods or unmanifested containers prior to arrival into the United States.

2.2.4 The International Convention for the Safety of Life at Sea (SOLAS) and Its Amendments

The International Convention for the Safety of Life at Sea (SOLAS) is an international maritime safety treaty on minimum security arrangements for ships, ports and government agencies. The SOLAS Convention came into force in 1914 in response to the sinking of the Royal Mail Ship (RMS) Titanic in the North Atlantic Ocean on 15 April 1912 after colliding with an iceberg during its voyage from Southampton, UK to New York City. Nowadays the SOLAS Convention in its successive forms is considered to be the most important of all international treaties concerning the safety of merchant ships **(14)** and many countries have turned these international requirements into their national laws.

International Ship and Port Facility Security (ISPS) Code is an amendment to the Safety of Life at Sea (SOLAS) Convention. The ISPS code came into force in 2004 and applies to ships on international voyages (including passenger ships, cargo ships of 500 gross tonnage and upwards, and mobile offshore drilling units) and the port facilities serving such ships **(15)**. The main objectives of the ISPS Code are:

- Detection of security threats (terrorist attacks);
- Establishment of roles and responsibilities for maritime security for governments, local administrations, ship and port industries etc.;
- Creation of a methodology for security assessments.

Because of the many types and sizes of ships and ports the Code does not specify measures that each facility must take to ensure safety. Instead it defines requirements for security plans, officers, certain onboard equipment – for ships, and ports alike.

The Maritime Transportation Security Act of 2002 (or MTSA), which came into force on July 1, 2004, is the U.S. implementation of the International Ship and Port Facility Security (ISPS) Code. The act provides a security program for all nation's ports to better identify and prevent terrorism threats.

2.3 Related Work

Supply chains are becoming more and more sophisticated and global. As a result, sharing knowledge and information along the logistics processes is needed to achieve transparency, efficiency and security in the supply chain. The role of efficient cooperation between the participants of the supply chain is rapidly growing and that requires the information and communication systems used for managing transport and logistics operation to interact efficiently, whilst both sharing and protecting information. In other words information systems should be secure and interoperable so that relevant stakeholders can share the information according to their own business rules. To develop such systems and concepts many publically funded research activities as well as in-house development projects were started.

In this section existing projects aimed to improve the visibility and security of the supply chain will be described. Also included are projects which focus on the efficiency

of the supply chain in order to provide an overview of the current situation in supply chain management.

2.3.1 Secure Supply Chain Management - SECURESCM

SecureSCM is partly funded by the European Union's Seventh Framework Programme. The project tries to solve the security problems arising while sharing information between supply chain partners. These problems prevent the development of collaborative supply chain management, as the majority of data accompanying a trade transaction is sensitive and supply chain partners are afraid of revealing it due to a high risk of unauthorized access.

As a solution to the problem SecureSCM implemented secure computation protocols for collaborative Supply Chain management. In their approach the project team implemented and evaluated these protocols using a prototype for data protection in the Aerospace and Logistics industry. The application was tested and analyzed within the context of supply chain management in the Italian firm Avio Aerospace Propulsion.

Although the final goal of the project is the same as that of the ECSIT project (to make the supply chain more secure and efficient), SecureSCM deals with a different aspect of security - information security. SecureSCM improves the security of the supply chain by introducing cryptographic protocols to protect data flow in communication between supply chain participants, whereas the ECSIT project is aimed to enhance security of the physical transportation process.

2.3.2 Smart Container Chain Management – SMART-CM

SecureSCM The goal of the SMART-CM project is to make supply chains more secure and efficient by developing a neutral platform for secure data communication between supply chain partners, as well as proposing an information exchange standard (protocol) on container security status.

The project is co-funded through European Union's Seventh Framework of the European Commission and has many partners among terminal and transport operators, logistical services providers, customs authorities as well as researchers, consultants and

technology providers. Originally the solution was developed for sea freight containers, but as it is stated in **(16)**, all findings are "equally applicable to all other forms of surface transportation, including road, rail, or barge, and may in the future be applicable to air freight transportation".

The SMART- CM platform consists of three layers:

- **Information gateway:** the entry point for information collection from different sources, such as container security tags/e-seals, port Management Information Systems (MIS), and fleet management systems.
- **Visibility (infrastructure):** the tool for the visualization of the information for logistic operators, web-based software.
- **Value added services:** this layer provides additional functionality for partners of supply chain, based on data collected from the previous two layers (for example transportation re-scheduling) **(17)**.

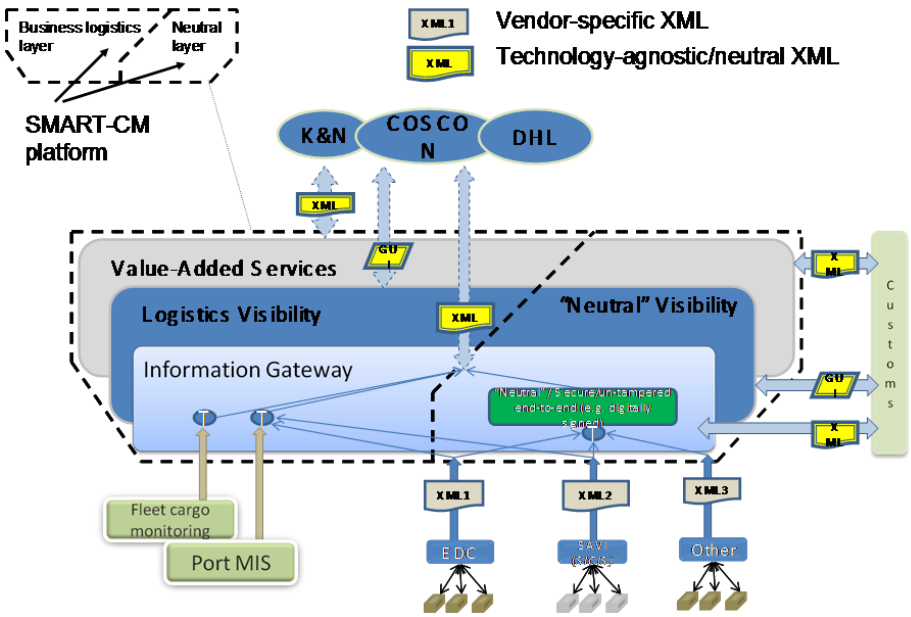

Figure 1 SMART-CM Platform (taken from (17))

One of the possible solutions for SMART-CM platform deployment described in **(16)** is the Global System Architecture currently in use by the Global Data Synchronization

Network (GDSN) for data synchronization between a supplier and a customer in the Consumer Goods / Retail Industry.

As a concept the following steps demonstrate how to synchronize data between the supplier and retailer platforms:

- the seller loads data (registers product) into its data pool;
- part of this data is sent to the Global Registry of an international not-for-profit association GS1;
- the buyer, through its data pool, subscribes to a seller's product; thanks to the GS1 Global Registry, the seller's data pool with the needed information is identified and the request is sent to that data pool;
- the seller's data pool publishes the requested information about the product to the buyer's data pool, from where it is then available to the buyer;
- The buyer sends a confirmation to the seller via their respective data pools

For the SMART-CM solution this concept can be used in very similar way. The Container Security Device (hereinafter - CSD) Provider can play the role of "Supply/Seller", and the SMART-CM platform can be the "Retailer/Buyer", through which the customs authority requests information about the cargo. The "Source Data Pool" in this case should be replaced also by SMART-CM platform where the CSD sends the required security data. The "Recipient Data Pool" can be again the SMART-CM platform or another platform, for example a database of Shared Intermodal Container Information System (SICIS) which is developed within the INTEGRITY project. The equivalent to "GS1 Global Registry" element does not yet exist in the Global Container Security System architecture **(18)**.

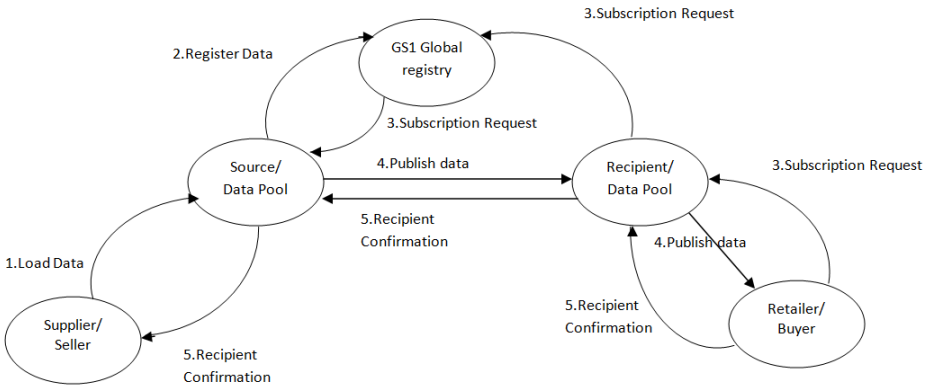

Figure 2 Model of a Possible Global System Architecture for the Global Container Security System (adopted from (16))

The SMART-CM platform was successfully tested in the Europe-Middle East (EU-ME) and Europe-Asia/Pacific (EU-AP) Corridors with help of project partners DHL, K+N, and COSCON as well as major port authorities from around the globe such as Antwerp, Rotterdam, Singapore, Ningbo, Dubai, and Nhava Sheva.

Although the approach used in this project is similar to the one used in ECSIT, the x-ray/3D/radioactivity scanning and container risk evaluation processes are not supported by the SMART-CM project. Moreover, the SMART-CM platform was intended for the Europe-Middle East and Europe-Asia/Pacific Corridors only.

2.3.3 Intermodal Global Door-to-Door Container Supply Chain Visibility – INTEGRITY

The INTEGRITY project tried to solve the problem of rapidly increasing volume of global container transport, bottlenecks in sea ports, conforming with new security regulations and inconsistent data about cargo through the development of the Shared Intermodal Container Information System (SICIS). The project is partly funded by the European Union's Seventh Framework and has partners such as the Institute of Shipping Economics and Logistics (ISL), DHL Global Forwarding N.V., and the RSM Erasmus University Rotterdam among others. The SICIS platform, as the main

deliverable of the project, will allow relevant stakeholders (authorized companies and authorities) to access status information of selected transport. This platform matches logistical data with security data which comes from electronic seals or other container security devices, and provides it to authorized participants of the supply chain. The long term goal of the project is the creation of a "Green lane", an equivalent of the "nothing to declare" green corridor at airports. The project aims to optimize "the cooperation between the transport industry and customs authorities in the China-EU trade corridor" **(19)**.

The SICIS system consolidates data from different sources such as the operating systems of participating container terminals and the CSDs attached to the container. With the second release of SICIS, container logistical data can be also obtained by tracking the vessel with help of Automatic Identification System (AIS), which serves to identify and locate vessels through the electronic exchange of data with other nearby ships and AIS base stations. SICIS provides all this information to authorized stakeholders based on a special system of access rights.

As the authors of the project state, the best level of monitoring can be achieved by utilizing CSDs, which can get the container position using GPS and transmit this information to SICIS **(20)**, or it can detect the container security status and raise an alert if for example the container was opened without authorization. However the system is not limited to containers with CSDs – it is still possible to track containers with the usual mechanical seals.

The SICIS platform has a SOA-architecture which allows implementation of interfaces to any kind of external data sources, such as terminal operating systems, AIS vessel tracking systems, CSD providers, port community systems, factories, and others.

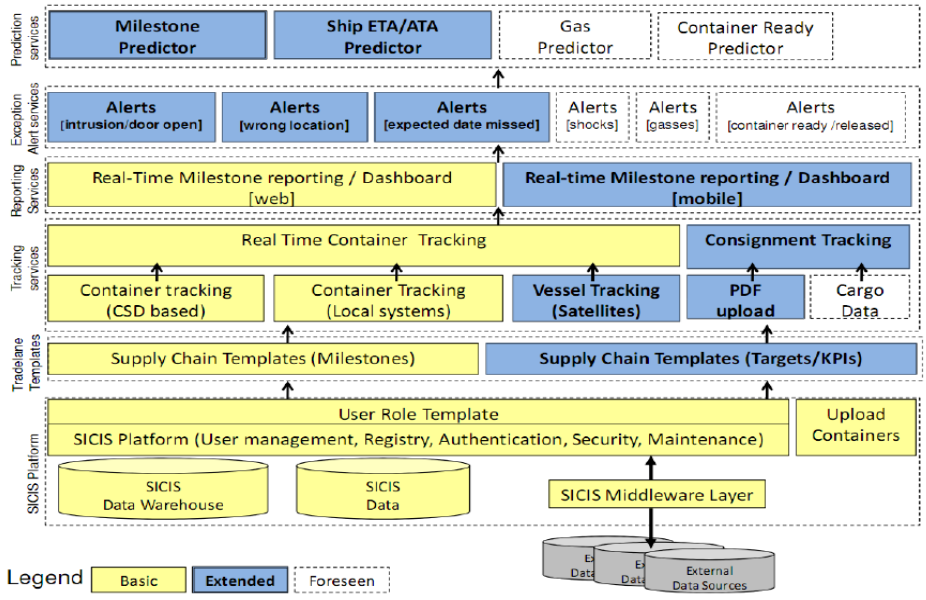

Figure 3 SICIS Architecture (taken from (20))

The SICIS platform cooperates with the SMART-CM platform and the interface between these two platforms is currently under development and will facilitate further data exchange between different sources.

The INTEGRITY project closely collaborates with other EU-funded partner projects, such as CHINOS, e-Freight, and ITAIDE (see below). Moreover, the SICIS platform is a part of the three-year CASSANDRA project, also funded by the EU via its Seventh Framework Programme.

However, the SICIS platform does not provide any tools for container risk evaluation process.

2.3.4 Information Technology for Adoption and Intelligent Design for e-Government Project – ITAIDE

The ITAIDE Project (Information Technology for Adoption and Intelligent Design for e-Government Project) is an EU-funded (Sixth Framework Programme) project aimed to improve security and reduce fraud in international trade and logistics.

The problem which the ITAIDE project highlights is the trade-off between increasing the security in international trade and reducing the administrative work for commercial and public administration organizations. The ITAIDE project's goal is to develop technological, procedural and organizational frameworks to simplify taxation processes using IT and improve the pan-European interoperability of taxation and customs systems. This goal in turn supports the long term objectives of the EU such as the introduction of Authorized Economic Operators (AEOs), the concept, according to which operators can be accredited by Customs as AEOs if they prove to fulfill all AEO requirements for safe and high quality internal processes; and Single Window Access service, that will allow all relevant parties to submit standardized information to custom authorities through a single entry point (6). The project has partners like the Copenhagen Business School, IBM Netherlands, SAP Research, the Danish Customs and Tax office, the University of Muenster, Lappeenranta City, the United Nations and the Economic Commission for Europe among others.

The approach of the project includes collaboration of research with business, the design and implementation of an information system based on SOA-architecture with integration of tamper resistant embedded controller (TREC) devices and Electronic Product Code Information Services (EPCIS), and the qualitative evaluation of the solution and its usability in Heineken. For further clarification the TREC is a container security wireless monitoring device that can transmit information about the container to which it is attached, such as the physical location of the container, its temperature, humidity, acceleration and door status **(21)**. EPICS is a standard which defines interfaces, discovery services, and security mechanisms for capturing and querying Electronic Product Code (EPC) related data **(22)**.

The solution allows data collection in distributed databases and implementation of simple queries such as tracing goods throughout the whole supply chain and finding the current location of the container using a given unique consignment reference number.

The proposed eCustoms model was demonstrated in the Beer Living Lab (BLL) which is a pilot project of the ITAIDE project for redesigning EU customs procedures **(23)**, and consisted of TREC IBM devices installed on pilot containers. The accompanying Shipment Monitoring Services (SMS) aimed to capture and forward events obtained

from TRECs, using three distributed EPCIS standard event repositories – one for each involved entity: Heineken, the Dutch Customs Authority (DTA) and Safmarine (a company which provides container and break-bulk shipping services worldwide), an ERP system in Heineken for declaration message generation and three Shipment Information Sharing Services (SIS) web portals to search, view and process shipment data **(24)**. All these components were bound together in an information system with Service Oriented Architecture and tested for interoperability.

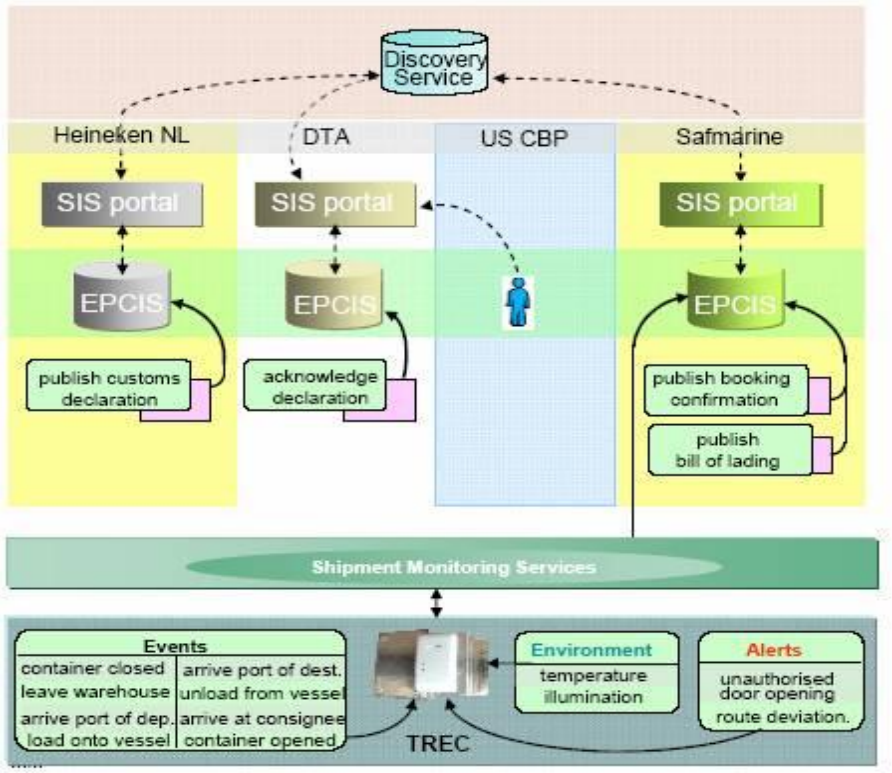

Figure 4 Architecture of the ITAIDE System (taken from (24))

The ITAIDE project is an inter-disciplinary project and represents a large amount of research conducted in standardization and interoperability areas.

The project, however, does not support x-ray/3D/radioactivity scanning and does not provide any tool for container risk evaluation by customs.

2.3.5 European Inter-Disciplinary Research on Intelligent Cargo for Efficient, Safe and Environment-Friendly Logistics – EURIDICE

EURIDICE is an integrated project funded by the EU's Seventh Framework Programme. The project aims to improve logistical performance and make it more secure and environmentally friendly through the development and implementation of the intelligent cargo concept. The concept includes building the information services platform which will allow the interaction of individual cargo items with the surrounding environment and relevant users. According to the concept, Intelligent Cargo should connect itself to "logistics service providers, industrial users and authorities to exchange transport-related information and perform specific services whenever required along the transport chain" **(25)**.

The information service platform which was delivered within the project allows users to uphold the network of connected cargo objects (making them identifiable and able to communicate), provide basic services, such as querying information about cargo, and interoperability for integration with other services. The smart cargo within this infrastructure can identify itself, detect the context (its location at every moment), monitor its status and detect changes in the goods conditions, for example, change of temperature. Finally, based on obtained information, the cargo can act independently, for example alert the owner that its current position is different from the planned location.

