ERASMUS UNIVERSITEIT ROTTERDAM

PROTECT

Transumo

Information needs, requirements and recommendations for Supply Chain Security

PROTECT Work Package 5.1

Master’s thesis Economics & ICT

Date: November 10, 2008

Version: Final

Author: Nawid Popal (276467)

Contributions: Dutch Tax and Customs Administration
Erasmus University Rotterdam
Delft University of Technology
Port infolink
Port of Rotterdam Authority
TNO

Supervisors: Dr. Ir. J. van den Berg (Erasmus University Rotterdam/Delft University of Technology)
Drs. Marcel van Oosterhout (RSM Erasmus University Rotterdam)

Co-reader: Dr. F. Frasincar (Erasmus University Rotterdam)

Acknowledgements

This Master's thesis is a result of my seven months of internship at the Rotterdam School of Management (RSM) at the Erasmus University Rotterdam where I had a very pleasant time to work on the research with a lot of very interesting people. The research presented in this thesis is part of a research project called PROTECT. In this project, many organizations cooperate which are doing research in the field of supply chain security.

First, I would like to specially thank my coach Dr. Ir. Jan van den Berg from Erasmus University Rotterdam, who is now working at TU Delft and who was also the person who introduced me to the PROTECT project. Thanks a lot for your support, patient and coaching during the entire research period and after that during the writing of this thesis. I could absolutely not have reached this quality without your input on research methodology and direction. I want to thank you for your participation in the experts brainstorm sessions and for your comments on research findings which are presented in this thesis.

Second, I would like to thank my other coach Drs. Marcel van Oosterhout from RSM Erasmus University Rotterdam. Thank you for your always useful and important feedback and input on the research and contents of my thesis. It would have absolutely not been possible to write this thesis in this quality without your advice and coaching about the contents of the thesis. Also thank you for the planning and execution of the experts brainstorm sessions.

I want to specially thank MSc. Mark Meijer for his close cooperation not only at the beginning but also during the entire period of this research. Thank you for the very pleasant teamwork and for execution of the interviews and many hours of collaboration at RSM and TNO. I wish you a lot of good luck and success in your life and career.

I also want to thank the many people from the PROTECT project that were involved in the two weekly experts brainstorm sessions at RSM Erasmus University Rotterdam. I want to thank Iwan van der Wolf from Port infolink for his participation and useful insight in the area of information exchange, information needs and information availability in container transport. Also many thanks to Jurjen Duintjer from port authorities (Havenbedrijf Rotterdam), Bauke Padding from Dutch customs, Thierry Verduijn and his successor Sandra Krupe from TNO for their involvement in PROTECT and their contributions to the experts brainstorm sessions. I would also like to thank Dr. F. Frasincar for his willingness to be the co-readership for this thesis.

Not to forget, I would like to thank the supply chain companies and other institutions that were so kind to make time for us to conduct interviews with them for the purpose of this research and of course also for their participation at the validation workshop.

I cannot end without thanking my family, on whose constant encouragement and love I have relied throughout my entire study. I am grateful for the support and encouragement of all my family members and friends and in particular my eldest brother Ahmad Shah Popal who has been as a rolemodel for me throughout my entire study.

Management summary

Organizations active in the supply chain for container transport are more and more concerned about threats affecting supply chain operations. Both supply chain companies and regulatory authorities take security measurers to decrease the threat of terrorist attacks, smuggling and theft. For these security measures, the organizations have information requirements in order to take adequate actions. The goal is to improve the security of the supply chain through identifying the information needs and requirements and through better information exchange between the actors in the supply chain.

The drive for supply chain security is caused by rules and regulations of the regulatory authorities and by the business value of the security measures. Awareness about supply chain security causes companies to adopt security measures to achieve a competitive advantage. Security measures and associated information exchanges are more acceptable if business value is present. Some threats however cannot be countered by individual supply chain companies. Security measures to counter these threats have to be enforced by the regulatory authorities. To stimulate these companies, they can be offered incentives like logistic advantages and shorter lead-times. Identifying the information which is needed and required to apply and execute the supply chain measures, is a very essential part of the job.

The focus of this research is on the information needs, requirements and recommendations for the supply chain security. The main objectives of this thesis is to explore and identify the information which is needed to be exchanged among the supply chain organizations in order to improve the level of supply chain security. To identify, as much as possible, a complete overview of the information needs, desk research and field research is conducted. During the desk research a simplified version of the complete supply chain process is designed and the weakest links are identified. During the field research an extensive number of supply chain organizations are interviewed and the processes within their organizations are analysed. Also the progress of the research is periodically discussed during the expert sessions where representatives from supply chain organizations, supply chain experts, Dutch customs and experts from the Erasmus University of Rotterdam (RMS) were present.