The EURIDICE system is highly distributed and consists of two physical areas: the "fixed platform", representing the "server" part, and "mobile device" which is simply all mobile devices connected to the system. The fixed platform communicates with the mobile devices through Software Agent architecture based on FIPA specifications, which is a collection of standards for promoting the interoperation of agents and the services that they can represent. External applications (developed and maintained by external stakeholders) interact with the platform also via Web Services, while object discovery systems along with event and cargo master data are provided by a part of the EURIDICE system which implements the ONS/EPCIS standard. As it was mentioned

above, the Electronic Product Code Information Services (EPCIS) is a standard that defines interfaces for the sharing of data among trading partners. The function of the Object Name Service (ONS) is to transform the EPC stored, for example, on RFID-Tags, via their corresponding Identity URI encodings into URLs, which may respectively point to a Web Service or other information resource **(26)**.

The distribution of the system is achieved by deployment of software components on mobile devices which are attached to vehicles, containers, terminals, etc. Some of the mobile devices can act only as sensors for detection of other mobile devices (for example devices installed in marine port terminals), while others can process their data before sending the results to the system (for example, CSDs installed on the container). All implemented services are deployed as Web Services and can be accessed by other services, applications and agents according to the security specifications. Communication within the agents happens through the FIPA ACL (FIPA Agent Communication Language) Message protocol, developed by Foundation for Intelligent Physical Agents.

As the EURIDICE system is highly distributed, event and object meta data is physically stored in several databases owned by the different organizations which participate in the supply chain and can be accessed via interfaces defined by Event Meta Information and Discovery Services.

For interoperability between different ERP systems of the supply chain participants the EURIDICE knowledge model is implemented in an ontology format. In additional to interoperability between ERP systems, the EURIDICE knowledge base set of ontologies and rules allows the intelligent cargo to do reasoning, context detection, and data mining tasks of trend detection.

Special adapter for legacy system should be installed on stakeholder site to make data available for the EURIDICE system. This adapter can consist of an EPCIS component for exposing stakeholder business domain data and an Identity provider component for stakeholder authentication in the EURIDICE system without duplicating the information.

The EURIDICE infrastructure was tested in eight pilot scenarios, each of them demonstrating the system benefits in specific business contexts including: cargo

transportation, cooperative warehousing through cargo-centric information services, self-returning empty pallets and boxes, and automated billing of goods in transit among others. Benefits include real time detection of exceptions which can be triggered by cargo as a result of deviation from the defined route, time, or physical condition of the goods with respect to the distributor's order, better planning based on information about deviations, minimization of human error, etc.

The EURIDICE project cooperates with the previously discussed SMART-CM and an interface between the two platforms can be developed. The SMART-CM platform can pull data from EURIDICE to collect information about intelligent cargo positions. At the same time the SMART-CM platform can also provide data from CSDs to the EURIDICE platform.

The EURIDICE platform brings innovation to shipment monitoring services with help of CSDs but does not provide neither collaboration between entities in the supply chain nor a tool for risk evaluation process of obtained data.

2.3.6 Common Assessment and Analysis of Risk in Global Supply Chains – CASSANDRA

The CASSANDRA is co-funded by European Commission within its Seventh Framework a follow up to the INTEGRITY, ITAIDE and SMART-CM project. The INTEGRITY project uses trade lanes from China to Europe to evaluate the functionality of the SICIS system - CASSANDRA adapts this approach and extends the scope to trade lanes from Europe to the US.

The CASSANDRA research problem has been formulated as follows: "How to integrate existing commercial supply chain visibility solutions and data capture technologies across supply chains to enhance risk assessment and to enable the adoption of a risk based approach to supply chain management for both private sector companies and government authorities?" **(27)**.

The goal of the project is to enhance the visibility of supply chain management and cooperation between all involved parties by developing a new data sharing concept, the so-called "data pipeline", which will connect existing information sources in the supply chain. Moreover in order to improve the efficiency of government agencies the

CASSANDRA project will design and implement a new approach for risk assessment based on information obtained from the whole supply chain. The combination of a new Risk Based Approach (RBA) and the data pipeline concept will be demonstrated and evaluated in the following three global trade lanes: China-Europe, Europe-USA and Europe-Africa.

2.3.7 Robust and Available SCM - Support IT Platform – RescueIT

RescureIT (Robust and available SCM - Support IT platform) is a European project which aims to develop a distributed, service-based IT infrastructure to make the supply chain more secure and transparent. The difference between this project and the ECSIT is that the RescueIT system is intended to monitor fresh food products, by measuring temperature, pressure, etc. The project scenario is the protection of fresh food products during the logistical process from production to the consumer. The core of the RescureIT platform is the risk database, within which existing standards and regulations can be mapped. The criteria for risk evaluation used in the RescureIT project are different from those used in ECSIT: they are based on the physical qualities of fresh food products.

2.3.8 Management Framework for Intelligent Intermodal Transport– FREIGHTWISE

The FRIGHTWISE project, co-funded by the European Commission through its Sixth Framework, aims to simplify the existing complexity of intermodal (multimodel) transport management. Developed based on previous European and national efforts, it is intended to simplify the procedure of supply chain planning and choosing available transport services for any type of cargo. The FRIGHTWISE Framework should achieve a high quality of collaboration and allow standardization across different transport modes **(28)**.

The FRIGHTWISE Framework is based on the reference model from the Norwegian project ARKTRANS and consists of four roles (Transport User, Transport Service Provider, Transport Regulator and Transport Network Manager); three business phases

(Planning, Execution, and Completion), Information Packages (messages exchanged by the roles: Transport Service Description, Transport Execution Plan, etc.) and processes for the transport chain. For example, the Transport Service Provider can describe its services by publishing "Transport Service Description" (TSD) that contains specific information on the single transport service. The TSD is a standard XML file that can be reached by the Transport User through a browser or suited application **(28)**. The framework allows the Transport Service Providers to advertise their services in an agreed format while Transport Users can search among transport services and negotiate details.

The previously discussed SMART-CM platform can use the XML format developed within the FREIGHTWISE project for transportation planning. In particular SMART-CM relies on Transport Execution Plan (TEP) and Transport Service Description (TSD) messages.

2.3.9 E-Freight

The co-funded via Seventh Framework Programme European project E-Freight can be considered as a continuation of the FREIGHTWISE project. The project objectives are to establish open freight transport e-market places to enable transport users to easily find and use direct or combined transport services suitable for their purpose. Moreover by developing "a single transport document in electronic form" (electronic waybill) the project aims to implement the concept of "single window", according to which all relevant parties can submit standardized information to custom authorities through a single entry point **(29)**.

The E-Freight concept includes following components:

- **e-Freight Framework –** a reference model for information exchange among participants of the supply chain;
- **e-Freight Platform –** a software infrastructure for e-Freight Framework implementation and e-Freight Solutions deployment;
- **e-Freight Services –** pieces of software used as elementary blocks for e-Freight Solutions;

- **e-Freight Solutions -** applications that perform meaningful functions in the area of Freight Transport & Logistics.

The e-Freight concept is depicted in figure below.

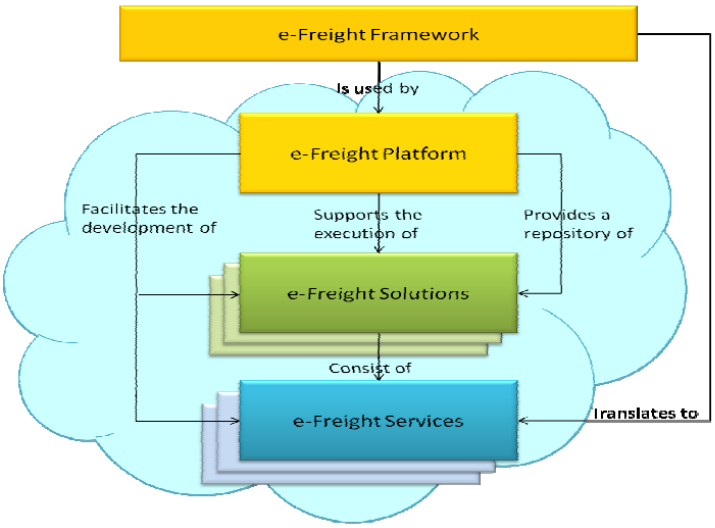

Figure 5 The e-Freight Concept (taken from (30))

The e-Freight Framework serves as a reference model to support paperless information exchange between all stakeholders in Freight Transport and Logistics. "The e-Freight Framework is in line with the Common Framework developed as a joint effort between the projects FREIGHTWISE, e-Freight, INTEGRITY, SMART-CM, EURIDICE, SMARTFREIGHT and DiSCwise and is a description of processes, actors, information and other domain entities" **(30)**. To ensure interoperability the e-Freight project works closely with standardization organization GS1.

The core e-Freight solutions are:

- **Next Generation National Single Window (NGNSW):** an application which represents a single entry point for the submission of all relevant transport documents in a standardized format.
- **Central EU National Single Windows' Support Services:** an application which holds the registry of all NGNSWs; it facilitates the information exchange through NGNSW and aims to provide statistical and data services.

- **Collaborative Security Risk Management:** an application that provides relevant stakeholders (logistics companies, suppliers, customs authorities, etc.) with real time tracking of trucks and vessels and security risk information sharing.
- **Monitoring of Transport Services Execution:** an application for transport services status monitoring and detection of deviations from the defined transport plan.
- **Co-modal Shipment Planning:** an application helping transport clients in specifying and negotiating the terms of transportation.
- **Single Transport Document:** an application for the generation of electronic transport Document (waybills) from existing operational data, based on a common standardized scheme.

According to the concept a National Single Window could be a single system at a National level. The system should collect information from relevant stakeholders and make this information available for authorized users within the country. For example this system can be a Maritime National Single Window, an EU initiative for a system which collects relevant information from businesses in the maritime domain and presents it to administrations, such as Port Authorities and National Maritime Authorities. Similarly, a Customs National Single Window is a system which allocates goods related information. Many countries already started to develop these kinds of National Windows. The current problem which the e-Freight project aims to solve is the lack of information exchange between these National systems. The project develops a "multimodal Single Window concept to facilitate exchange of electronic regulatory information, and which will satisfy the requirements of stakeholders in all transport modes." **(31)**.

Initially the prototype for National Single Window was a centralized system but after a demonstration to the user community the approach was shifted to the development of a distributed application due to the problem of system ownership and the devastating effect it would have if a central reporting facility is compromised with regard to security.

2.3.10 Container Handling in Intermodal Nodes – Optimal and Secure – CHINOS

CHINOS, a European project co-funded through its Sixth Framework, has as its objective to provide more reliable data on the state of containers from a logistical and security point of view.

The project tackles the following problems in the current situation:

- **Commercial:** the rapidly increasing volume of container traffic being handled in ports;
- **Legal/Security:** the growth in new security regulations for fighting against terrorism;
- **Technical:** the problem of integrating new technologies, such as RFID transponders, and combining them with existing classical bolt seals.

The system delivered within the project encompasses the latest technologies available on the market and provides information about the security status of the container such as identification, seal condition and damage documentation. The CHINOS system has four components:

- an automatic container identification unit (ACIU) consisting of a container identification system (CIS) and an electronic seal system (e-seal) which uses RFID;
- a damage documentation system (DDS) which uses high-resolution cameras;
- a chain event manager (CEM) which uses a supply chain event management approach;
- a communication controller (CC) which integrates different components.

Although most of the hardware components already exist, they are not integrated into a single system and some modifications and specially designed interface software was needed in order to build such a system.

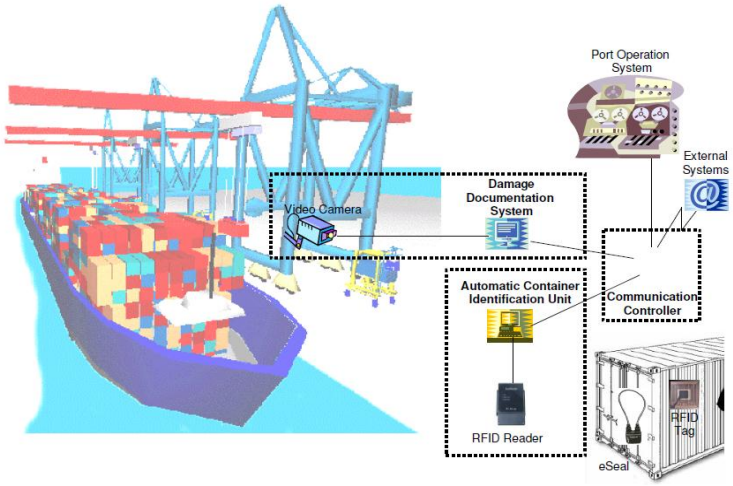

Figure 6 CHINOS System Architecture (taken from (32))

The system was installed and tested in different locations: in a large sea port in the North Sea (Bremerhaven), a medium-sized port in the Mediterranean (Thessaloniki), and terminals/freight villages in Poland (Pruszków) and Austria (Graz).

2.4 SAP Solutions

In this section I present my research on existing SAP solutions for supply chain management. The purpose of the research is to understand functionality available and use this information for development of the prototype for a Container Risk Evaluation Tool that builds upon the current state of the art.

2.4.1 SAP Global Trade Services

SAP Global Trade Services (SAP GTS) is a part of the SAP BusinessObjects Governance, Risk and Compliance (SAP BusinessObjects GRC) solution, which also includes components such as Access Control, Process Control, Risk Management and Note Fiscal Electronica. SAP GTS is based on an application server from SAP AG - SAP Web Application Server 6.20/6.40 - and can be connected to both SAP and non-SAP feeder systems **(33)**. The main purpose of SAP GTS is to automate global trade processes, help users work with huge numbers of documents and comply with legal

regulations, such as International Traffic in Arms Regulations (ITAR), AEO program, REACH Regulation, etc.

SAP GTS can be deployed as a stand-alone application for consolidated foreign trade activities or as a co-deployment on the hub of several SAP GRC solutions, for example Nota Fiscal Electronica (NFE) or Process Control/Risk Management (PC/RM). For small businesses SAP GTS can be installed as a co-deployment on ERP for global trade processes in a simple landscape.

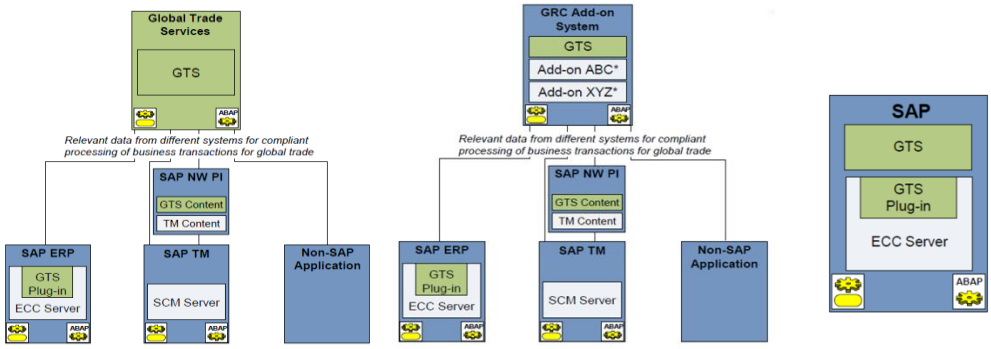

Figure 7 SAP GTS Deployment Options. Picture is taken from (34).
From left to right: SAP GTS Stand-Alone Hub, SAP GTS Co-Deployment and SAP GTS Co-Deployment for small businesses. Here, SAP TM stands for SAP Transport Management, SAP ECC – SAP Enterprise Central Component (SAP ERP), SCM – SAP Supply Chain Management solution – a part of SAP Business Suite

SAP GTS has four modules:

- **SAP Compliance Management** - the part of the system, responsible for export and import legal control and sanctioned party list screening (checks against boycott lists issued by governments containing companies with which trade is prohibited by law);
- **SAP Customs Management** - the component responsible for transit procedures, customs processing, printing of trade documents and customs communications;
- **SAP Risk Management**, - the component used for preference processing, letter of credit processing and restitution;
- **SAP Electronic Compliance Reporting** – the component which is responsible for intrastat declarations: documents containing certain information

which a company in European Union is obliged to declare if it trades with other members of European Union.

SAP GTS can be integrated with logistics, sales, and finance processes of the SAP ERP system. For example, in the Customs Management component of SAP GTS it is possible to create customs declarations prior to goods receipt and perform a preliminary customs duty calculation based on purchase order from SAP ERP. For customs export processing SAP GTS can be integrated with SAP Transportation Management (SAP TM) – which is a solution from SAP for planning, execution and controlling the physical movements of goods. This allows the creation of export declarations based on freight orders from SAP TM. Some information such as nationality of the means of transport crossing the border, nationality of the inland means of transport, invoice value (net value), packaging data, dangerous goods number, etc. can be uploaded to SAP GTS system from SAP TM. SAP GTS can be also integrated with the SAP Environment, Health, and Safety Management (SAP EHS Management) application for compliance with Registration, Evaluation, Authorization, and Restriction of Chemicals (REACH) Regulation.

SAP GTS helps companies comply with:

- **"10+2" Importer Security Filling (ISF)** – a new rule which requires importers to electronically submit 10 data elements to U. S. Customs and Border Protection (CBP) department, as well as the carrier – to submit 2 more data elements. This data should be provided at least 24 hours before goods are loaded onto an ocean vessel for shipment into the U.S. SAP GTS tracks all relevant fields of documents in the system and automatically prepopulates forms for Importer Security Filling regulation. Data for ISF can be provided only via automated electronic means. U. S. Customs and Border Protection suggests that data should be filed via the Automated Broker Interface (ABI) – a component of the U.S. Customs Service's Automated Commercial System that permits qualified participants to electronically file required import data with Customs **(13)**. SAP GTS is an ABI-certified solution which allows the direct submission of data from the system to CBP.

- **International Traffic in Arms Regulations (ITAR)** – a set of United States government regulations that controls the export of military equipment, services and technology which are included in the United States Munitions List (USML). SAP GTS helps to classify products in the system by assigning them their USML numbers, automatically blocks relevant transaction where items require special license, and maintains audit trail for inspection when requested by authorities.
- **AEO** - an authorized economic operator, a status for European based company which meets requirements for safe and secure internal processes. This status allows the company to conduct simplified electronic processing within the shortest possible timeframe. SAP GTS along with SAP Risk Management helps to meet these requirements by supporting supply chain risk management **(35)**.
- **REACH Regulation** – Registration, Evaluation, Authorization, and Restriction of Chemicals Regulations is the European Union Regulation for the production and use of chemical substances. Compliance can be achieved by integrating SAP GTS with SAP ERP and SAP EHS Management. The results of compliance checks in SAP EHS Management are transferred to SAP GTS, where items get special statuses in relevant documents **(35)**. SAP GTS can ban the import/export of substances from/to specific countries, and automatically check for quantity restrictions of substances in import/export-relevant documents.

2.4.2 SAP Investigative Case Management for Public Sector

SAP Investigative Case Management (SAP ICM) is a solution for the Public Sector which supports police and other investigating authorities in the prevention, detection and investigation of crime. It is intended to provide an investigative platform for end-to-end investigation lifecycle support. SAP ICM runs on top of SAP Customer Relationship Management 7.0 (SAP CRM 7.0) –software for managing a company's interactions with customers.

The solution is able to integrate information from different systems and databases, giving users a profound picture of the investigative lifecycle. It supports advanced workflow and scheduling capabilities which minimize administrative work. SAP ICM can also be integrated with tools for data visualization and text analysis. For example, text analysis tools from the SAP BusinessObjects portfolio can extract, categories and summarize text information from a wide range of document types **(36)**.

SAP ICM supports such security mechanisms as single sign-on, role-based authorization, central user management, secure information exchange with encryption, public key infrastructure support and secure document exchange with digital signature.

Main entities in SAP ICM are Case, Lead, Location, Object, Person and Organization, Incident, and Activity. It is possible to create associations between entity data using Relationship and rate the reliability level of data using a Reliability Matrix. Case can be an object, a crime or offence under police investigation. This object is used to group related entities into a single, central access point for investigators **(37)**. Lead is an observation of the police that can be connected to the crime. A case can be created from a lead if an offence has been committed. Activity is a task that can be performed by an employee of law enforced agency. Incident is an observation which is relevant for some investigative work. An incident and the associated data can be bounded into one lead or case. Person and Organization are those parties that are the focus of policing activities and investigative cases. They can be suspects, victims, witnesses or criminal organizations.