As a result, a very large number of information is identified as being important and even essential to be exchanged efficiently among the supply chain organizations to help improve the level of supply chain security. It has become clear that a lot of the identified information already exist in different information systems which are used by different supply chain organizations, but not exchanged efficiently.

To mention the requirements related to the identified information needs, the importance of the security of the information itself is extensively discussed. The importance of the confidentiality, integrity and availability (CIA) of the information frequently mentioned and applied. The confidentiality, integrity and availability of the security related information is at risk when the ways in which this information is exchanged, are not well defined.

Index

1 Introduction

This chapter introduces the research, which is presented in this thesis. It describes the context and background of the research followed by its objectives. Thereafter, the scope of the research is defined. After that, the methodology used is described. This chapter ends with a brief outline/reading guide of this thesis.

1.1 Context/Background

In this thesis the supply chain security (SCS) of container transport is addressed. The logistic process of transporting containers is vulnerable and deserves attention in order to improve the security in the supply chain (SC). Because 90% of world's trade is conducted by using container transport [Barnes, P. & Oloruntoba, R. (2005)], a disruption of the system may have a significant impact on the world economy. Protecting the SC against threats that could cause these disruptions is therefore necessary. Making efforts to protect the SC against threats like terrorist attacks, smuggling and theft is the main interest of this thesis.

The research presented in this thesis concerns the first part of the work package 5 (WP 5) of the PROTECT project. The main purpose of this work package is to define and analyze the information needs, information requirements, information availability and information interchange between the parties that are directly or indirectly involved in the SC in order to create and maintain a more secure SC.

Participants in the PROTECT project are the Erasmus University Rotterdam, TNO, het havenbedrijf Rotterdam NV (Port of Rotterdam), Buck Consultants International, Dutch Customs, EVO, NDL, TLN, DNV and TU/Delft (Delft University of Technology). A full list of abbreviations is presented in appendix F.

The results from the first part of WP 5 have been used as input for the second part of the WP 5, work package 5.2 (WP 5.2).

Figure 1 offers a graphical representation of WP 5 and the scope of both sub work packages.

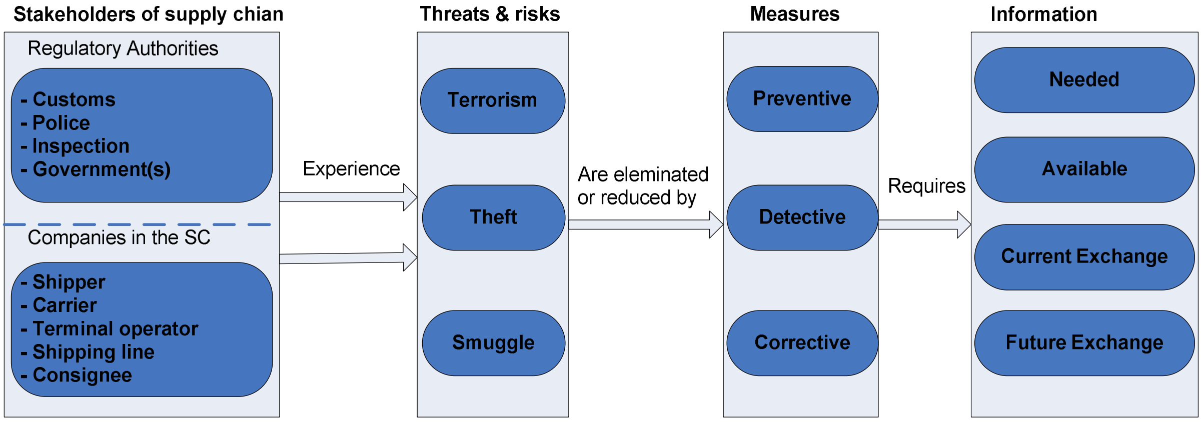


Figure 1: Graphic representation of work package 5.1

The research conducted and represented in this thesis is part of a larger project called PROTECT (http://protect.transumo.nl). PROTECT is a Transumo project. The aim of PROTECT is the development of repayable SCs. This project aims to determine what the decisive factors that can secure the international SC of companies are. To achieve this, this project not only uses the substantial knowledge of SCs and structures but also the knowledge that is gained during the development and implementation of the measures to make the corporate processes more secure and repayable.

1.2 Research objective

The SC consist of a complex mix of physical and non-physical (logistic) processes which are proceeding each other and/or are going parallel with each other. As described in the previous paragraph, the supply chain is of a high importance for the global economy and global security. This means that SC deserves a lot of attention on the field of security and securing the processes.