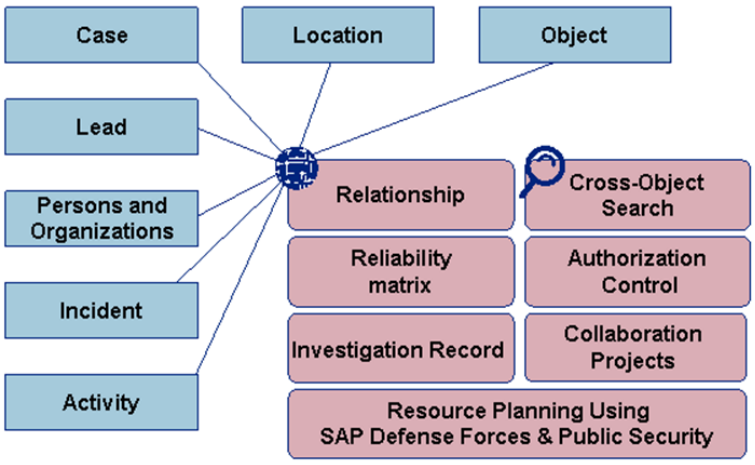

Figure 8. Main Entities, Relationships and activities of SAP ICM. Picture is taken from (37)

SAP ICM can be used in integration with SAP Defense Forces & Public Security when investigating complex criminal activities or during resource planning.

With SAP ICM it is possible to gain a single, complete, real-time view of the case, track the suspects and witnesses, manage case activities and access to the documents, search in the content of documents related to a case, easily analyze all case-related data and generate reports.

2.4.3 SAP Transportation Management

SAP Transportation Management (SAP TM) is a solution from SAP which aims to help companies organize and track the physical transportations of goods. SAP TM allows the creation of forwarding orders and freight bookings based on information from feeder systems, the planning and monitoring of the transportation, the calculating of transportation charges and compliance with foreign trade and dangerous goods regulations.

SAP TM can be used as a stand-alone application but it brings most benefit when it is installed together with SAP ERP Central Component (SAP ECC 6.0) for end-to-end process integration. For example, shipment (or transportation) requests can be generated based on transportation orders from SAP ERP. Moreover, SAP TM can be integrated also with following SAP solutions:

SAP Global Trade Services (SAP GTS) - for customs and compliance management. In SAP GTS relevant export declarations can be generated based on information from freight orders in SAP TM.

SAP Event Management (SAP EM), a SAP solution for managing activities within and between companies, - for event notifications and event handling during the transportation of goods.

SAP Environment, Health, and Safety Management (SAP EHS Management) - for dangerous goods handling, which is regulated by numerous laws and regulations, such as special requirements for receiving goods and goods issue processes, storage, labeling and printouts.

This process integration supports visibility and transparency for both global and domestic shipping, allow a company optimize and enhance its transportation management processes and make better business decisions.

2.4.4 SAP Auto-ID Enterprise

SAP Auto-ID Enterprise **(38)** is a solution for serialization of information in a wide variety of supply chain, manufacturing, service, etc. and comprises two products: the SAP Auto-ID Infrastructure (SAP AII) and SAP Object Event repository. SAP Auto-ID Enterprise supports technologies such as linear bar codes, RFID tags, sensors, etc. and support standard-based serialization such as Electronic product Code or EPC, a standard used to track the progress of objects as they move through the supply chain **(22)**.

SAP Object Event Repository is the repository which allows capturing, storage and querying data about uniquely identified objects. It is implemented together with multiple instances of SAP Auto-ID (SAP automatic-identification) infrastructure as part of SAP Auto-ID Enterprise. SAP Auto-ID is networked infrastructure that can acquire, filter, aggregate, store and publish massively high volumes of real-time Auto-ID information from electronically tagged items (e. g. a bar code, or RFID tag), sensors and global positioning systems (GPS). Auto-ID is integrated as an information service in SAP NetWeaver as part of the information integration layer. To monitor information from tagged items, SAP Auto-ID uses the Electronic Product Code (EPC), which is attached to every physical object of interest and uniquely identifies this object.

Automatic monitoring of events, setting up alerts and exception management scenarios happens in SAP Object Event Repository through use of SAP Event Management **(39)**

Chapter 3

The Concept

In the following chapter I present the concept for container risk evaluation process. I describe the main steps of the process as well as discuss reasons for the chosen design.

3.1 Definition of the Problem

As a part of the ECSIT project the overall goal of my Master's Thesis is to make the supply chain of containerized cargo more secure, efficient and effective. With introduction of House Resolution 1 (or "100% scanning law") marine ports face a big problem of increased workload and scanning of every container may lead to unacceptable bottle-necks in their work.

Every day Customs Authorities process a huge amount of data in order to decide which sea containers can cross the border and which cannot. The correct decision must be made quickly and at low cost. At the same time legislation for international trade is constantly changing with governments introducing more laws and regulations.

It is against this backdrop that I address in my Master's Thesis the uncertainties presented, in particular:

- which exact information is needed for container risk evaluation;
- how this information can be evaluated;
- how to integrate the risk evaluation process into the supply chain.

The problem of possible industry espionage that can occur as a result of sharing security related supply chain data is not the focus of this Master's Thesis. The problem is described in greater detail in Chapter 5 "Evaluation".

3.2 The Risk Evaluation Process

The process of container risk evaluation which I suggest in my Master's Thesis is semi-automatic. It means that part of the process can be done automatically according to the algorithm implemented in the prototype developed within the project while another part can only be processed manually. The reason for this particular design is that although human errors can be minimized and speed at which data is analyzed by implementing algorithms increased, the final decision about the container should only be made by an authorized member of the customs authorities.

The process of analyzing data for deciding if a certain container can be released into the US is time consuming since customs authorities have to check a lot of information. At the same time marine ports such as Port of Bremerhaven handle around 54.7 million tons of containerized cargo annually (data for the Port of Bremerhaven, 2008 **(40)**). Taking into account substantial volumes of the US bound cargo involved the necessity to scan every container can lead to unacceptable bottle-necks in the work of marine ports. In the process of Container Risk Evaluation developed within the ECSIT project I suggest an alternative for the "100% scanning" law: after automatic thorough analysis of all relevant information for container security available for the customs authorities, the container is sent for scanning only if some security issues were discovered by the system during its transportation. Security alerts from the system can be raised if for example the container seal was opened during the transportation or one of the carriers is not AEO/C-TPAT certified.

In the ECSIT project we assume that the port has an x-ray gate at the entrance to the harbor for initial scanning while the container is entering the harbor as well as another inside the harbor for further scanning if needed.

The process of Container Risk Evaluation can be divided into three phases:

- Automatic capturing of data by the system during packing and transportation of the container from the manufacturer to the entrance of the last foreign port before loading onto vessel bound for the USA;
- Automatic analysis of all incidents that could have happened during the previous phase in order to decide if the container should be scanned or not (the

subprocess which takes place while the container is waiting for permission to enter the harbor);

- Manual analysis of scan images and all incidents that happened with the container during its transportation to the harbor entrance (the subprocess takes place when the container is inside the harbor).

The process is different when the container cannot be scanned or if no incidents occurred during its transportation to the harbor entrance: details are described later in this section. The process is represented at the high level in the picture below:

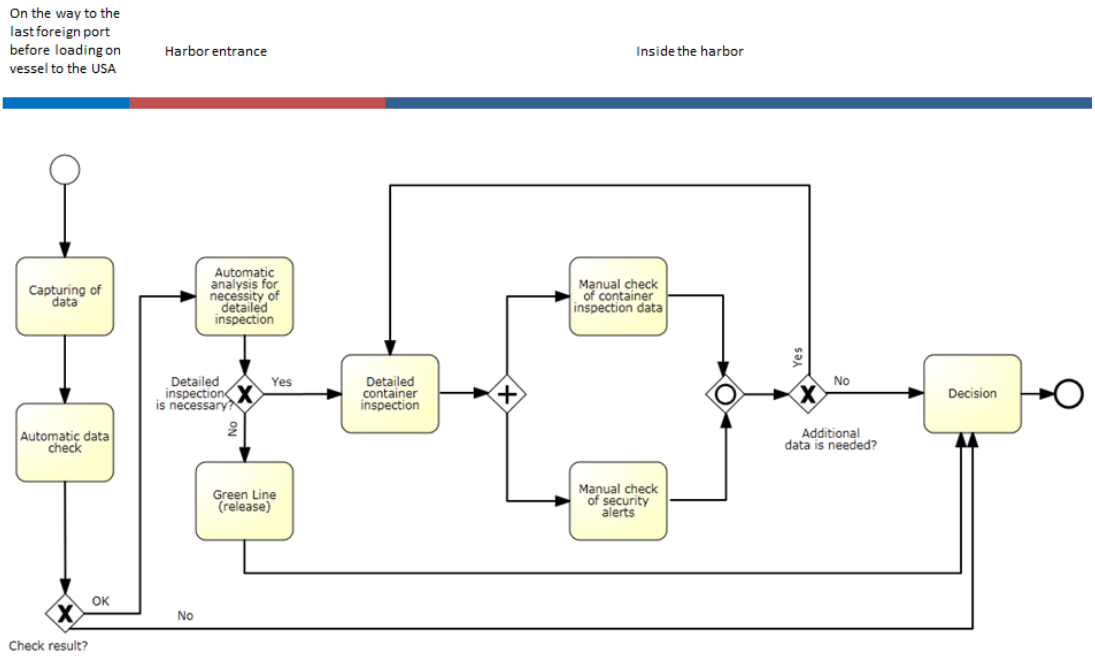

Figure 9 Three Steps of the Process

In the following sections I describe the main steps of the process, the types of data which should be collected for the Container Risk Evaluation process and finally, give several examples of possible systems alerts.

3.2.1 Automatic Capturing of Data

The process starts with the automatic capturing of relevant security data and uploading it to an IT system for evaluation. Data such as supplier ID, buyer ID, container ID,

container parameters, port of landing, etc. is first gathered when the container is packed at the loading area by the supplier. All data which feeds into the system is automatically checked for completeness, compliance and against criteria detailing prohibited cargo, terrorist organizations, and economic and political embargoes. If the data is incomplete, a request for additional information is sent automatically. These steps of the process are executed during the transportation of the container to the last port before loading onto a vessel bound for the USA.

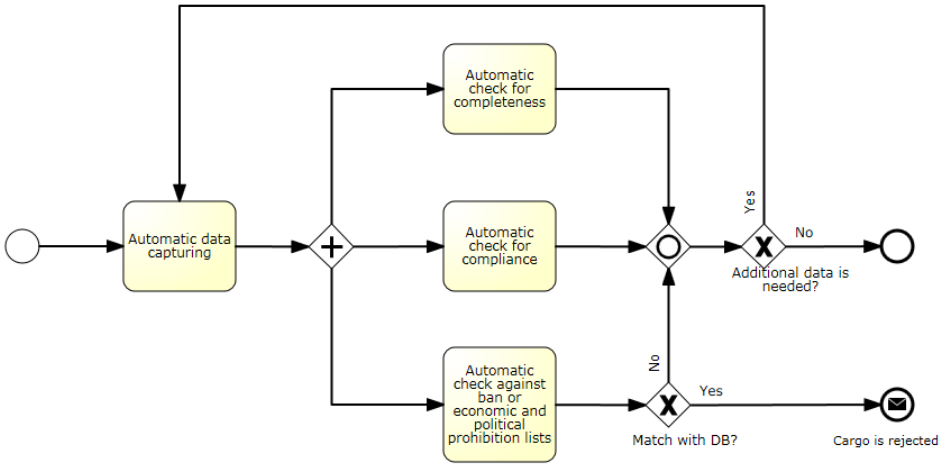

Figure 10 Automatic capturing of data

The main steps of the process are not strictly tied to the data which should be captured during the transportation of the cargo. The parameters according to which data is checked as well as the sort of data can be easily adjusted to the current law or customs authorities' needs. Later I describe data which the Container Risk Evaluation Tool captures for automatic analysis of the risk.

3.2.2 Data for Capturing

There are several European and international regulations which oblige supply chain actors to submit certain data as part of declaration for international transportation of cargo.

The European Commission regulation No 1875/2006 amending Regulation (EEC) No 2454/93 provides provisions for the implementation of Council Regulation (EEC) No 2913/92 which lists requirements for entry and exit summary declarations. The annex 30A in the regulation contains the detailed data elements that must be provided as part of the summary declarations for all goods entering and leaving the customs territory of the EU.

The table below is adopted from **(41)** and displays the required data elements. The table excludes situations when participants of the supply chain have Authorized Economic Operator (AEO) status, in which case the number of data requirements is reduced. Table does not present requirements for postal, road and rail modes of transportation either. "Item level" indicates an element that is requested at the declaration item of goods level, "header level" indicates an element which is required at declaration header level and "cons. level" - a data element which must be submitted on a consignment level.

Name	Exit summary declaration	Entry summary declaration
Number of items	header level	header level
Unique consignment reference number	item/header level	item/header level
Transport document number	item/header level	item/header level
Consignor	item/header level	item/header level
Person lodging the summary declaration	header level	header level
Consignee	item/header level	item/header level
Carrier		cons. level
Notify party		item/header level
Identity and nationality of active means of transport crossing the border		cons. level
Conveyance reference number		cons. level
First place of arrival code		cons. level
Date and time of arrival at the first place of arrival in Customs territory		cons. level
Country(ies) of routing codes	header level	header level
Customs office of exit	header level	
Location of goods	header level	
Place of loading		item/header level
Place of unloading code		item/header level
Goods description	item level	item level
Type of packages (code)	item level	item level
Number of packages	item level	item level

Shipping marks	item/header level	item/header level
Equipment identification number, if containerized	item/header level	item/header level
Goods item number	item level	item level
Commodity code	item level	item level
Gross mass (kg)	item/header level	item/header level
UN Dangerous Goods code	item level	item level
Seal number	item/header level	item/header level
Transport charges method of payment code	item/header level	item/header level
Declaration date	header level	header level
Signature/Authentication	header level	header level
Other specific circumstance indicator	header level	header level

Table 1 ICS/ECS data elements

According to the Importer Security Filing (ISF) or "10+2" rule the following data must be provided to the customs authorities before the cargo is laden aboard a vessel destined for the United States:

Importer of Record Number – as it was explained earlier in the Chapter 3 Background Information and Related Work, it can be an Internal Revenue Service (IRS) number, Employer Identification Number (EIN) or Social Security Number (SSN);

Consignee number - if the deliver-to is other than the importer of record, it is the Internal Revenue Service (IRS) number, Employer Identification Number (EIN) or Social Security Number (SSN);

Seller (Owner) name/address – as it is explained in the ISF Regulation, it is the name/ address of the last known entity by whom the goods are sold;

Buyer (Owner) name/address – the name of the owner of the goods, it can be the same as Seller ISF-10 data element;

Ship to name and address - the name and address of the first deliver-to party scheduled to physically receive the goods after the goods have been released from customs custody (CBP requires the actual name/address, not the corporate address);

Manufacturer (Supplier) name/address - the name and address of the organization that last manufactured, assembled, produced, or grew the commodity, or the name and address of the supplier of the finished goods in the country from which the goods are leaving;

Country of origin - country of origin specified for each article in the shipment;

Commodity HTS-6 - 6-digit HTS number for each article in shipment, the Commodity Harmonized Tariff Schedule of the United States (HTSUS) number must be provided in the six-digit format, and is used for determining tariff classifications for goods imported into the US.

Two more data elements are needed to be provided as early as possible, but no later than 24 hours prior to the ship's arrival at a U. S. port: **Container Stuffing location** and **Consolidator name/address**.

The set of data described above is considered to be the "Cargo Details" category of information available for customs authorities according to the Container Risk Evaluation Tool terminology.

For risk evaluation it is vital to collect data about the seal of the container. Nowadays simple bolt seals are the most often used for shipping containers, but in the concept I assume that electronic smart seals, which allow data exchange with backend systems and record opening and closing of the container are used. Data from electronic seal helps to analyze all accidents which might happen with the container during its transportation, for example, unauthorized opening of the container in an attempt to smuggle goods.

For reliability analysis of the participants of the corresponding supply chain it is useful to capture the data about their possession of relevant **certificates/statuses**, such as AEO status or C-TPAT certification.

Moreover within the ECSIT project it is possible to collect certain **logistical information** of the container such as the GPS coordinates of business location where the container was recorded by RFID/bar code readers, as well as time stamp of the corresponding event.

Information about the cargo can be obtained by customs authorities from three main sources:

- other authorities (domestic or foreign);
- supply chain participants - information can be provided before, during and after the physical flow of the cargo;
- external sources, i.e. third party sources such as media or individual citizens, as suggested by CASSANDRA in **(41)**.

More detailed they are depicted in the figure below:

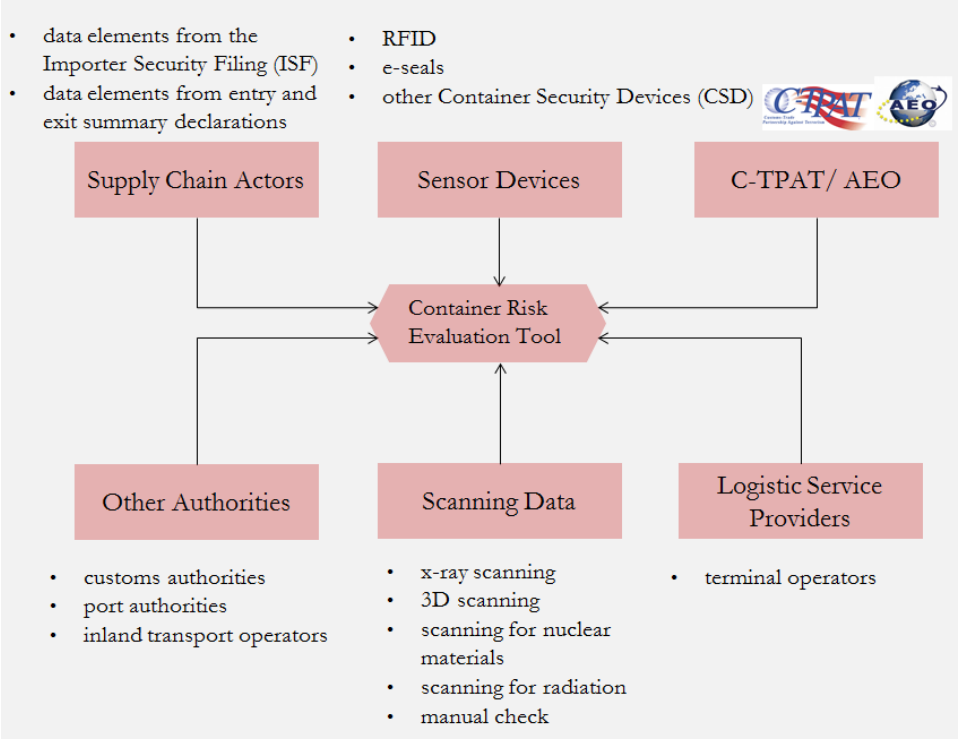

Figure 11 Main sources of information about the container

Some of required data is collected from various governmental organizations. In general it can be authorities that issue different licenses, permits and certificates. In most cases such organizations maintain electronic databases of certified operators. For example the database of Authorized Economic Operators can be found in **(7)**.

Supply chain participants mainly exporters, importers and carriers are obliged by law to submit a certain data to customs authorities. If cargo is intended for the United States a certain data must be submitted to U.S. customs authorities before the cargo is laden aboard a vessel destined for the United States (the Importer Security Filing law). In EU territory the Import Control System (ICS) obliges carriers to submit pre-arrival information for all cargo entering EU territory for shipment risk analysis purposes. The Import Control System (ICS) is an electronic security declaration management system for the transportation of goods into the European Union customs territory. Detailed information must be provided in the form of an Entry Summary Declaration (ESD) that includes information about "contents of cargo, planned routing and traders

involved with the movement of the goods" **(42)**. For containerized maritime cargo, this information must be submitted 24 hours before loading at the port of origin. A complete list of ICS/ECS data is shown in Table 1 of this paper.