The research represented in this thesis has objectives that fit within the research objective of the overall work package. The main problem of the Protect work packages can be described as follows [http://protect.transumo.nl]:

How can the security of the supply chain for container transport be improved by sharing security relevant information by the actors of that supply chain?

This research objective is not directly addressed in this thesis but clarifies the general goal to which the outcomes of the research, presented in this thesis, will contribute. Different elements of the research objective deserve extra attention. First, in this research objective the assumption is made that better information sharing can improve the security of the SC. Secondly; by the actors in the SC all organizations that are directly or indirectly involved in the process of container transport are meant. Finally information exchange covers all types of information exchange like personal communication, faxes, telephone calls and different types of digital information exchanges.

The research objective of WP 5.1 can be derived from the overall objective of WP 5. The research objective of WP 5.1 is described as follows:

Which information is needed to improve the supply chain security and how can this information be exchanged among the parties, directly and indirectly, involved in the supply chain?

Definition 1: Research objective work package 5.1

The main objective of WP 5.1 is to describe and analyze the SCS, determine the weak links in the SC and to define the information needs for strengthening those links. In this work package the available information will be gathered and analyzed and also conditions, under which the parties are ready to provide security relevant information, will be briefly described. In order to provide practical and realistic recommendations, this analysis will take the regulating authorities and the requirements from the authorities and the companies in account. The assumption is that this all will eventually contribute to a more secure SC.

In order to be able to achieve the research objective of WP 5.1, the main research objective of WP 5.1 is divided in the following four research questions:

(1) Which security threats and risks do the parties involved in the logistic process, consider important with respect to the security of the SC?

(2) Which security measures can improve the security level of the SC?

(3a) What operational and security relevant information is needed to reduce SCS related risks and make the SC more secure?

(3b) How the can current information exchange among the SC parties be characterized and which factors hinder or stimulate the adoption of security relevant information sharing?

(4) What is the gap between the current information availability and the desired information availability with regards to SCS and what are recommendations to bridge this gap?

Definition 2: Research questions work package 5.1

The first research question identifies the most common and important threats and risks that are experienced by the parties involved the SC. The second research question is a follow up on the first research question. It defines security measures which could decrease or eliminate the threats and risks that are mentioned in the previous research question. The focus of the third (3a) research question is on determining the information that is needed to prevent a certain threat from happening, to detect a certain threat when it has happened or to correct the damage caused by a certain threat. (3b) It also examines the state of the current information availability and it characterizes the current information sharing among the SC parties and clarifies the facts and condition under which the SC parties will adopt security relevant information sharing. The fourth research question is a follow up of the third research question. It focuses on the difference (gap) between the current information availability and the future (desirable) information availability. It also discusses the possibilities to fill/bridge this gap.

By providing answers to these research questions the main objective of this thesis will be achieved.

1.3 Scope

The focus of analyses in this thesis is on the transport of containers through the port of Rotterdam. In this thesis the focus will be on *what* information can be shared between the different actors in the supply chain in order to fulfil these needs.

The scope of WP 5.1 is depicted in Figure 2. From top to bottom the scope is narrowed leading finally to information needs. The final results from this thesis have been used as input (basis) for work package 5.2.