Third parties can also provide information which can be relevant for risk evaluation; they can be informants or companies specializing in risk-related information and data collection.

Sources where information about the cargo and supply chain partners can be fed into the system for container risk evaluation are described later in this chapter in section "Integration of the Container Risk Evaluation Process with the Secure Supply Chain Process Supported by the ECSIT Infrastructure".

3.2.3 Automatic Analysis of Incidents

For efficient process implementation the decision about container scanning should be ready by the time when container arrives to the harbor. As it was mentioned above only containers with suspicious supply chain participants or raised security alerts based on analysis of the container's route and seal log have to be sent for scanning or manual check while entering the harbor. Other containers can enter the harbor without scanning and can be released without further inspection. The diagram below shows the process flow and a detailed description of the second phase of the process follows after.

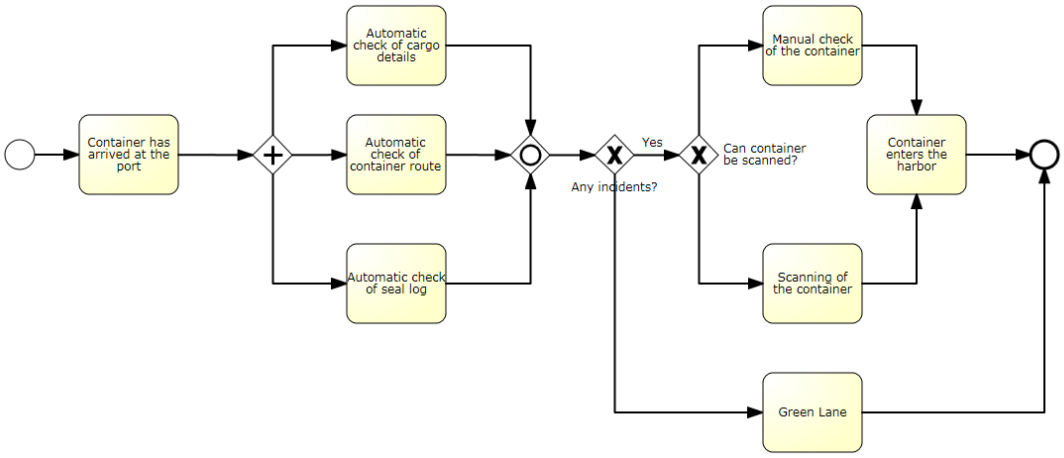

Figure 12 Automatic analysis of incidents

As soon as the container arrives at the harbor entrance the system decides whether it must be sent for detailed inspection. The decision is made automatically based on general data about the supply chain partners such as name, address, and certifications as well as all incidents which occurred during the transport, e.g. unauthorized opening of the container seal or deviation from the defined route. Not all system alerts are caused by criminal action connected to the container: for example the seal of the container can be opened for random inspection during the transportation but the automatic check of seal log can raise an incident in this case. The reason for that is the fact that customs authorities need to be absolutely sure about the container which enters the harbor without any detailed inspection as it is possible green line scenario: the container should not carry anything suspicious.

A detailed inspection of the container includes x-ray container scanning, scanning for nuclear materials or radiation or manually inspection if the cargo cannot be scanned. If there are no suspicious incidents the system can decide to release the cargo without inspection.

The automatic container risk evaluation process is based on an analysis of data categories such as Cargo Details, Cargo Route, Scan Result and Seal Log, which are described below.

Cargo Details. Data which is provided within the Cargo Details category as it was mentioned above, mainly data from the Importer Security Filing (ISF) data elements, provides information about supply chain participants. This data allows checking business partners against database of terrorist organizations, economic and political embargoes. Based on this data the system can check if all supply chain participants are trusted organizations, e. g. they have AEO status, C-TPAT certificate or equivalent. Later information from the Cargo Details category, such as Commodity HTS Number, HazMat Code, and cargo description from the Cargo Manifest can be used by customs authorities during the analysis of results from x-ray scan or manual check.

Cargo Route. The idea of the automatic cargo route analysis is to monitor for deviation from the planned route or suspicious stops during which manipulation with the container can occur or unauthorized seal opening can occur. The information about the route can be obtained with the help of RFID and GPS Tracking Devices attached to the

container. The information about unauthorized opening of the container can be derived through the seal log provided by container's electronic seal.

By analyzing the cargo route several scenarios can be implemented. Below I describe some of them.

Scenario 1. One scenario can be the comparison by the system of the actual and planned cargo routes. This is possible to implement if a company responsible for the container transportation has provided a transport plan to the customs authorities. In this case the time threshold should be set in the system after which the system should compare the real GPS coordinates of the container with the ones listed in the plan as well as the time when the container appeared there. It is obvious than an 100% match is impossible even if the container followed the planned route but a time frame can be set up within which the deviation is not considered to be critical.

Scenario 2. Another scenario can be the use of a geo-fence. A geo-fence is a virtual perimeter for a real world geographical area. It allows the drawing of zones around places and triggering alerts in software where the geo-fence was implemented if borders of these zones were crossed.

Figure 13 Example of geo-fence (taken from (43))

While planning the container route the transportation company can set a geo-fence for the container. With the help of GPS Tracking Devices attached to the container any crossing of the geo-fence can be easily detected and recorded. Later this data should be provided to Container Risk Evaluation Tool where it will raise system alerts.

Scenario 3. The simplest scenario can be the analysis of all planned stops together with a seal log. The time threshold can be set up in the system to take into account the duration of scheduled container stops. If a time frame for a stop is exceeded, the system triggers an alert. This means false alerts could be generated if for example the truck with the container is delayed due to a congestion of containers waiting to be loaded. That is why it is necessary to check the data from the seal log: if the seal was opened during the suspiciously long stop then the probability of smuggling or tampering is very high and the container should be sent for a scanning.

All the scenarios described above can be combined into one if the corresponding technologies are implemented within an infrastructure in use.

Seal Log. Data from the electronic seal log is important for container risk evaluation. This data can contain information about the seal standard, unauthorized seal opening or change of the seal for a lower standard during the container transportation.

In case of using smart Container Security Devices (CSD) such as sensors which can measure temperature, humidity or cargo weight, this category can display information about anomalies detected by these devices.

Scan Results. The Scan Result data set contains scan images, the indicator if the cargo is radioactive, and lists of radioactive substances. In general this data should be analyzed manually. The only case when this data can be analyzed by the system is if the container needs to be sent for radioactivity scanning. A system alert can be raised if radiation levels above certain threshold are detected. The threshold can be set in the system in advance.

3.2.4 Examples of System Alerts

The research on customs risk management conducted by the CASSANDRA project (**(41)**, **(44)**) provided 14 illustrative examples on what might be considered as "high risk indicators" by customs administrations, based on information obtained from the supply chain participants. These examples are presented in the table below.

Supply chain actor / stage	Illustration on what might be considered as "high risk indicators"
Shipper	Shipper has not exported the specific commodity before Shipper information cannot be found from commercial registers or from the Internet
Commodity	Hazardous materials which may be used for terrorist acts: e.g. Sulphur Dioxide and Iridium 192 Common materials which may be used for concealment purposes: e.g. sugar and auto parts
Country of origin	High level of corruption in the country Non-existing (or low) level of export controls: e.g. pre-cursor chemicals, narcotics, and dual use goods.
Carrier	Specific crew associated with organized crime Carrier history of frequent violations of customs enforced regulations
Container	Goods description does not match with the container type or with the total weight of the container. Discrepancies in seal numbers (documents versus actual seal)
Routing and transshipments	Routing of shipment is not cost effective Transshipment cost paid with cash
Importer	The frequency of imports does not support a "sustainable business". A suspect employee is working for the importer.

Table 2 High Risk Indicators

3.2.5 Manual Analysis of Incidents and Scan Image

The container which went through detailed inspection while entering the harbor is subject to manual analysis of the security risk by a customs officer. The idea of the whole process is that the IT system can only help to evaluate the security risk of the container but only a particular person, a customs officer, can make the final decision if the container can be released or not. Every case corresponding to a certain container has a history log in the system, so that it is possible to track all the actions of the person responsible for the case. The way how cases are assigned to employees of the customs office does not influence the process of the risk evaluation. In the prototype developed

within the ECSIT project cases are assigned automatically to the first employee who is available at the time when the information from a detailed inspection of the container is available. It is implemented in this way as I assume that customs officers should not have right to choose the case in order to avoid possible subjectivity in the decision and congestion of "unattractive" cases.

When information from a detailed inspection is available, the customs officer analyses the scan image or results from manual check together with all security alerts. This can include checking suspicious supply chain partners, seal logs, container parameters, cargo descriptions etc. This part of the process can be repeated if the container is sent for scanning inside the harbor or if after all inspections it is sent for an additional manual check. After the manual analysis of all data the decision on whether container should be released or rejected must be made.

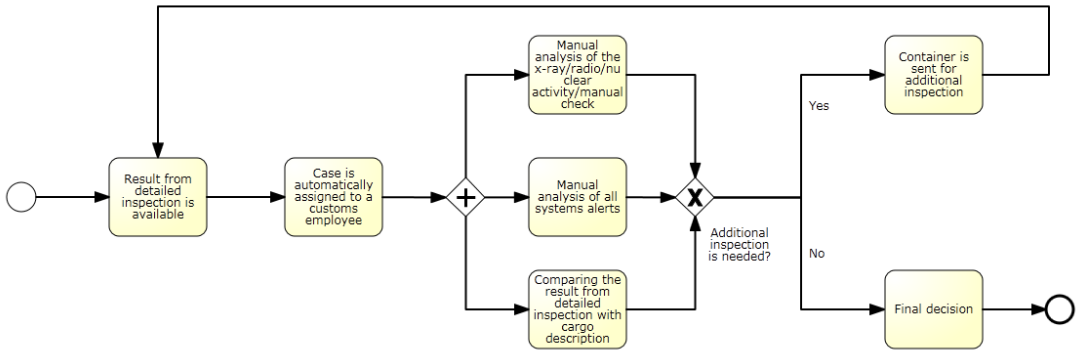

Figure 14 Manual Analysis of Incidents and Scan Image

3.3 Integration of the Container Risk Evaluation Process with the Secure Supply Chain Process Supported by the ECSIT Infrastructure

Earlier in this chapter I discuss the type of information that might be required by the customs authorities for risk evaluation process. I also describe sources of this information from legislative point of view i. e. which type of data is obliged to be

provided to the customs authorities by which regulation/law. Finally I outline at a high level the sources of this information (e.g. port authorities, terminal operators, sensor devices, etc.). In this section I briefly discuss the integration of the Container Risk Evaluation process with the ECSIT infrastructure and sources from where the information comes into the Container Risk Evaluation Tool.

Integration with LCH Repository. The Container Risk Evaluation Tool is integrated with SAP Object Event Repository, described in Chapter 2 "Background Information and Related Work". In the ECSIT infrastructure SAP Object Event Repository, or EPCIS Repository, is one of the components of the Logistic Collaboration Hub, a platform for collaboration of the supply chain actors. Information from RFID tags and bar code readers is fed from partner systems to the EPCIS Repository of the Logistic Collaboration Hub, from where it is retrieved by the Container Risk Evaluation Tool. EPCIS is a query interface and a protocol developed by EPCglobal so that supply chain partners have a common method of integrating object unique information **(22)**. The EPCIS standards based data repository, implemented as SAP Object Event Repository, allows product serialization (tracking a product as it moves through the supply chain), data capture and storage in a standardized format (in the form of EPCIS events).

Integration with GPS navigation and Smart Lock systems. Although the GPS coordinates of events which are recorded by RFID and bar code readers are fed into the Logistic Collaboration Hub, the integration with the project partner's GPS navigation and smart lock systems is planned for near future as the GPS coordinates of locations where events are recorded do not provide a constant tracking of the containers.

Information from the RFID/bar code readers, GPS systems and smart locks constitutes additional logistical information or Cargo Route category as described in this chapter earlier.

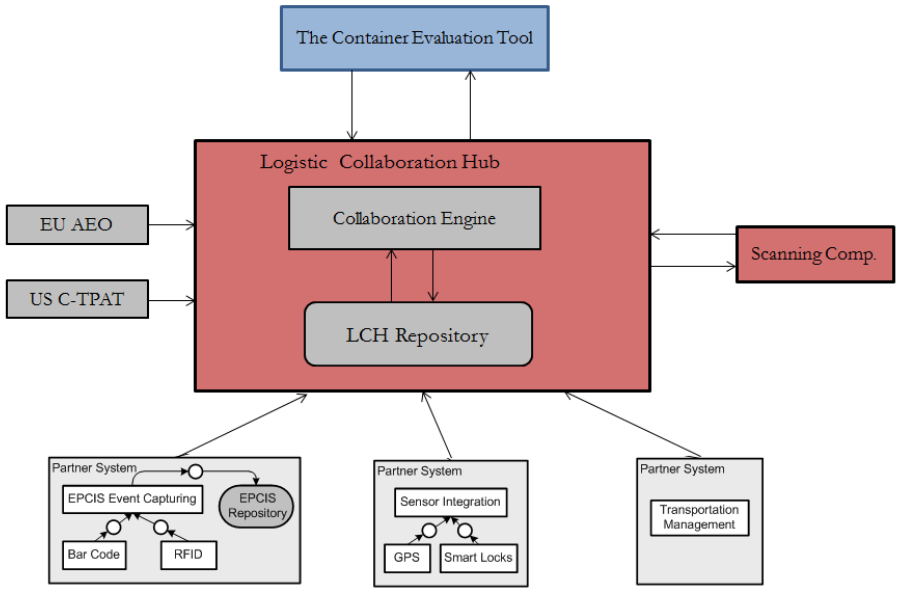

Figure 15 Integration of the Container risk Evaluation Tool with the ECSIT Infrastructure

Integration with Collaboration Engine. Another component of the Logistic Collaboration Hub is a Collaboration Engine which is responsible for the secure supply chain. It supports the collaboration of supply chain actors and information exchange between them. Data about the shipper, seller, importer, etc. can be provided through this Collaboration Engine. This data forms the Cargo Details category of information needed for the risk evaluation process. The integration with data from the Collaboration Engine is not implemented yet.

One of the options for customs authorities to collect data on the supply chain partners (such as name, address, AEO/C-TPAT certification and so on) is to get it directly from the partner's systems.

Integration with Scanning Component. The Container Risk Evaluation Tool should be integrated also with the scanning component of the ECSIT infrastructure. Currently only the integration between the Logistic Collaboration Hub and scanning component is implemented. To be precise, Collaboration Engine gets the link to the scan image of the container which is physically stored in the local database of the scanning component. For the real deployment of the system the direct channel between the Container Risk Evaluation Tool and the scanning component should be established.

Integration with AEO/C-TPAT databases. For real implementation of the concept, the mechanism for AEO status/C-TPAT certification verification of the supply chain partners must be provided. At the present moment although the information if a partner is certified or not can be theoretically provided by the Collaboration Engine, the procedure of verification and confirmation of this information does not exist yet.

Chapter 4

Description of the Container Risk Evaluation Tool

In the following chapter I present the design of the Container Risk Evaluation Tool developed within my Master's Thesis Project. As a first step the technologies, which are used for the implementation are described. After that I outline the overall design of the application. Finally I discuss the integration of the application with the ECSIT project infrastructure.

4.1 Technical Description

After conducting research on existing technical solutions for supply chain management, transportation management and global trade the following technologies have been chosen for the Container Risk Evaluation Tool:

- SAP NetWeaver 7.0
- SAP Auto-ID Enterprise, comprising of two products: SAP Object Event Repository (SAP OER) and SAP Auto-ID Infrastructure (SAP AII)
- SAP Event Management (SAP EM)
- SAP Visual Business Component
- SAP Web Dypro ABAP

Later I describe each technology in more detail and outline the reasons for its selection for use in the implementation of the prototype.

SAP NetWeaver 7.0 **(45)** has been chosen as a development platform for the Container Risk Evaluation Tool prototype. The main reasons for this decision are:

- a significant part of the functionality needed is already implemented in the SAP Global Trade Services (SAP GTS) system, as described in Chapter 2

"Background Information" (for example, the algorithm of check for compliance with the Importer Security Filing, also known as the "10+2" initiative, or compliance with REACH Regulation, etc.);

- there is a possibility that customs authorities already use SAP Enterprise Core Component (SAP ECC), SAP Global Trade Services (SAP GTS) and SAP Customer Relationship Management (SAP CRM) in their everyday work – the integration of the Tool with these systems is technically very easy to implement;
- the majority of big importers run SAP solutions such as SAP GTS, SAP CRM and SAP Transportation Management (SAP TM), which makes it easy to integrate the Container Risk Evaluation Tool with the systems of both supply chain actors and customs authorities.

SAP NetWeaver is the current service-oriented integration platform which provides the development and runtime environment for SAP applications and can be used for integration with other applications and systems. For user interface development I use Web Dynpro for ABAP (WD ABAP) technology, which is the SAP standard UI technology for developing Web applications in the ABAP environment. It consists of a runtime environment and a graphical development environment with special Web Dynpro tools that are integrated in the ABAP Workbench (development tool of SAP NetWeaver platform).

As already made clear above the programing language used for the prototype development is ABAP – Advanced Business Application Programming, a high-level programming language created by SAP.

In the Container Risk Evaluation Tool a geographical map is used for displaying the route of the cargo. This technology is provided by SAP Visual Business, a user interface technology that visualizes data from SAP and external data sources on a single screen. In the prototype SAP Visual Business Component is embedded into a Web Dynpro application (the Container Risk Evaluation Tool itself) so that application can define a data exchange between the Visual Business application and the Web Dynpro application. Thus, data available within the Web Dynpro is used to illustrate business elements such as the locations of the container and the links between them that represent the container route. In the prototype the Visual Business component is

integrated by means of Web Dynpro technology. For use of SAP Visual Business component the Microsoft .NET Framework 3.5 Service Pack 1 is used.

The prototype is integrated with SAP Auto-ID Enterprise by being a Web Dynpro application in SAP Object Event Repository. SAP Auto-ID Enterprise **(38)** is a solution for the serialization of information and comprises of two products: the SAP Auto-ID Infrastructure (SAP AII) and SAP Object Event repository. SAP Object Event Repository is the repository which allows the capturing, storage and querying data about uniquely identified objects. The system is described in greater detail in Chapter 2 "Background Information and Related Work".

The automatic monitoring of events, setting up of alerts and exception management scenarios is handled in SAP Object Event Repository through the use of SAP Event Management **(39)**.

4.2 Design of the Prototype

The Container Risk Evaluation Tool is a Web Dynpro application with the name ZCUS_RISK_EVALUATION_V2, integrated into the SAP OER system. It has six main views: FIRST_VIEW, CARGO_DETAILS, CARGO_ROUTE, SCAN_RESULT, SEAL_LOG and DOCUMENTS. In addition to these six views it also has several auxiliary views which are not described here. View of Web Dynpro application contains the visible part of Web Dynpro components. Consequently, it consists primarily of UI elements. Additionally, the View controller allows for responding to user actions.