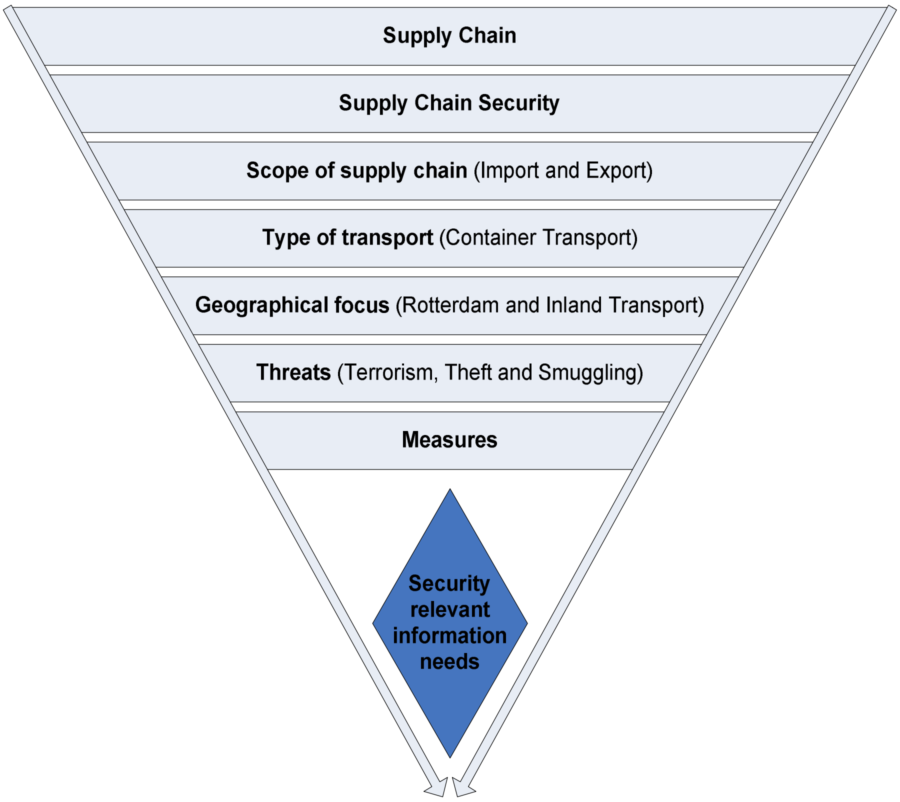

Supply Chain
Supply Chain Security
Scope of supply chain (Import and Export)
Type of transport (Container Transport)
Geographical focus (Rotterdam and Inland Transport)
Threats (Terrorism, Theft and Smuggling)
Measures
Security relevant information needs

Figure 2: Scope of work package 5.1

In order to narrow the scope of this thesis, the financial aspects of the SCS are omitted. The analysis considers a high level description of information needs, availability, readiness to share and possibilities of information exchange between the different parties in the SC.

As stated previously in this chapter, the results from WP 5.1 are used as input for WP 5.2. In work package 5.2, the information exchange between the different actors active in the SC for container transport is used as a basis for analysis. The aim of this work package is to make recommendations for the development of information system architecture (ISA) that the different actors can use to improve SCS [Meijer 2007].

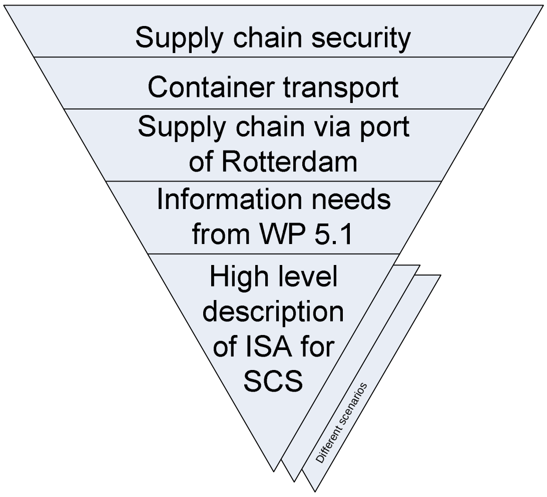

Supply chain security
Container transport
Supply chain via port of Rotterdam
Information needs from WP 5.1
High level description of ISA for SCS
Different scenarios

Figure 3: Scope of work package 5.2 [adopted from Meijer 2007]

The following figure illustrates the work package 5 and shows how it is divided in WP 5.1 and WP 5.2.

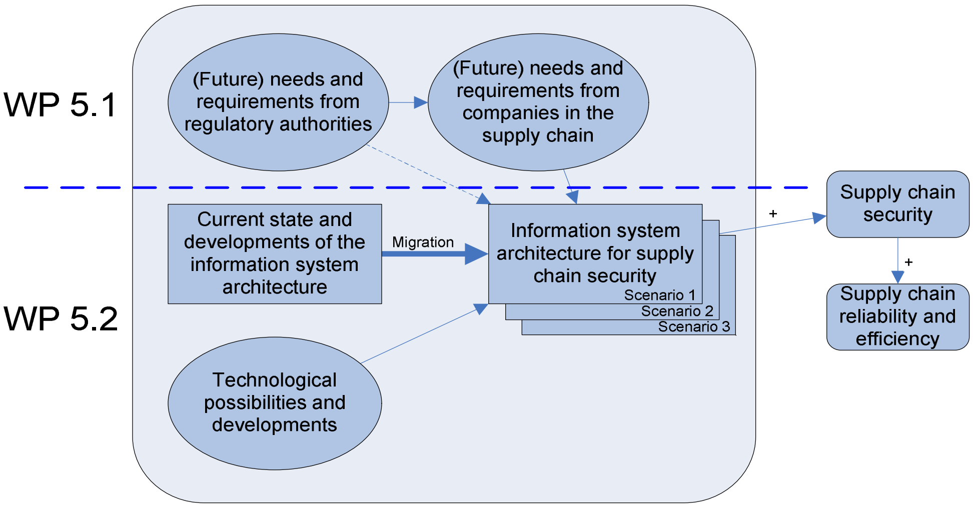

WP 5.1
WP 5.2
(Future) needs and requirements from regulatory authorities
(Future) needs and requirements from companies in the supply chain
Current state and developments of the information system architecture
Migration
Information system architecture for supply chain security
Scenario 1
Scenario 2
Scenario 3
Technological possibilities and developments
+
Supply chain security
+
Supply chain reliability and efficiency