In any Web Dynpro application views are grouped into a window to be displayed into a relevant context and enable navigation between individual views. In the Container Risk Evaluation Tool the window which groups all main views is called MAIN and is initialized when the application starts:

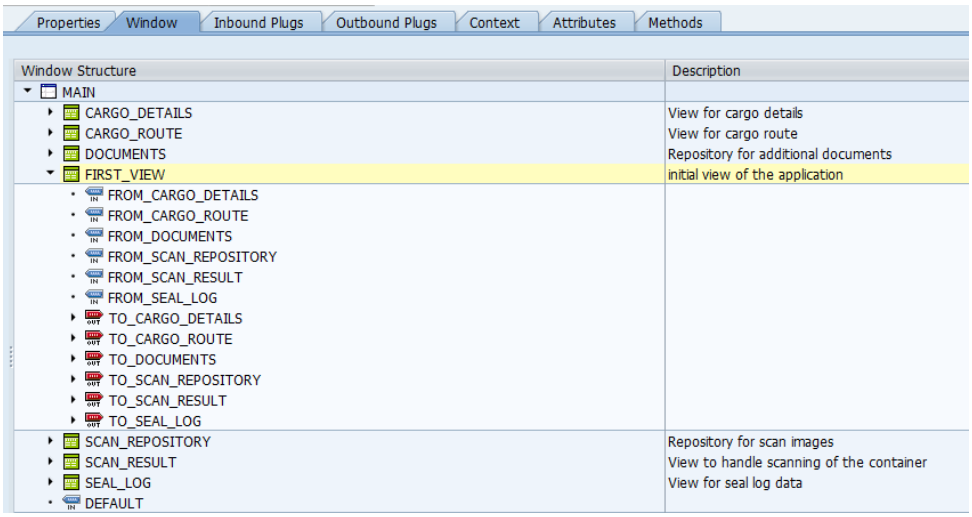

Figure 16 the main window of the application and its content

For navigation purposes each view has inbound and outbound plugs, which represent entry and exit points for the view. All actions, which are needed to be implemented when a plug fires, are set in a corresponding for that plug method. From the figure above it is seen that the FIRST_VIEW, the initial view that is seen by the user when the application starts, has several inbound and outbound plugs. From the user point of view they fire when the user wants to go to a risk category and back, as it is seen from the figure below:

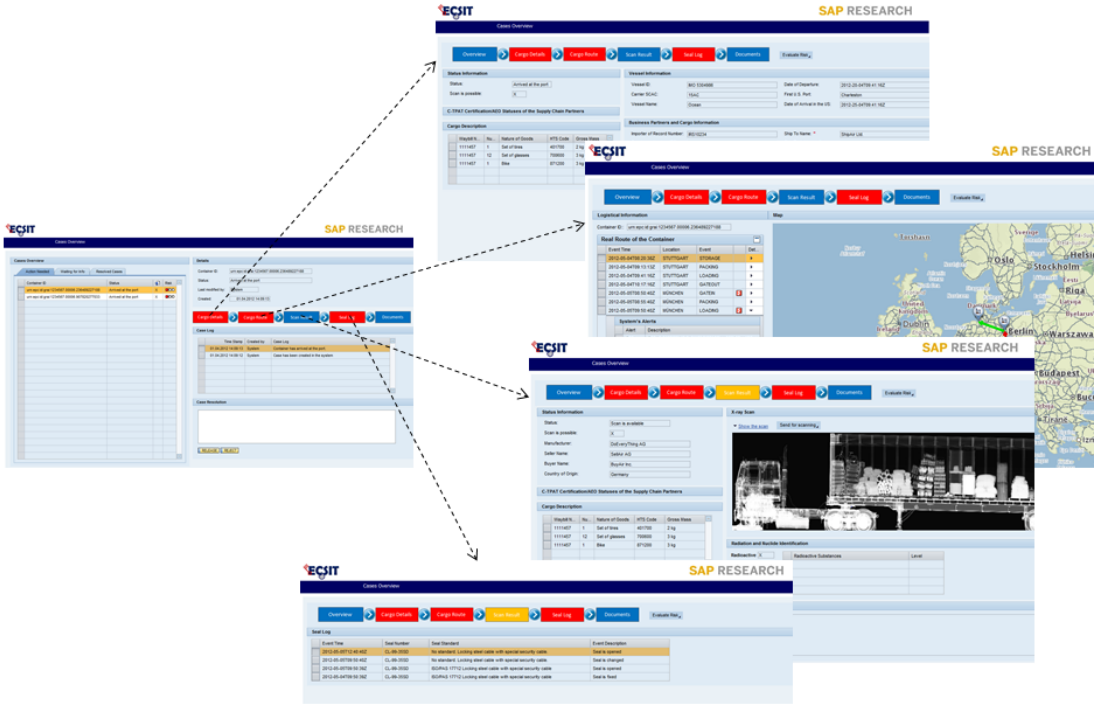

Figure 17 Views of the application

As an example, the figure below explains what is happening when a user navigates from the initial view (cases overview) to the view with cargo details. When a user presses the button "Cargo Details" on the initial view, the corresponding outbound plug of the FIRST_VIEW fires:

```
3  method ONACTIONGO_TO_CARGO_DETAILS .
4
5      wd_this->fire_to_cargo_details_plg(
6      ).
7
8  endmethod.
```

Figure 18 Outbound plug "to_cargo_details" of the initial view

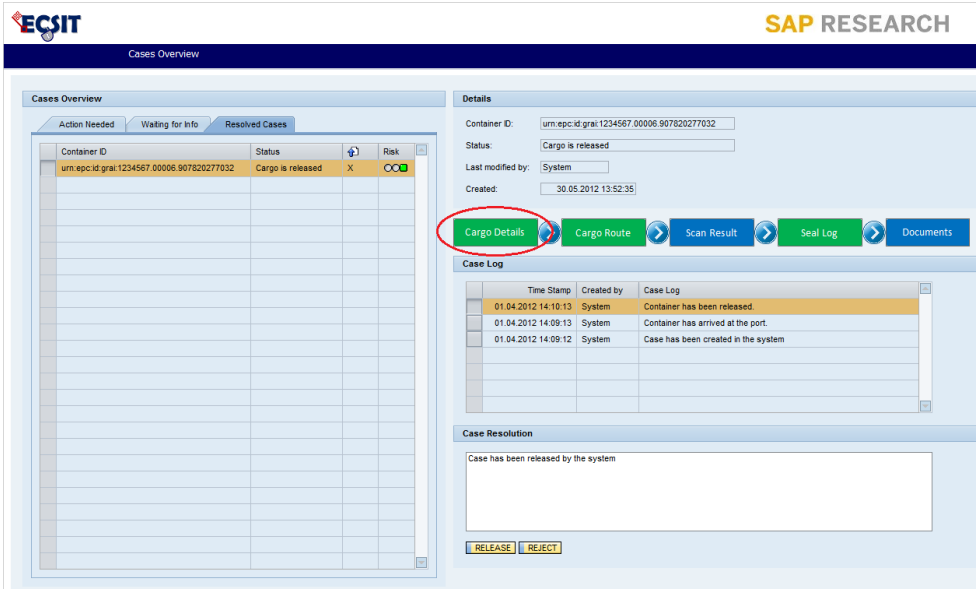

Figure 19 Navigation to the cargo details view

In the method which is responsible for firing the corresponding inbound plug of the CARGO_DETAILS view all actions that should be implemented while opening the view are set. For example, the cargo details data (mainly ISF data) is displayed on the screen:

```
"""""""""""""""ISF data"""""""""""""""""""""""""""""""""""""""""""""""""""

DATA lo_nd_cargo_details TYPE REF TO if_wd_context_node.
DATA lo_el_cargo_details TYPE REF TO if_wd_context_element.
DATA ls_cargo_details TYPE wd_this->element_cargo_details.
DATA lv_case_id TYPE wd_this->element_cargo_details-case_id.
DATA lo_nd_isf_data TYPE REF TO if_wd_context_node.
DATA lo_el_isf_data TYPE REF TO if_wd_context_element.
DATA ls_isf_data TYPE wd_this->element_isf_data.

lo_nd_cargo_details = wd_context->get_child_node( name = wd_this->wdctx_cargo_details ).
lo_el_cargo_details = lo_nd_cargo_details->get_element( ).

lo_el_cargo_details->get_attribute(
  EXPORTING
    name = `CASE_ID`
  IMPORTING
    value = lv_case_id ).

lo_nd_isf_data = wd_context->get_child_node( name = wd_this->wdctx_isf_data ).
lo_el_isf_data = lo_nd_isf_data->get_element( ).

SELECT * FROM zcus_isf_data
  INTO CORRESPONDING FIELDS OF ls_isf_data
  WHERE case_id = lv_case_id.
ENDSELECT.


lo_el_isf_data->set_static_attributes(
   static_attributes = ls_isf_data ).
```

Figure 20 A piece of code from the HANDLEFROM_FIRST_VIEW method

The whole logic of the application is implemented in the manner as described above. The only difference from a design point of view is the implementation of the methods responsible for retrieving data from SAP Object Event Repository, such as ID of the containers, loading of the container, storage, arriving of the container to the storage area, etc. These methods are implemented in a separate assistant class of the application. For using a map in the Web Dynpro application, SAP Visual Business Component is embedded into it. In the application the standard Geo-Map window (MAIN_WINDOW of the SAP Visual Business Component) is embedded into CARGO_ROUTE view with the help of UI Element MAP:

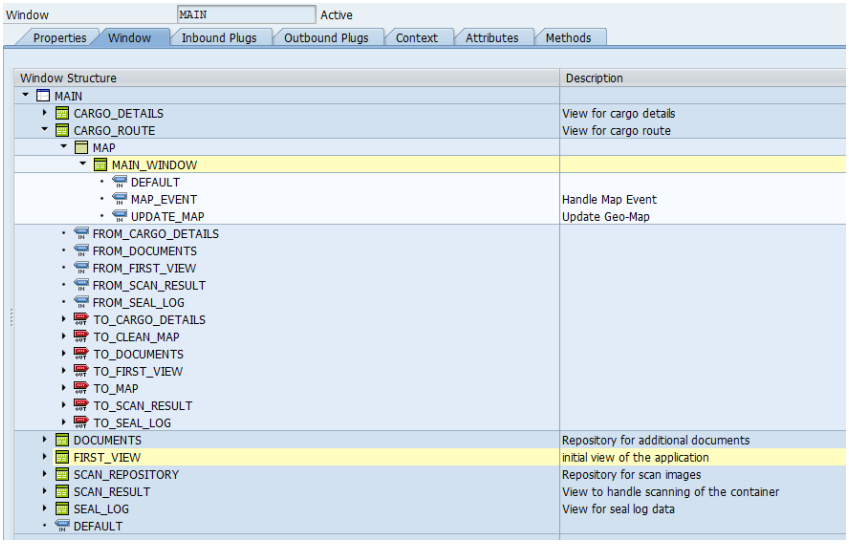

Figure 21 Embedded into the CARGO_ROUTE view for the map

Navigation and data flow between SAP Visual Business Component and the Web Dynpro application is implemented with the help of Inbound and Outbound plugs in the same way as it is described above for all views of the application.

4.3 Integration of the Container Risk Evaluation Tool with the ECSIT Infrastructure

Earlier in Chapter 3 "The Concept" I describe the concept of how the Container Risk Evaluation Process can be integrated into the secure supply chain supported by the ECSIT infrastructure and the sources of security relevant information that can be collected for the Container Risk Evaluation Tool. In the following section I describe in detail how the integration of the Container Risk Evaluation Tool with the ECSIT infrastructure is implemented.

Integration with LCH Repository. As described in the previous chapter, a main component of the ECSIT Infrastructure is the Logistic Collaboration Hub, a platform for collaboration between supply chain actors. The Container Risk Evaluation Tool is integrated with the EPCIS standards based data repository of this Hub, which is represented by the SAP Object Event Repository, described in Chapter 2 "Background Information and Related Work". EPCIS is a query interface and a protocol developed by EPCglobal, so that supply chain partners have a common method of integrating object unique information **(22)**.

In the Container Risk Evaluation Tool the information, obtained from SAP OER is used for logistic related information, such as tracking of the container along with the supply chain and route assessment (e.g. comparison of the actual cargo route with the planned route).

The Container Risk Evaluation Tool is a Web Dynpro application in the SAP OER system. The integration is implemented in the way that an auxiliary background program in the SAP OER system retrieves data in a standard XML form from the event repository and pushes it to the local database tables which are used by the Tool. From these database tables the application retrieves relevant data by means of a standard way in ABAP - Open SQL language which provides uniform syntax and semantics for all of the database systems supported by the SAP.

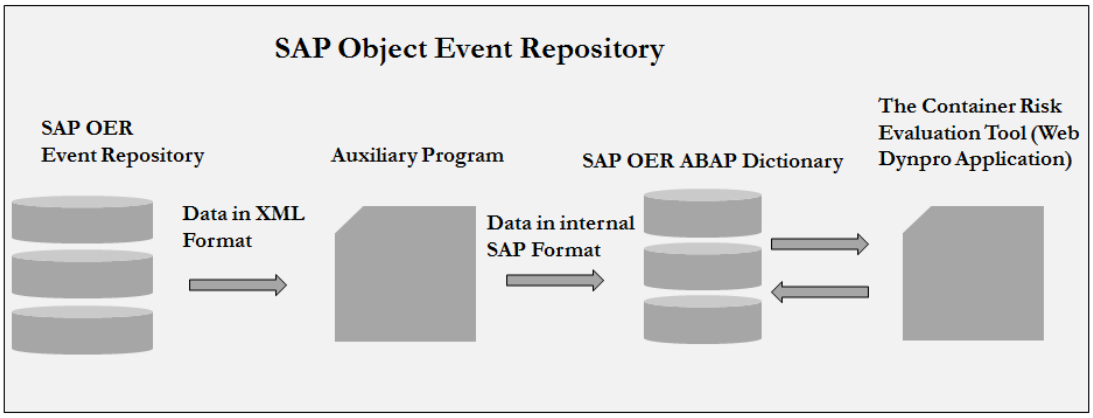

Figure 22 Integration of the Tool with SAP OER

Integration with Collaboration Engine. The integration of the Tool with the Collaboration Engine, described in Chapter 3 "The Concept" is not currently implemented due to the fact that the process of data flow has not been established yet. Integration can be performed with the help of XML format for data exchange between two systems. Another option can be to use IDoc (stands for intermediate document) – a standard data structure for electronic data interchange (EDI) between SAP systems or between SAP application and external programs. The IDoc data format is similar to XML in purpose but differs in syntax.

Integration with AEO/C-TPAT databases. Integration with the Collaboration Engine can theoretically provide the Container Risk Evaluation Tool with information if a supply chain actor is certified or not. But the verification mechanism has not been established yet, as the way how to get access to the database of AEO/C-TPAT certified companies and automatically verify data is not clear at the present moment. On the official web site of European Commission **(7)** it is possible to validate an Authorized Economic Operators by entering the full holder name. But it is not clear yet how this database can be integrated into the ECSIT infrastructure. Accesses to the database of C-TPAT certified companies is granted only to C-TPAT holders and can be accessed on the Customs-Trade Partnership Against Terrorism Security Link Portal **(46)**.

Integration with Scanning Component. The integration with the scanning component of the ECSIT infrastructure is also not implemented as it is not known at the present moment under which circumstances the customs authorities will request

scan images i.e. if they need to get scan image of every scanned container or only under special request.

Chapter 5

Evaluation

5.1 Possible scenarios

Three scenarios have been selected to test and evaluate the process for container risk evaluation as well as the tool developed within this work.
Each scenario refers to a possible business case of cargo transportation from Germany to the USA. The aim is of course not to cover all the possible activities in the transport process and risk evaluation, but rather to map different relevant situations where the Container Risk Evaluation Process can be put into practice.

5.1.1 Scenario A: Deviation from the planed route and unauthorized seal opening

The objective of this use-case is to demonstrate the Container Risk Evaluation process in the situation where the container has changed its planned route and a seal was opened without authorization during the transportation. The case can be illustrative for scenarios involving terrorism and smuggling of prohibited goods. Terrorist organizations may be involved in cross-border cargo flows for many reasons: they can embed into the cargo destructive objects and materials, for example an explosive device, or they can use international supply chain to deliver materials, equipment and people across borders in order to prepare and carry out their malicious operations.

A-1 Business scenario. The scenario involves an international supply chain of cargo from the German city of Stuttgart to an American marine port in Charleston via the port of Bremerhaven in Germany. A risk of the sea container is evaluated by customs authorities with help of the Container Risk Evaluation Tool when the container is at the last foreign port before it is loaded onto a vessel destined for the United States.

A-2 Automatic capturing of data. According to the process flow, described in Chapter 3 "The Concept", automatic data capturing begin during the transportation of the container. When the first element of data is fed into the system, a case is created automatically by the system. The term "Case" is borrowed from the terminology of SAP Investigative Case Management system, described in Chapter 2 "Background Information and Related Work". In the Container Risk Evaluation Tool a "Case" corresponds to a container whose risk is evaluated. The data capturing continues until the moment when the container has arrived at the last foreign port before loading onto a vessel to the USA. During data capture the system checks obtained data for compliance and against criteria detailing prohibited cargo, terrorist organizations, and economic and political embargoes.

In the figure below one can see a case created in the Container Risk Evaluation system with the ID number `urn:epc:id:grai:1234567.00006.236489227188` and the status "Waiting for information", as well as four risk categories corresponding to that case. These categories present information about the cargo in a structured way: in every category the information is gathered according to the risk aspect which is evaluated separately in the system, but the overall picture of the situation can be derived only after thorough analysis of all categories together. These categories are: Cargo Details, Cargo Route, Scan Result and Seal Log. The categories are described more detail in Chapter 3 "The Concept". The fifth category "Documents" contains additionally requested shipping documents that can be useful for risk assessment, such as Bill of Lading or Sales Order.

While capturing data the system does not evaluate the risk of the categories, so it is seen in the figure below that all categories are blue colored meaning that the risk is not evaluated yet. It is also seen that the case has appeared on the "Waiting for information" tab of the cases table and the overall risk of the container is not evaluated (it is colored in a yellow color). While the case is on the "Waiting for information" tab the customs officer does not need to do anything with it. It is assumed that the customs officer does not check this case until it appears on the "Action needed" tab of the table.

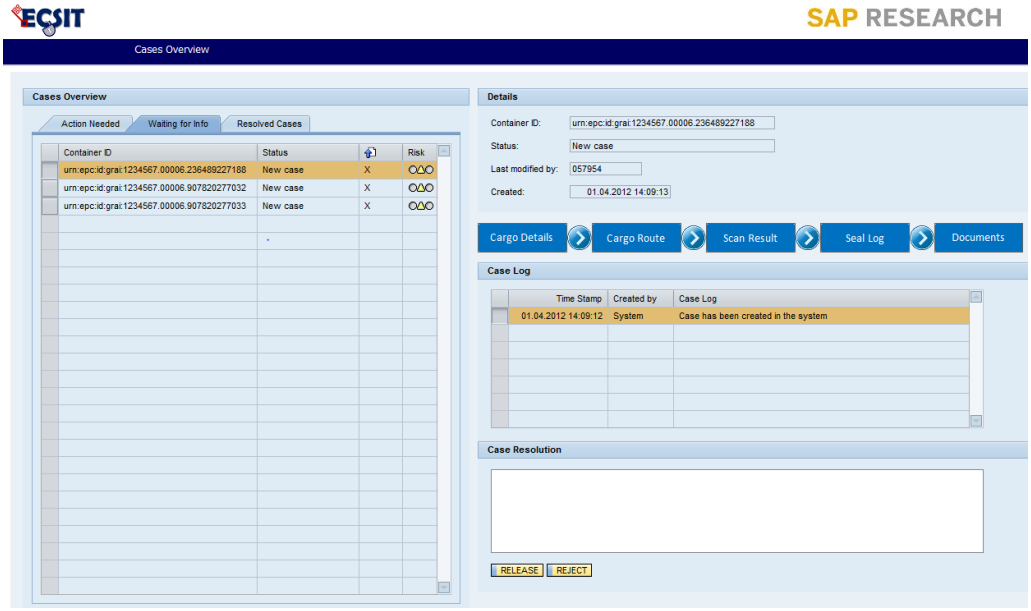

Figure 23 Initial view of the application

A-2.1 Evaluation of the concept. The weakest part of the concept is the extent to which data from sources of information as described in the previous chapter is sufficient for risk evaluation of the container. Customs authorities are not willing to provide any information about the process of risk evaluation they currently use. The main reason for this is the potential security threat that revealing this information can cause. We can only assume that the information described in Chapter 3 "The Concept" is sufficient enough to make the decision on the necessity of scanning the container as well as on releasing the container into the country, with only one correction that it is impossible to be 100% sure about the content of the container in question. Because of this issue I suggest in my concept to scan as a sample a certain percentage of the containers which originally were supposed to be released without any detailed inspection (Green Lane containers, described in section 5.1.3 of this chapter).