Figure 4: Graphical representation of WP 5 [adopted from Meijer 2007]

1.4 Research methodology

As mentioned in paragraph 1.2, the main objective of this thesis is to present the results of the possibilities for information exchange between the parties – directly and indirectly – involved in the SC to improve SCS and which information is needed to achieve this. The methodology of this research has been as follows:

<u>Part one: literature study (exploratory research)</u>

Exploratory research *is a type of research conducted because a problem has not been clearly defined. Exploratory research helps determine the best research design, data collection method and selection of subjects. Given its fundamental nature, exploratory research often concludes that a perceived problem doesn't actually exist* [http://wikipedia.org].

Based on the literature study and the expert brainstorm sessions – periodical meetings with experts involved in PROTECT – (a complete list of the people involved in the expert sessions is to be found in appendix B) an exploratory research has been conducted where it has became clear what is understood under SC and specifically for container transport. The difference between the import and export processes is described. In order to better visualize this difference, the schemes for the physical flows of the container transport for both processes are developed. The security aspect for the SC is discussed and defined. Also the stakeholders of the SC are mentioned.

Part two: analysis (exploratory research)

Based on the findings from *Part one*, a system (Microsoft Excel sheets) is developed where the SCS threats and risks (terrorism, theft and/or smuggle) are analyzed for both import and export processes. In this system the main SCS threats and risks and also the weakest security related links in the SC have become clear. This is followed by the possible measure(s) (preventive, detective and/or corrective) for each possible SCS threat and risk. For each SCS measure, the required information is described. There is also attention for the current and the future (desired) information availability and the possible gap between them.

Part three: development of the SCS measures adoption model and the conceptual framework (constructive research)

Constructive research *is perhaps the most common computer science research method. This type of approach demands a form of validation that doesn't need to be quite as empirically based as in other types of research like exploratory research. Nevertheless the conclusions have to be objectively argued and defined. This may involve evaluating the "construct" being developed analytically against some predefined criteria or performing some benchmark tests with the prototype. The term "construct" is often used in this context to refer to the new contribution being developed. Construct can be a new theory, algorithm, model, software, or a framework* [http://wikipedia.org].

In this part, the challenges that are to be faced in making the SC parties accept and implement the SCS measures are discussed. This is achieved by conducting desk research, filed research in the form of interviews with the SC parties and during the expert brainstorm sessions. Based on the findings a SCS measures adoption model is developed. This model describes the possibilities for making the SC parties accept and implement the SCS measures (obligatory, voluntarily, etc.). After that a conceptual framework is developed where the effects of the information exchange among the SC parties, implementation of the SCS measures and other changes on the SC for container transport, is described.

Part four: empirical validation gap (constructive research)

The findings from *part two and three* are validated during a validation workshop with attendees from different parties involved in the SC. During the workshop the findings are presented and discussed. This workshop resulted in editing some of the findings and in exploring the possibilities for further research. Part four ends with conclusion and recommendation for further research.

Following figure presents an overview of the research methodology mentioned in this paragraph.

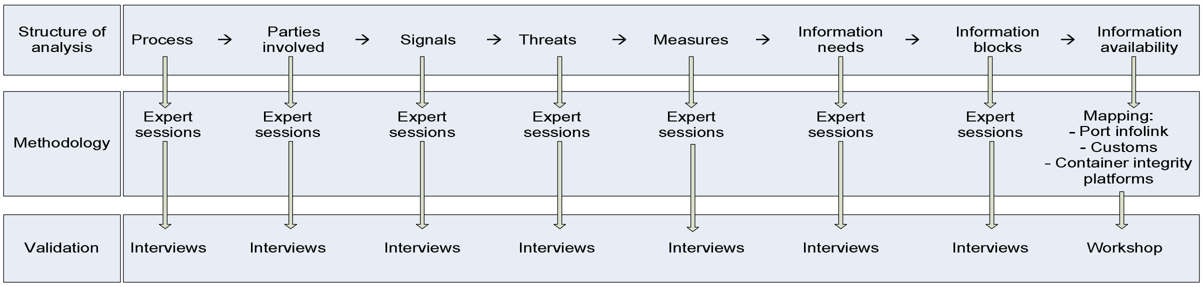


Figure 5: The research methodology of work package 5.1

1.5 Outline/Reading guide

This subsection provides a short outline of the thesis. The contents of each chapter will be shortly described. A graphical representation of the outline is illustrated in Figure 6 (p. 15).

Chapter 2: Supply chain for container transport

In this chapter the container transport will be introduced. A description will be given on what container transport actually is. To visualize the container transport, import and export schemes of the physical processes that are related to the container transport, are drawn. Also the parties that are directly and indirectly involved in the SC are described.

Chapter 3: SCS threats and risks

In this chapter, the possible threats and risks that are related to processes in the SC are analyzed and described. The threats could be terrorism, theft or smuggle.

Chapter 4: Security measures for enhancing the SCS and SC visibility

The possible threats and risks that are mentioned in chapter 3 lead to defining measures. This chapter describes the measures that could be taken in case of a certain threat. The measures can be characterized as preventive, detective, corrective or currently.

Chapter 5: Information needs, availability and exchange for enhancing SCS and visibility

Based on the analysis results from chapter 3 and 4, the information which is needed and the information which is available is defined. Also the gap between the current and future (desirable) information needs will be described.

Chapter 6: Acceptance and implementation challenges

The measures that are defined in chapter 4 and the information needs analyzed and defined in chapter 5 must be used. In chapter 6 the issues and challenges that are to be faced in order to convince the parties in the SC to accept and implement the measures, are discussed. The readiness and conditions under which the parties in the SC are willing to exchange information is discussed.

Chapter 7: Validation

In this chapter, the results from the validation workshop for the research findings are described. This chapter explains briefly the method that is used to present the findings and the comments that are received from the attendees of this workshop.

Chapter 8: Conclusions and recommendations

In this last chapter the main conclusion of the research is presented. Besides this, the opportunities for further research based on the findings in this thesis are identified. Also the recommendations for PROTECT and research limitations are included in this chapter.