A-2.2 Evaluation of the prototype. The automatic capturing of data from the Cargo Details risk category is not currently implemented in the prototype. A certain part of that data can be fed into the system after integration with the Logistic Collaboration Hub, a platform for cooperation between all supply chain actors, developed within the

ECSIT project. The integration is planned for the near future and described in greater details in Chapter 4 "Description of the Container Risk Evaluation Tool" and Chapter 6 "Summary and Future Work".

The current implementation of the prototype also does not support automatic integration with the infrastructure of electronic seals and sensors on the container. This integration is planned and described in the next chapter.

Data about the route of the container is obtained through SAP Object Event Repository. This part of the functionality is fully implemented in the prototype and described in Chapter 4 "Description of the Container Risk Evaluation Tool".

A-3 Automatic analysis of the incidents. As mentioned in Chapter 3 "The Concept", in order to avoid undesirable congestion of containers in front of the entrance to the harbor the decision about container scanning should be ready to be made by the time the container arrives at the harbor. In the figure below it is seen that after initial automatic evaluation of the potential risk several categories are colored in red, which means that, based on the provided information, some incidents during the container transportation were detected and the risk of the container is estimated as high. In the described situation the container is automatically sent for x-ray scanning and radioactivity analysis while entering the harbor.

The incidents detected by the system in the given scenario are:

- Absence of AEO status/C-TPAT certification or any compliant status, and invalid address of Buyer and Ship-To party – data related to the Cargo Details category;
- Deviation from the planned route – data related to the Cargo Route category;
- Unauthorized opening of the container – data related to the Seal Log category.

A-3.1 Evaluation of the concept. It is not clear yet if the absence of the AEO status or C-TPAT certification of one of the participants of the supply chain should be considered as an incident and has to lead to the obligatory scanning of the container. It is also not clear how the system should react in the case of the misspelling of the name or address of one of the participants of the supply chain. In the worst case scenario if

the misspelling is the only incident detected by the system the container will still be sent for obligatory scanning while entering the port and that can lead to unnecessary overload in the work of the marine ports.

A-3.2 Evaluation of the prototype. The automatic analysis of incidents is not fully implemented yet, partly due to the fact that not all data is fed into the system automatically.

Significantly, it has not been finally decided how the cargo route should be evaluated. At the current moment it is assumed in the system that a planned route should be automatically obtained by the system before the transportation of the container. It is assumed that the system should compare the planned route with the events obtained from the SAP Object Event Repository. Although events are automatically fed into the system (this part is implemented in the prototype), the algorithm for matching this data is currently not implemented because of the absence of information about the format in which the real cargo route can be obtained.

A-4 Manual check of the scan image and all incidents. When the scan image and information about the container radioactivity have been obtained, the case appears on the "Action needed" tab and Scan Result category color becomes yellow. The yellow color of the category means that the risk of that category cannot be automatically evaluated and a manual check is needed. In Case Log Table it is possible to check the reason why the case has appeared on the "Action needed" tab - the scan image of the container is available. Moreover the status of the case now is "Scan is available". The status and case log help the customs officer who is assigned to the case quickly understand what action is needed from him or her.

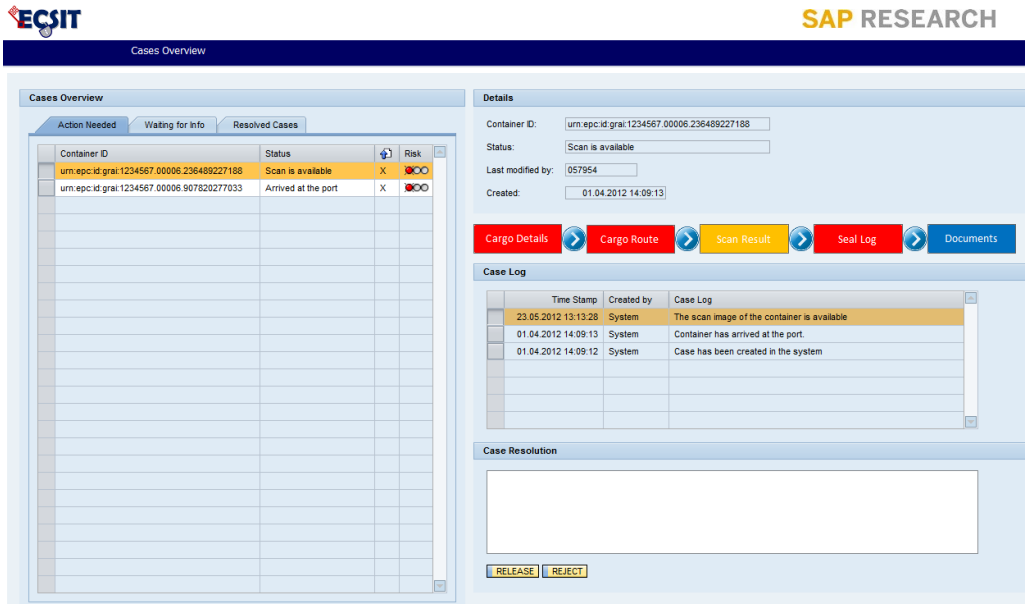

Figure 24 Initial view after automatic risk evaluation

From that moment the customs officer can begin the manual risk evaluation process. In the prototype it is assumed that cases are assigned automatically to the first employee who is available at the time when the information from a detailed inspection of the container is available – an employee cannot choose which case is assigned to them. It is implemented in this way in order to avoid possible subjectivity in the decision.

The sequence of actions for risk evaluation process depends on the customs employee. In general the employee should check step by step all incidents that were detected by the system and compare scan image or manual check results with cargo description from the cargo manifest. If the employee requests additional information (for example the container should be sent for additional manual check or for scanning for nuclear materials), the case appears again on the tab "Waiting for information" with the corresponding status and relevant risk category highlighted in a yellow color.

In the given scenario the employee has decided to check the Cargo Details category first. In the figure below one can see the Cargo Details view of the application and all detected incidents corresponding to that risk category.

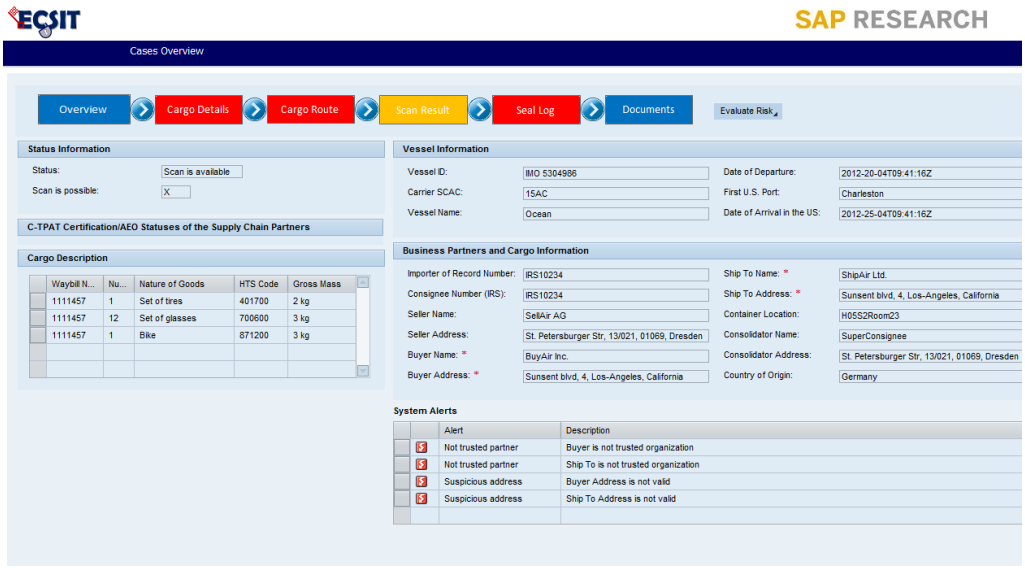

Figure 25 Cargo Details view

It is easily noticeable that the system has detected that neither the Buyer nor Ship-To party has C-TPAT certification, AEO or equivalent compliance status. The absence of C-TPAT certification/AEO status does not show yet that the container poses a high risk but it must be analyzed together with other incidents. The system has also detected that the addresses of Buyer and Ship-To party are not valid. After checking for misspelling the employee is convinced that both the Buyer and Ship-To party either do not exist in reality or have some problems with documents. After analysis of cargo details the employee marks that category as category with high risk which is seen in the figure below. The mark helps the customs officer to understand that this category has been already manually checked and there is no need to come back to it.

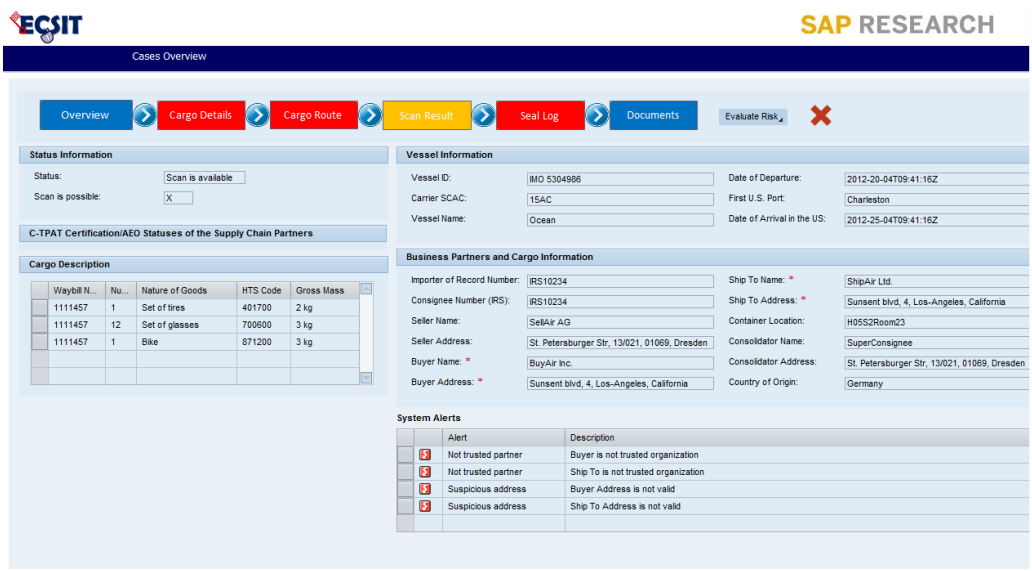

Figure 26 Cargo Details view - already checked

After Cargo Details the employee decides to check cargo route. It is seen from figure 31 that according to the scenario a deviation from the planned route of the container has been detected. Moreover in Munich it is detected that the seal was opened and replaced with a seal of a lower standard. The seal log is possible to check also in the Seal Log Category (figure 32).

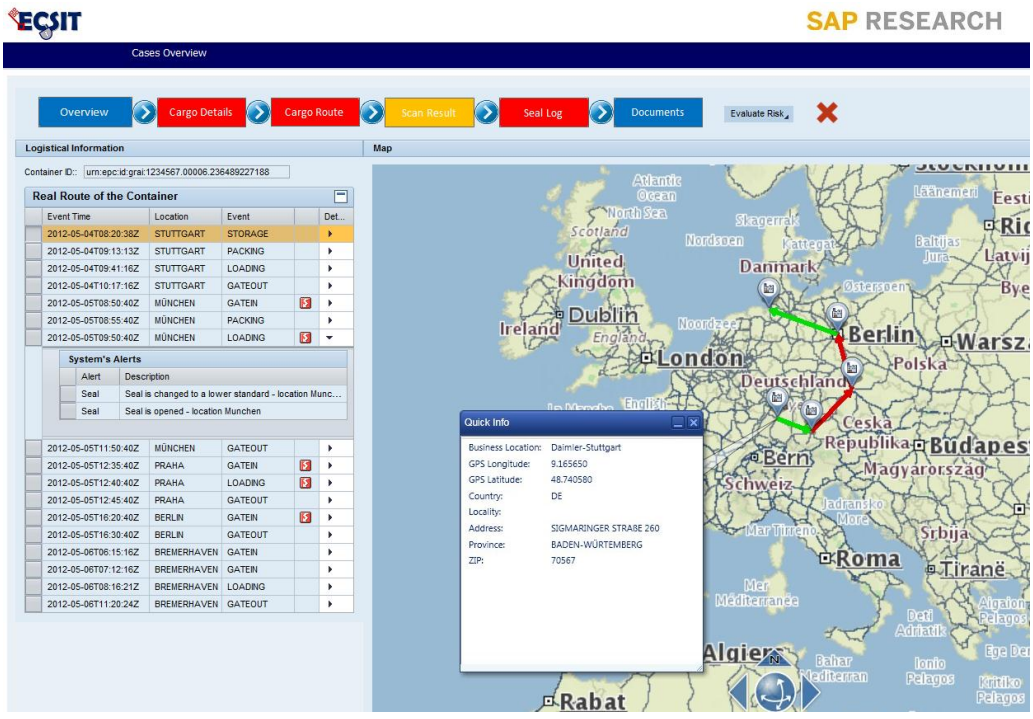

Figure 27 Cargo Route view

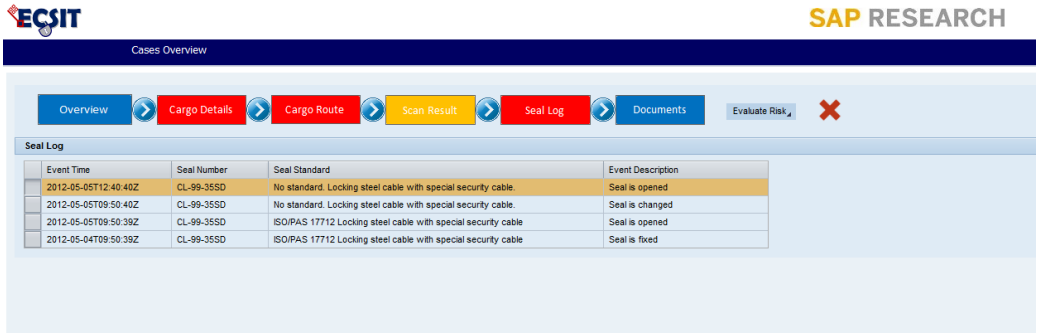

Figure 28 Seal Log view

It is important to manually check the scan image obtained and the results from the radioactivity analysis. This information is presented in the Scan Result category. As it is seen from the figure below, although the container is supposed to contain only tires, glasses and a bike, according to the Cargo Description, scanning has shown that cargo is radioactive.

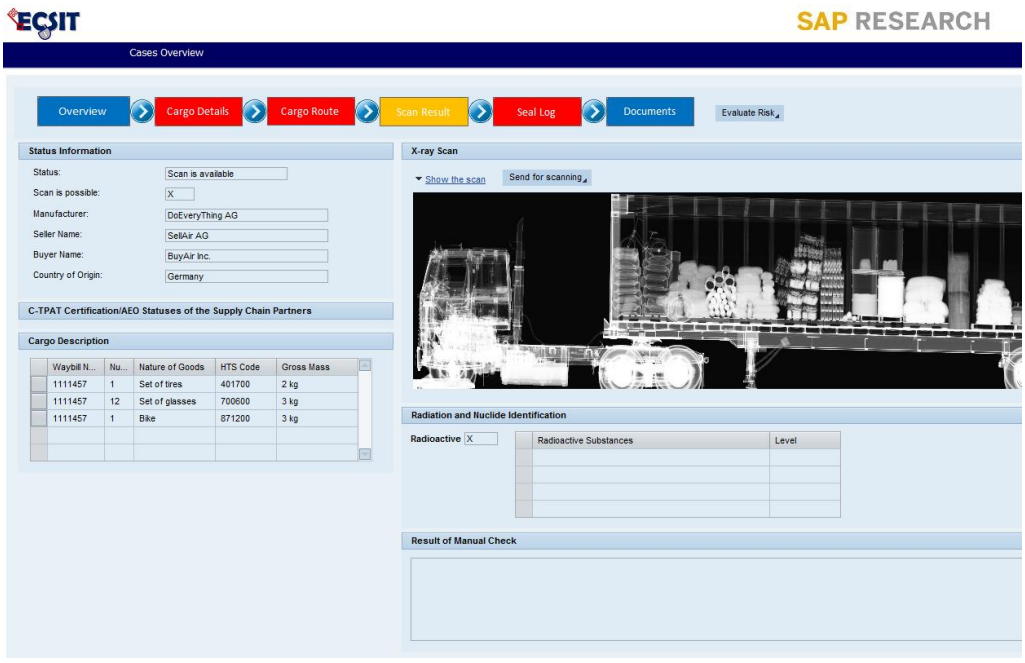

Figure 29 Scan Result view

All incidents detected by the system indicate the high risk of the container. The employee can send the container for additional scanning for nuclear identification and wait for results or immediately mark the Scan Result category as checked and reject the container.

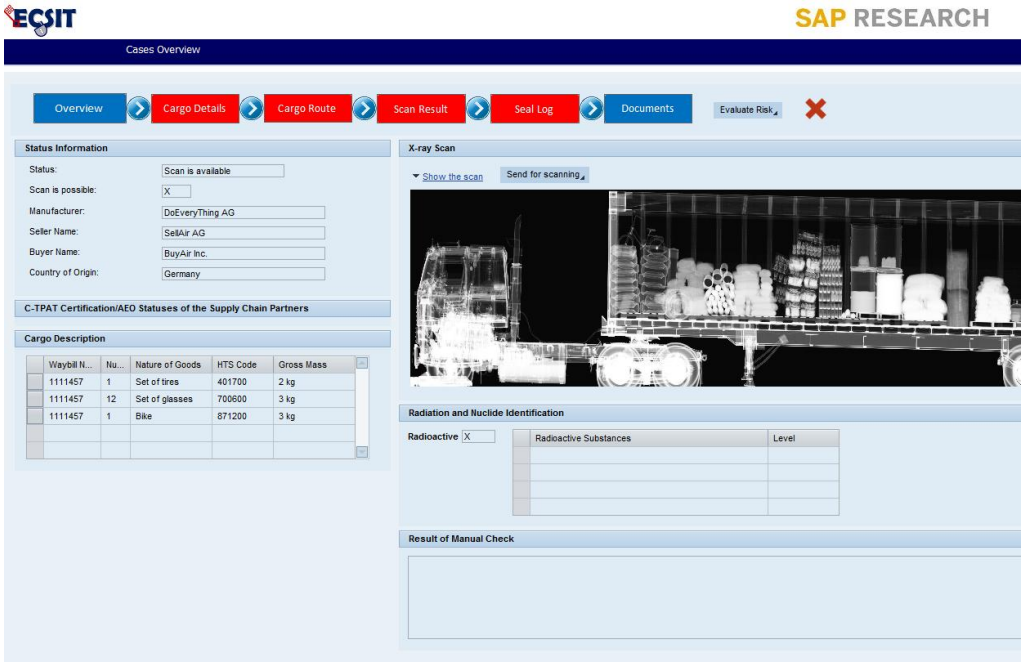

Figure 30 The Scan Result category is checked

If the container is rejected the corresponding case appears in the "Resolved Cases" tab with the status "Rejected", as seen in the figure below.