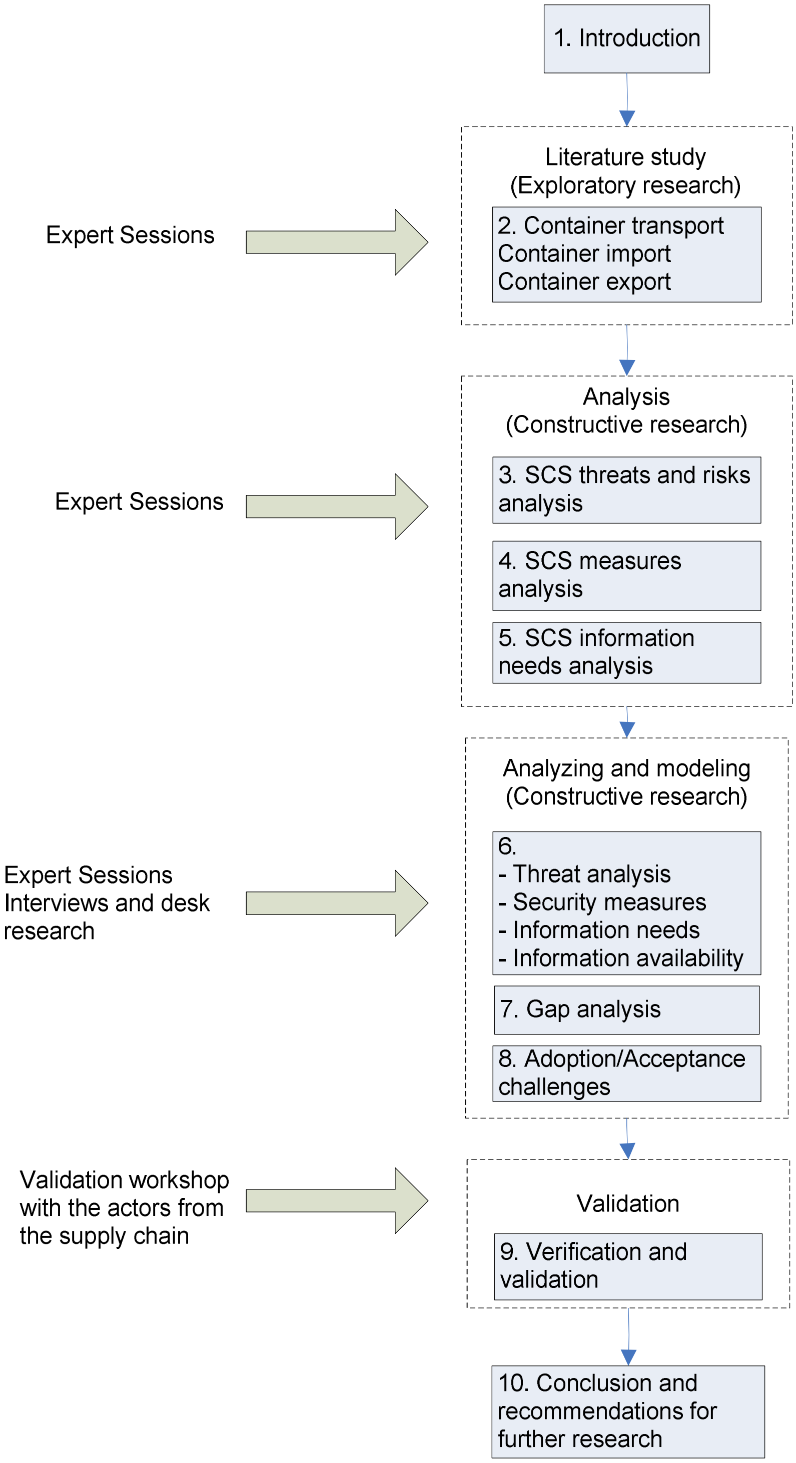


Figure 6: Research approach work package 5.1

2 Supply chain for container transport

This chapter describes the SC in container transport. It clarifies what is meant by SC in container transport. The purpose of this chapter is to provide a clear understanding of the physical processes in container transport, what the corresponding information flow is and which parties are involved in transporting a container from a shipper to a consignee.

This chapter is outlined as follows: section 2.1 explains what the supply chain is and how is it defined for this research. Section 2.2 explains the import part of the SC. It describes the (physical) processes that are involved in import part of the SC. Section 2.3 explains the export part of the SC. It describes the (physical) processes that are involved in export part of the SC. Section 2.4 explains the security issues involved in the SC. It clarifies the term security in relation to SC. And finally section 2.5 introduces the parties that are – directly or indirectly – involved in the SC.

2.1 Supply Chain

2.1.1 Definition

Supply chain is a broad term. When searching for the exact meaning of the SC, a lot of different descriptions are to be found on internet and in the literature. SC is described as "*A supply chain, logistics network, or supply network is a coordinated system of organizations, people, activities, information and resources involved in moving a product or service in physical or virtual manner from supplier to customer. Supply chain activities (also known as value chain or life cycle processes) transform raw material and components into a finished product that is delivered to the end customer. Supply chains link value chains*" [http://en.wikipedia.org/wiki/Supply_chain]

Supply chains are nonlinear dynamic systems, the control of which is complicated by long, variable delays in product and information flows. A SC consists of five basic activities namely; Buy, Make, Move, Store, and Sell [Joshi V. Y. 2000]. These are listed in table 1. The main focus of this thesis is on the third activity namely; the "Move".

Activity	Description
Buy	Choosing suppliers, long term contracts vs. short term deals.
Make	Factory locations, Product lines, Proximity to end customer.
Move	*Setting up transportation network, outsourcing vs. in-house function.*
Store	Distribution network design, warehouse locations.
Sell	Demand forecasting, special promotions.

Table 1: Supply chain activities [Joshi V.Y. 2000]

The SC has been defined by [Christopher M. (2004)] as "*The network of organizations that are involved, through upstream and downstream linkages, in the different processes and activities that produce value in the form of products and services in the hands of the ultimate consumer.*"

Because the focus of this thesis is on the transportation activity (container transport) only, therefore for the purpose of this thesis some changes and clarifications of the (terms used in) above definition is made. First of all "*the organizations that produce value in the form of products and services*" are here all organizations involved in the physical process of transporting a container. This excludes the organizations that are involved in the Buy, Make, Store, and sell activities of a SC. The "*ultimate customers*" are here the sender and receiver (also called shipper and consignee) of the goods transferred in a container.

Hence the definition for SC for container transport is here defined as:

> *The network of organizations that are involved, through upstream and downstream linkages, in the different container transport related processes and activities that produce value in the form of products and services in the hands of the ultimate consumer (shipper or consignee).*

Definition 3: Definition of supply chain (adopted from Christopher M. 2004 and edited)

This definition is visualized in the following figure. It shows the physical flow and the information flow through out the entire SC.