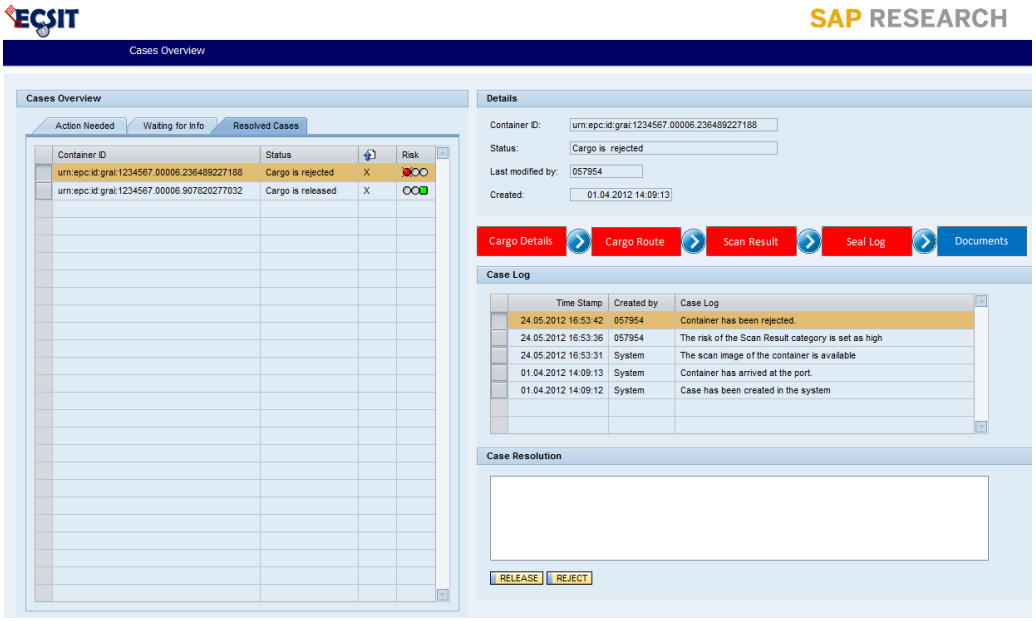

Figure 31 Container is rejected

A-4.1 Evaluation of the concept. In the described scenario certain information about the cargo (such as the address of the buyer, the absence of AEO/C-TPAT statuses, etc.) indicated that the container should be scanned. These indicators can be different. The research on customs risk management conducted by the CASSANDRA project (**(41), (44)**) provided 14 illustrative examples on what might be considered as "high risk indicators" by customs administrations, based on information obtained from the supply chain participants. These examples are presented in Chapter 3 "The Concept".

As it is seen from the scenario, a lot of information can be derived from the data provided by the system. In the given scenario the discrepancy between the scan result with Cargo Description together with information about deviation from the planned route and unauthorized seal opening during the transportation is critical as it shows the possibility of smuggling of radioactive dangerous substances that can be used for a radiological weapon. This example shows very clearly how additional logistical data can help with the evaluation process.

A-4.2 Evaluation of the prototype. The example described in this section has shown how easily the prototype allows the matching of various kinds of information provided to the customs authorities by different sources. For example it is easier to evaluate the content of the container, comparing cargo description from the cargo manifest with the scan image if this information is grouped together and displayed on the same view, as it is implemented in the Scan Result view. The same applies to matching seal log data with the cargo route, which is presented in the same view (the Cargo Route category).

In the above described scenario the case has different statuses during its lifetime. A status changes after certain actions are conducted automatically by the system or manually by the customs employee. The status flow is depicted in the figure below. The color of each status in the figure corresponds to the color of one of the risk categories which influenced on status change. The color coding of case statuses help custom officers to understand at a glance the current state of the case.

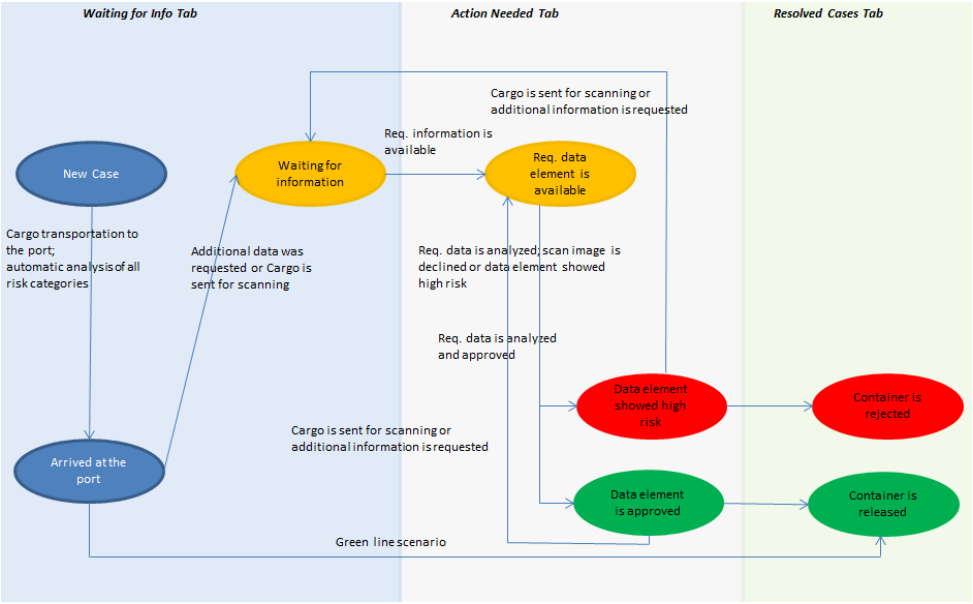

Figure 32 Status Flow

5.1.2 Scenario B: Not Trusted Party

The objective of this scenario is to demonstrate that not all incidents automatically detected by the system lead to the cargo being rejected. As the concept developed within the project introduces the Green Lane scenario (illustrated in section 5.3 "Scenario C: Green lane") which allows the release of the cargo without any detailed inspection, we need to be sure as much as possible that the cargo does not pose any risk. It is assumed in the concept that it is better to scan more containers than miss one with a high risk.

B-1 Business scenario. As in the previous scenario the container is transported from Stuttgart to the American marine port in Charleston. Both containers from each scenario are supposed to be loaded onto the same vessel.

The case described in this scenario has an ID number `urn:epc:id:grai:1234567.00006.907820277033`. Actions which are similar to those discussed in the previous section are not repeated in this section.

B-2 Automatic capturing of data. Automatic data capturing takes place in the same manner as for the previous case, described in 5.1.1/A-2 section. For this container the customs authorities need the same data elements as they required for the previous case, because according to the scenario both containers are transported from Germany to the USA on the same vessel and on the same date.

B-3 Automatic analysis of the incidents. Automatic analysis of the incidents for this case is also very similar to the analysis of the case described above. As in the previous case the container is sent for scanning because an incident is detected by the system.

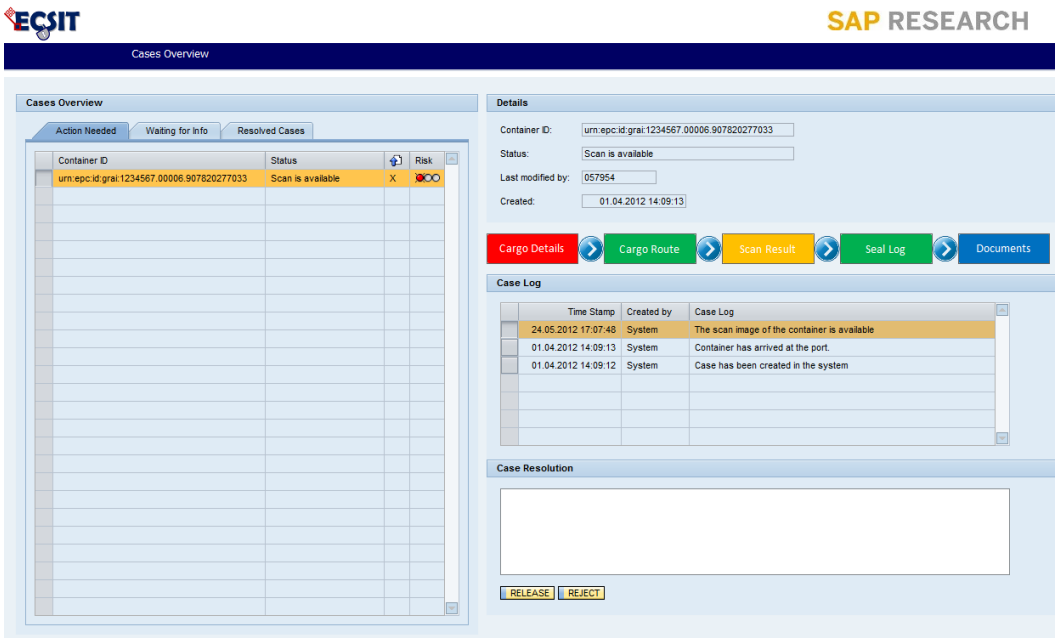

Figure 33 Initial View

B-4 Manual check of the scan image and all incidents. As in the previous example the customs employee decides to check the incidents in the Cargo Details category. It is seen from the figure below that according to the scenario the only incident that has been detected by the system is the fact that the Seller is not a trusted party, i.e. the Seller is not C-TPAT certified/ does not have AEO status.

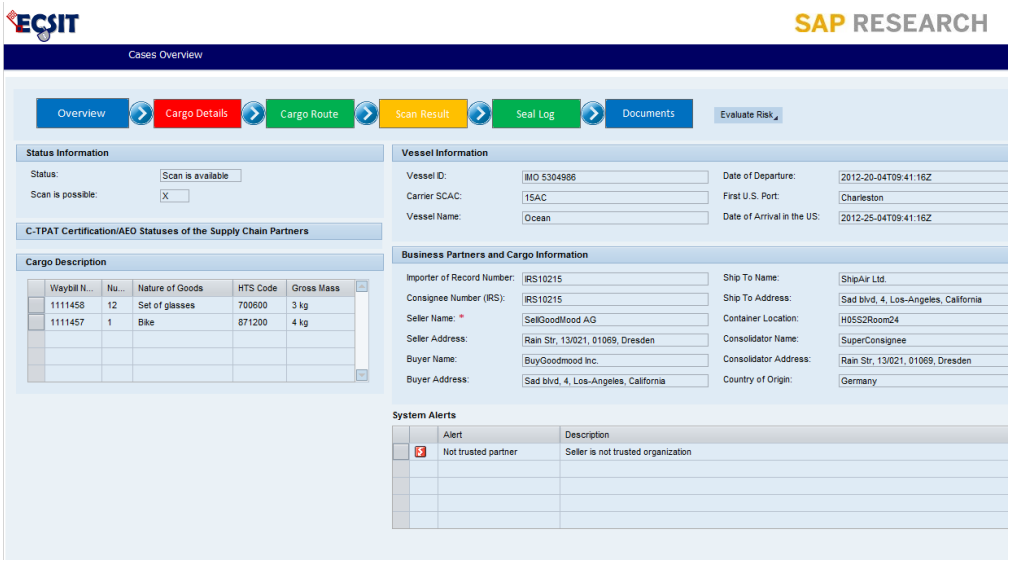

Figure 34 Cargo Details View

After the Cargo Details category the employee checks the scan image of the container together with the cargo description. As it is seen from the figure below, the cargo description matches with the scan image and no radiation has been detected during the scanning. Keeping in mind that all other categories do not show any alerts the employee decides to release the container although one of the participants of the supply chain is not a trusted party.

B-4.1 Evaluation of the concept. This example has shown that not all alerts lead to the rejection of the cargo when attempting to enter the USA. As it is mentioned previously, it is assumed in the concept that it is better to scan more containers than miss one with a high risk.

Another possible alert could be for example container seal opening during the transportation as a result of an unscheduled but authorized check. The Seal Log in this case still records the opening of the container; the system automatically detects it as an incident and will send the container for scanning.

B-4.2 Evaluation of the prototype. As in the previous example, the prototype has shown that evaluating the container risk is easier when all relevant information is collected and displayed together in corresponding categories. For example, for the Scan

Result category one can match the cargo description provided by the Cargo Manifest with scan image and ensure that everything that is listed in the description is displayed by the image and identify anything that is not listed.

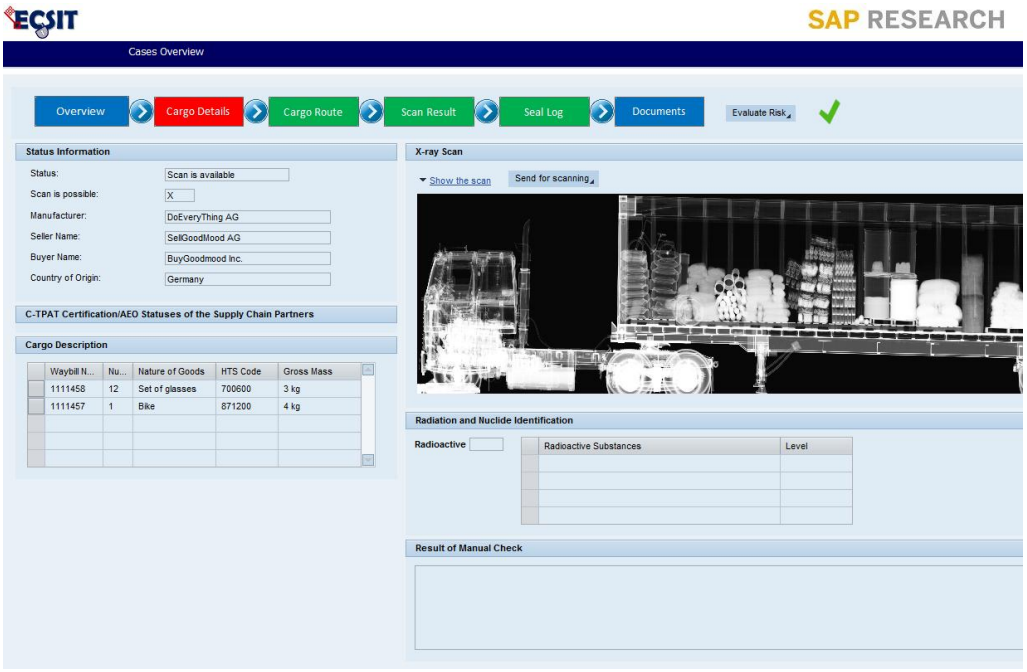

Figure 35 Scan Image of the container is checked

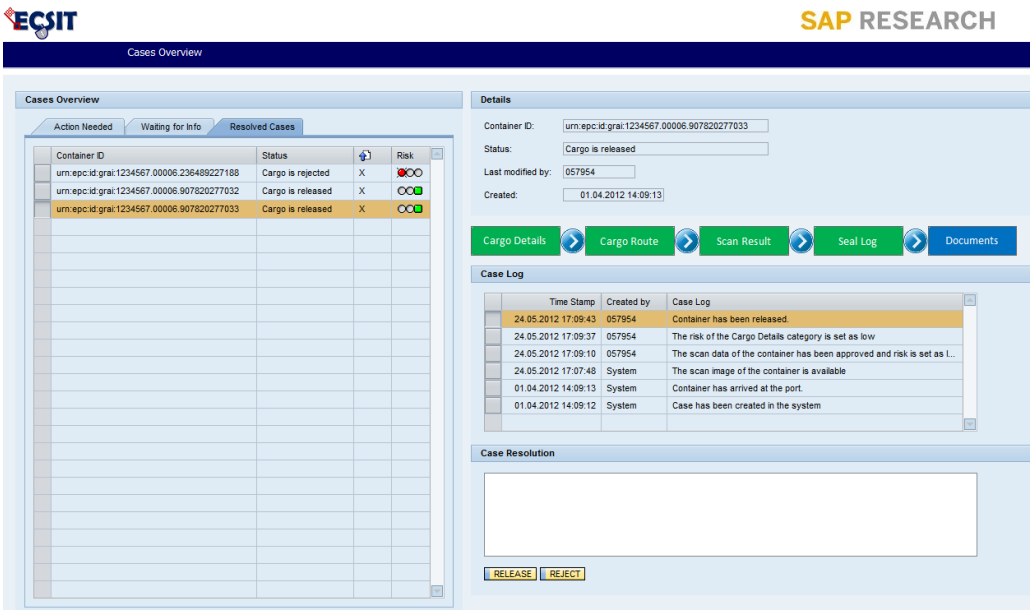

Figure 36 Container is Released

5.1.3 Scenario C: Green Lane

The next case illustrates a possible Green Lane scenario where the container is released without any detailed inspection at the port before loading onto the vessel bound for the USA.

C-1 Business scenario. As in the previous scenario the container is transported from Stuttgart to the American marine port in Charleston. The case corresponding to the container has the ID number `urn:epc:id:grai:1234567.00006.907820277032`. It is seen from the figure below that like in all previous scenarios case is created automatically when the first data element is captured by the system.

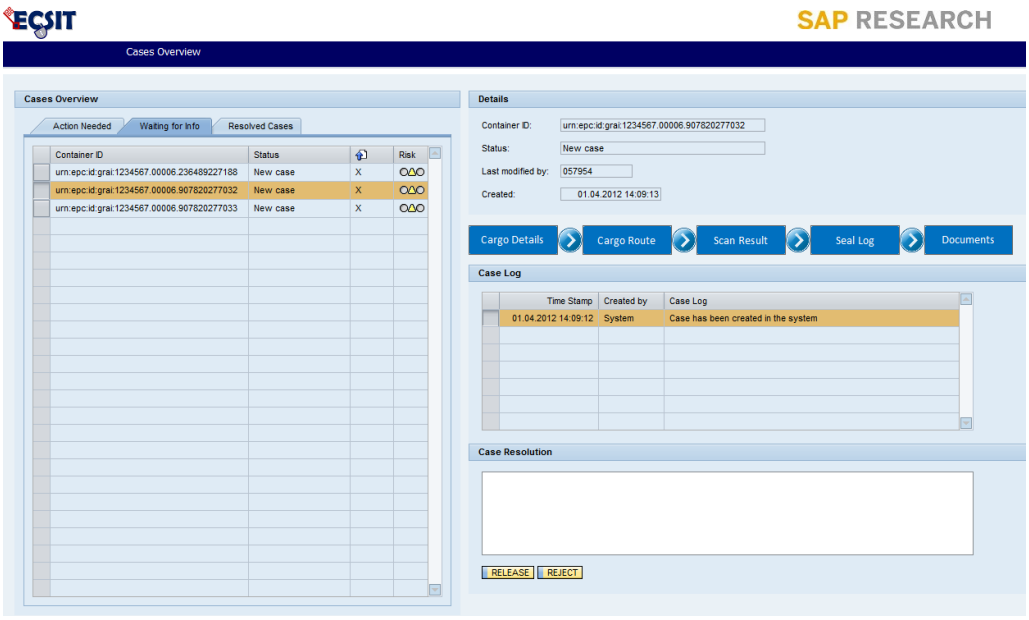

Figure 37 Case is created in the system

C-2 Automatic capturing of data. Automatic data capturing is the same as for all cases described above because according to the scenario all containers are transported from Germany to the USA on the same vessel and on the same date.

C-3 Automatic analysis of the incidents. The algorithm for the automatic analysis of incidents is the same as one described for the previous cases. The only difference is in

the outcome of the analysis: in this example no incidents are detected by the system and the container can enter the port without any additional inspection.

C-4 Manual check of the scan image and all incidents. As the objective of the Green Lane scenario is the automatic release of the cargo without a manual check and further detailed inspection the customs officer does not work with this case in the system: when the case is created it appears on the "Waiting for information" tab, it is assumed that when the container arrives at the port the system analysis the risk automatically, and since according to the scenario no incidents are detected (all participants of the supply chain are AEO authorized/ C-TPAT certified companies, the seal was not opened during the transportation of the container, the route deviation was not detected, etc.), the container is released and appears on the "Resolved Cases" tab with status "released", as it is seen from the figure below:

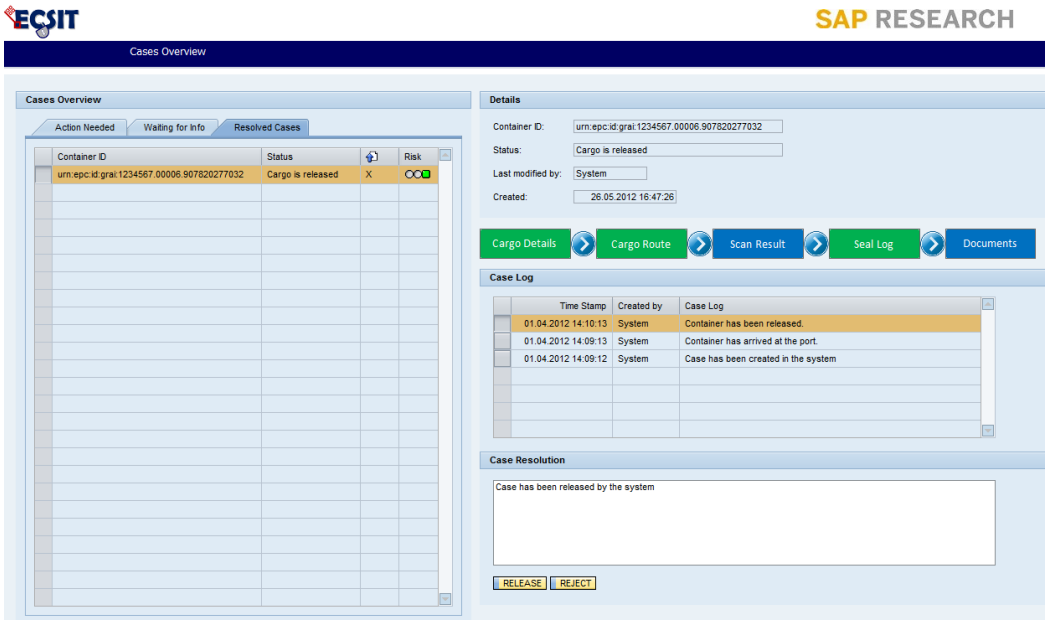

Figure 38 Container is released - green lane scenario

B-4.1 Evaluation of the concept. As it is mentioned before, even if all requested information is provided to the customs authorities they cannot be fully certain about the content of the container. That is why it is worth to scan as a sample a certain percentage of the containers which originally were supposed to be released without any detailed inspection.

B-4.2 Evaluation of the prototype. Currently, the functionality of automatically setting a certain percentage of green lane containers for additional detailed inspection as a parameter in the system in order to ensure the security and the integrity of the process is not implemented in the prototype. Random additional checks can be established in the system e.g. every 10^{th} green lane container is sent for x-ray scanning and radioactivity analysis.

5.2 Discussion

The Container Risk Evaluation Tool is a prototype of the application for risk evaluation of the containers bound for the USA and EU. It is apparent that the prototype does not have a certain part of the functionality implemented yet as it is not the final application, but it allows evaluation of the concept and serves as a good base for further discussions. The scenarios described above together with the concept were demonstrated during the knowledge sharing section to the partner project CASSANDRA. According to the feedback from the CASSANDRA project, the concept developed within the Master's Thesis project might be a good alternative to the "100% scanning law". The Container Evaluation Tool needs further development, especially performance tuning, and further integration with the ECSIT infrastructure. This additional work is described in greater detail in the next chapter.

A harsher criticism might be that the application is implemented in the SAP system and thereby, very dependent on the SAP environment. But as it is described above in Chapter 4 "Description of the Container Risk Evaluation Tool", the reason for the choice of SAP environment is the fact that it allows easy integration with SAP Object Event Repository, systems of the majority of European and American supply chain actors, and systems in use by customs authorities.

The concept suggested in the Master's Thesis also needs further clarification, especially in regards to the Green Lane scenario. Special laws or regulations need to be defined under which containers can legitimately avoid detailed inspection at the port before entering the country. Although at present this topic is of interest, a legislation base has

not yet been developed to enable the Green Lane scenario. All other weak parts of the concept are described in the previous section of this chapter.

Another problem that arises and which is not covered by the concept developed within the Master's Thesis project is the problem of possible industry espionage if supply chain partners reveal additional security related information. To solve the problem it should be decided exactly which information can be revealed to the customs authorities. One option can be to analyze all data in a neutral platform, for example in the Logistic Collaboration Hub described in Chapter 3 "The Concept", and then send the analysis outcome to the Container Risk Evaluation Tool which is hosted by the customs authorities. For example, the alert that the seal was opened does not contain any risk of industry espionage but only security relevant information which can be used to evaluate the risk of the container. In this case the neutral platform should be certified and recognized by the customs authorities.

The problem of industry espionage is not a focus of this thesis, but it is definitely warrants future research as without clear definition of how to protect security related information the concept of the container risk evaluation loses its practical sense.

The concept is not in its final form yet - it should go through a long period of evolution before being implemented in real life.

Chapter 6

Summary and Future Work

In this Master's Thesis report I have presented a concept for container security evaluation. The concept can be an alternative to the "100% scanning law" as it reduces the need for a container scan but enhances security through additional evaluation of logistical data of the container.

I have introduced a semi-automatic evaluation approach and a first prototype supporting the evaluation of security relevant container and supply chain data.

The prototype for the Container Risk Evaluation Tool, developed within the project

- reduces the need for container scanning and introduces a possible green lane scenario
- enhances security through additional security related information
- supports customs/border personnel during evaluation of container security risks

During the next stage of the project I plan to enhance and optimize the first version of the prototype.

The current implementation of the application does not have integration with the Logistic Collaboration Hub which is planned to be implemented in near future. The integration is needed as almost all data from Cargo Details category should be fed into the system from the Logistic Collaboration Hub, a platform for cooperation of all supply chain actors.

Another step in the development of the prototype is its integration with seal and sensor data from the ContainIT project, a partner research project in the scope of the secure supply chain management system. In the ContainIT project, goods are monitored with sensors along the supply chain in order to check any regulation violation during transportation, storage or manipulation. The ContainIT infrastructure of container security devices and sensors are planned to be used in the ECSIT project. Consequently,

data from the CSDs and sensors will be integrated into the Container Risk Evaluation Tool.

Performance tuning and further UI development is also a part of the future work. The prototype needs optimization for a larger number of cases in the system; the number of calls to the database should be limited and all required information should be held in memory in the form of internal tables - an ABAP structure that provides means of taking data from a fixed structure (tables of database) and storing it in working memory in ABAP.

As a result of the work accomplished during the Master's Thesis project, the current work forms a solid foundation for further development in the scope of secure supply chain management and supports a truly efficient risk evaluation process.

Appendix A

List of Acronyms

ABI	Automated Broker Interface
ACL	Agent Communication Language
AI	Artificial Intelligence
AIS	Automatic Identification System
CSD	Container Security Device
EPC	Electronic Product Code
EPCIS	EPC Information Services
ERP	Enterprise Resource Planning system
EU	European Union
FIPA	The Foundation for Intelligent Physical Agents
FP7	European Union Framework Program 7
CBP	Customs and Border Protection
EDI	Electronic Data Interchange
GDSN	Global Data Synchronization Network
GPS	Global Positioning System
ICT	Information and Communication Technologies
MIS	Management Information System

ONS	Object Name Service
RFID	Radio Frequency Identification
SCAC	Standard Carrier Alpha Code
SICIS	Shared Intermodal Container Information System
SOA	Service Oriented Architecture
TREC	Tamper Resistant Embedded Controller
WCO	World Customs Organization
WTO	World Trade Organization

Appendix B

Definition of Terms

Term	**Definition**
ABI	Automated Broker Interface - a component of the U.S. Customs Service's Automated Commercial System that permits qualified participants to electronically file required import data with Customs. Currently, over 96% of all entries filed with Customs are filed through ABI **(13)**.
SCAC	or Standard Carrier Alpha Code, a two-to-four letter identification, is used by the United States to identify freight carriers in computer systems and shipping documents such as Bill of Lading, Freight Bill and etc.
EPC	or Electronic Product Code, is a universal identifier for unique identification of physical objects. EPC is created and described by EPCglobal Tag Data Standard which can be freely downloaded in (20).
EPCglobal	is an organization created by cooperation between GS1 and GS1 US that works towards the worldwide adoption and standardization of Electronic Product Code (EPC) technology.
EPCIS	or Electronic Product Code Information Services, is a standard, developed by EPCglobal, which describes interfaces, discovery services, and security mechanisms for the capturing and querying Electronic Product Code (EPC) related data. In order to allow competition among IT providers the standard does not specify the possible implementation of the service operations or

databases.

FIPA or the Foundation for Intelligent Physical Agents, is an international organization which promotes technologies and interoperability specifications for physical agents. More information can be found in official web page of the organization in (21).

GDSN or GS1 Global Data Synchronization Network, is a network which connects trading partners to the GS1 Global Registry® via a network of interoperable GDSN-certified data pools.

GS1 is an international not-for-profit association founded in 1977 which is dedicated to the development and implementation of global standards and solutions to improve the efficiency and visibility of supply chains. Nowadays, the system of standards, developed by this association, is the most widely-used. The official web site of the organization is http://www.gs1.org/.

Intrastat certain information, which a company in European Union is obliged to declare if it trades goods with other members of European Union. The type of information depends on whether the value of Arrivals (purchases or imports) or Dispatches (sales or exports) exceeds the annual Intrastat exemption threshold/s. **(47)**.

ITAR or International Traffic in Arms Regulations – is a set of United States government regulations that controls the export and import of defense-related articles and services on the United States Munitions List **(48)**.

Ontology is a formal description of the concepts and relationships for enabling knowledge sharing and reuse. More formal definition can be found in (22): "Ontology is a formal specification of a

	shared conceptualization".
ONS	or Object Name Service, transforms the Electronic Product Code (EPC) into URLs.
REACH	Registration, Evaluation, Authorization, and Restriction of Chemicals (REACH), is European Union Regulation of December 18, 2006 which came into effect on June 1, 2007 (Regulation (EC) no 1907/2006). The regulation is about the production and use of chemical substances, and their potential impacts on human health and environment.
SAP Web Application Server (SAP Web AS)	an application server from SAP. It serves as the underlying infrastructure for all SAP solutions and supports both J2EE and ABAP. Basically all SAP applications run on top of the SAP Web AS. A non-SAP application that is based on J2EE could also run on the SAP Web AS.
Sanctioned Party List (SPL)	a list containing persons and companies with whom trade is prohibited by law
TREC	or Tamper Resistant Embedded Controller, is developed by IBM's Zurich Research Lab wireless container security device, which can track movements of the container to which it is attached and make this information available to authorized entities; it also can collect data about physical location of the container, its state (temperature, humidity, door status and others).

References

1. The White House. *National Strategy for Global Supply Chain Security. [Online] http://www.whitehouse.gov/sites/default/files/national_strategy_for_global_supply_chain_security.pdf.*

2. *H.R. 1. Implementing Recommendations of the 9/11 Commission Act* of 2007. [Online] [Cited: April 2, 2012.] http://www.govtrack.us/congress/bills/110/hr1.

3. CBP. U.S. Customs Container Security Initiative Guards America, Global Commerce From Terrorist Threat. *CBP.gov: Securing America's Borders.* [Online] [Cited: April 22, 2012] . http://www.cbp.gov/xp/cgov/newsroom/news_releases/archives/legacy/2002/112002/11012002_4.xml.

4. The White House. *The Act of 110th Congress of the United States of 4th of January, 2007.*

5. Thomas, Andrew R. *Supply Chain Security: International Practices and Innovations in Moving Goods Safely and Efficiently.* s.l. : Greenwood Publishing Group, 2010. 80-81.

6. European Commission. *Secure Trade and 100% Scanning of Containers.* Brussels : Commission Staff Working Document, 2010.

7. European Commission . Taxation and Customs Union. *Economic Operator Systems.* [Online] [Cited: April 18, 2012.] http://ec.europa.eu/taxation_customs/dds2/eos/eos_home.jsp?Lang=en .

8. European Commission. Article 5(a) of Council Regulation (EEC) No 2913/92 of 12 October 1992. 1992, 1992R2913.

9. European Commission. Commision Regulation (EC) No 1192/2008 of 17 November 2008. 2008.

10. Aigner S. *Mutual Recognition of Authorised Economic Operators and Security Measures.* World Customs Journal V4 No1. [Online] [Cited: April 30, 2012.] http://www.worldcustomsjournal.org/media/wcj/-2010/1/Aigner.pdf.

11. Supply Chain Security International, Inc. C-TPAT. [Online] 2012. [Cited: April 18, 2012.] http://www.c-tpat.com/.

12. CBP. C-TPAT: Customs-Trade Partnership Against Terrorism. *CBP.gov: Securing America's Borders.* [Online] [Cited: April 18, 2012.] http://www.cbp.gov/xp/cgov/trade/cargo_security/ctpat/.

13. CBP. Automated Broker Interface (ABI) and Contact Information. *CBP.gov Securing America's Borders.* [Online] [Cited: April 18, 2012.] http://www.cbp.gov/xp/cgov/trade/automated/automated_systems/acs/acs_abi_contact_info.xml.

14. IMO: International Maritime Organization. *International Convention for the Safety of Life at Sea (SOLAS).* [Online] 2011. [Cited: April 18, 2012.] http://www.imo.org/About/Conventions/ListOfConventions/Pages/International-Convention-for-the-Safety-of-Life-at-Sea-(SOLAS),-1974.aspx.

15. MSC Intersessional Working Group. The Diplomatic Conference on Maritime Security. *ISPS Code, Part A, 3.1.* London : s.n., 2002.

16. SMART-CM. *Container Security and Tracking Devices - Technical Specification and Communication Standards.* Brussels : The European Committee for Standardization Workshop on Container Security & Tracking Devices, 2011.

17. SMART-CM. *The SMART-CM Official Web Page.* [Online] [Cited: March 14, 2012.] http://www.smart-cm.eu/.

18. SMART-CM. *Container Security & Tracking Devices—Technical Specifications and Communication Standards.* Brussels : The European Committee for Standardization Workshop on Container Security & Tracking Devices., 2011.

19. INTEGRITY. The INTEGRITY Official Web Page. [Online] [Cited: March 14, 2012.] http://www.integrity-supplychain.eu/.

20. LogisticsForLife. Deliverable 1.2b *"Best Practice Cases".* 2011. 1.0-30.10.2011

21. Dolivo, F. *The IBM Secure Trade Lane Solution*. ERCIM NEWS . [Online] [Cited: March 14, 2012.] http://ercim-news.ercim.eu/the-ibm-secure-trade-lane-solution.

22. EPCGlobal. *EPC Information Services (EPCIS) Specification.* 2007. 1.0.1.

23. Baida Z., Rukanova B., Koldijk F., Tan Y.-H., Vogel T., Schmidt A., Sassen E., Ulankiewicz S., Liu J., Pengel M., Modder H., Flügge B., Kräussl Z. *Beer Living Lab - Final report.* 2008. D5.1:5.

24. ITAIDE. The ITAIDE Official Web Page. *Beer LL Demonstrator.* [Online] [Cited: March 15, 2012.] http://www.ve-forum.org/apps/pub.asp?Q=2306.

25. Paganelli P., Charalampos V., Cornelisse E., Damentka A., Forcolin M., Jermol M., Styczynski R., Szczurek W., Vedovato D. *The EURIDICE Peoject* - White Paper. 2009.

26. Hribernik K. A., Hans C., Thoben K.-D. *The Application of the EPCglobal Framework Architecture to Autonomous Controlled Logistics.* Bremen : Dynamics in logistics - second international conference, 2011.

27. Uronen K., Hintsa J. *CASSANDRA - The Project Deliverable No. D1.1.* 2012.

28. Di Re S., Rowland C., Paschalidou C., George T., Madsen E., Tyrinopoulos Y. *Freightwise Newsletter.* 2010.

29. E-Freight. Capabilities for Co-Modal Transport. *The E-Freight Official Web Page.* [Online] [Cited: March 15, 2012.] http://www.efreightproject.eu/.

30. Vayou M., Katsoulakos T. *The e-Freight Concept Supporting Alignment of EU Policy, Business and IT in Freight Transport and Logistics.* Pedersen, 2011. 1.3.

31. Katsoulakos T., Yannis Z., Doukas Charalampos, Maria L., Maglogiannis I. *Reference Solutions for Next Generation National Single Windows.* 2011.

32. Nils Meyer-Larsen, Frank Arendt. *CHINOS: Container Handling in Intermodal Nodes – Optimal and Secure!* Final Report. 2009.

33. SAP AG. SAP Global Trade Services. *Help Portal.* [Online] [Cited: March 16, 2012.] http://help.sap.com/saphelp_crm70/helpdata/EN/ea/de4a96904e40b6b7d9b1e9caf5b645/frameset.htm.

34. SAP AG. *How to Deploy SAP Solutions for Governance, Risk, and Compliance,* 2011.

35. SAP AG *Sap Solution in Detail. Enabling a Secure and Reliable International Supply Chain,* 2011.

36. SAP AG. SAP Launches Investigative Case Management Software to Help Police Solves Crimes. [Online] [Cited: March 20, 2012.] http://www.sap.com/corporateen/press/newsroom/press.epx?PressID=10901

37. SAP AG. *SAP Investigative Case Management Documentation*. Help Portal. [Online]http://help.sap.com/saphelp_crm70/helpdata/EN/ea/de4a96904e40b6b7d9b1e9caf5b645/frameset.htm.

38. SAP AG *SAP® Solutions for Auto-ID and Item Serialization.* 2009.

39. SAP AG. SAP Help Portal. *SAP Event Management.* [Online] [Cited: June 6, 2012.] http://help.sap.com/eventmanagement.

40. World Port Source. Port of Bremerhaven. [Online] [Cited: May 1, 2012.] http://www.worldportsource.com/ports/DEU_Port_of_Bremerhaven_2764.php.

41. Hintsa J., Männistö T., Urciuoli L., Ahokas J. Customs *Perspectives on Detection of Deliberate Regulatory Violations in Global Supply Chains - the Role of Information and Data in Risk Identification*. 2011, Vol. Version 2.0.

42. European Commission. *Annex 30A of Commission Regulation 1875/2006* .

43. Wikipedia. [Online] [Cited: May 09, 2012.] http://wikimediafoundation.org/wiki/Terms_of_Use%20(2012)/en?utm_source=TOU_top_TestClone2.

44. Hintsa, J., Männistö, T., Hameri A.P., Thibedeau C., Sahlstedt, J., Tsikolenko, V., Finger M., Granqvist M. *Customs risk management (CRiM): A Survey of 24 WCO Member Administrations*. Lausanne, Switzerland : Cross-border Research Association, EPFL & HEC UNIL, 2011.

45. SAP AG. SAP Help Portal. *SAP NetWeaver*. [Online] [Cited: June 6, 2012.] http://help.sap.com/netweaver.

46. CBP C-TPAT. C-TPAT Login. *Customs-Trade Partnership Against Terrorism Security Link Portal* . [Online] [Cited: June 8, 2012.] https://ctpat.cbp.dhs.gov/login.aspx?ReturnUrl=/Home.aspx.

47. Business Link. *Business Link. Information. Support. Compliance.* [Online] [Cited: March16,2012.] http://www.businesslink.gov.uk/bdotg/action/layer?topicId=1078096454.

48. The Office of the Federal Register National Archives and Records Administration. *Code of Federal Regulations*. Tittle 22 , Washington : U.S. Government Printing Office. Foreign Relations., 1999.

49. Berry, J. *The Logistics Action Plan and the Commission's Current Research on Freight Logistics*. Brussels : eFreight Conference, 2009.

50. Eveline van Stijn, Phuaphanthong T., Kerotho S., Pikart M., Hofman W., Tan Y.-H. *Single Window Implementation Framework*. Geneva : s.n., 2010. D5.0:4b.

51. Fjørtoft K. E., Hans W., Marit K. Natvig, Pedersen J. T. *FREIGHTWISE Framework Architecture, release 1*. 2007. D13.2-WP13.

52. EPC Tag Data Standard (TDS). [Online] [Cited: March 15, 2012.] http://www.gs1.org/gsmp/kc/epcglobal/tds.

53. FIPA. The Foundation for Intelligent Physical Agents. [Online] http://www.fipa.org/.

54. Gruber, T. R. *A Translation Approach to Portable Ontology Specifications.* s.l. : Knowledge Acquisition, 1993. 199-220.

55. Karl A. Hribernik, Hans C. *The Application of the EPCglobal Framework Architecture to Autonomous Controlled Logistics.*