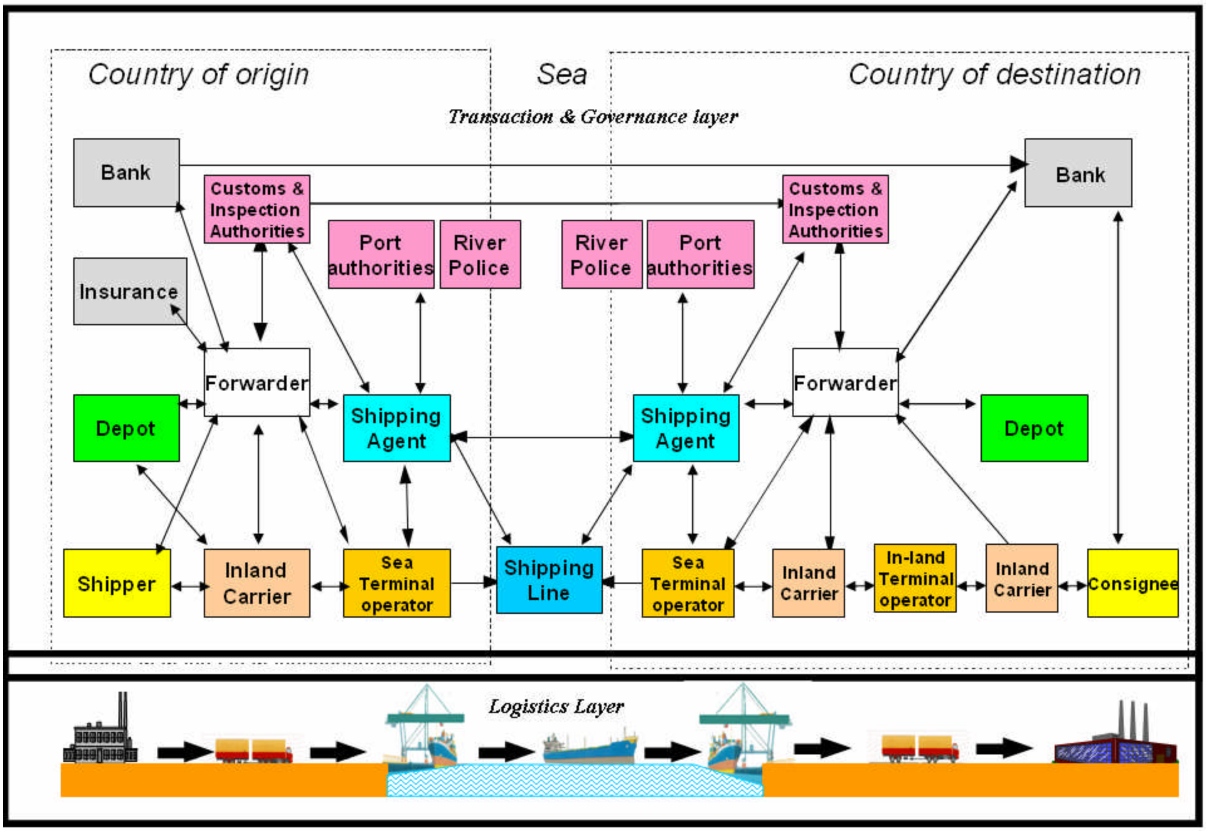


Figure 7: Carriage of goods [Oosterhout M. 2003]

Based on the discussions during the experts brainstorm sessions, the entire SC for container transport as defined here can be separated in two types of processes. The first type is the import process where the containers are sent by container ship from a country other than the Netherlands (foreign country) and transferred to the port of Rotterdam where after the containers will be transported via inland transport to its final destination. This import process is further discussed in paragraph 2.2.

The second type of process is the export process where the container is sent to an offshore country. The containers are brought to the port of Rotterdam via inland transport process. The containers are loaded onto the container ship and shipped to the offshore country port where the containers are unloaded from the container ship and transferred to its final destination trough an inland transport process [Meijer 2007]. This process is further described in paragraph 2.3.

Linking the physical flows of these two types of process creates a cycle where one type of process starts where the other ends. In other words, the physical part of the import process starts where the physical part of the export process ends and other ways around. This process cycle is visualized in figure 8.

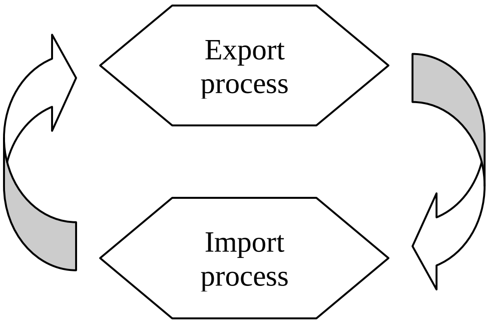


Figure 8: Graphical representation of import – export process cycle

2.2 Import

As mentioned earlier, the import process starts where the export process ends and visa versa. The following scheme shows the focus on the import and the different physical processes that are involved. This scheme has been developed based on the instructions from the expert brainstorm sessions and literature research. The scheme is also validated during the field research.

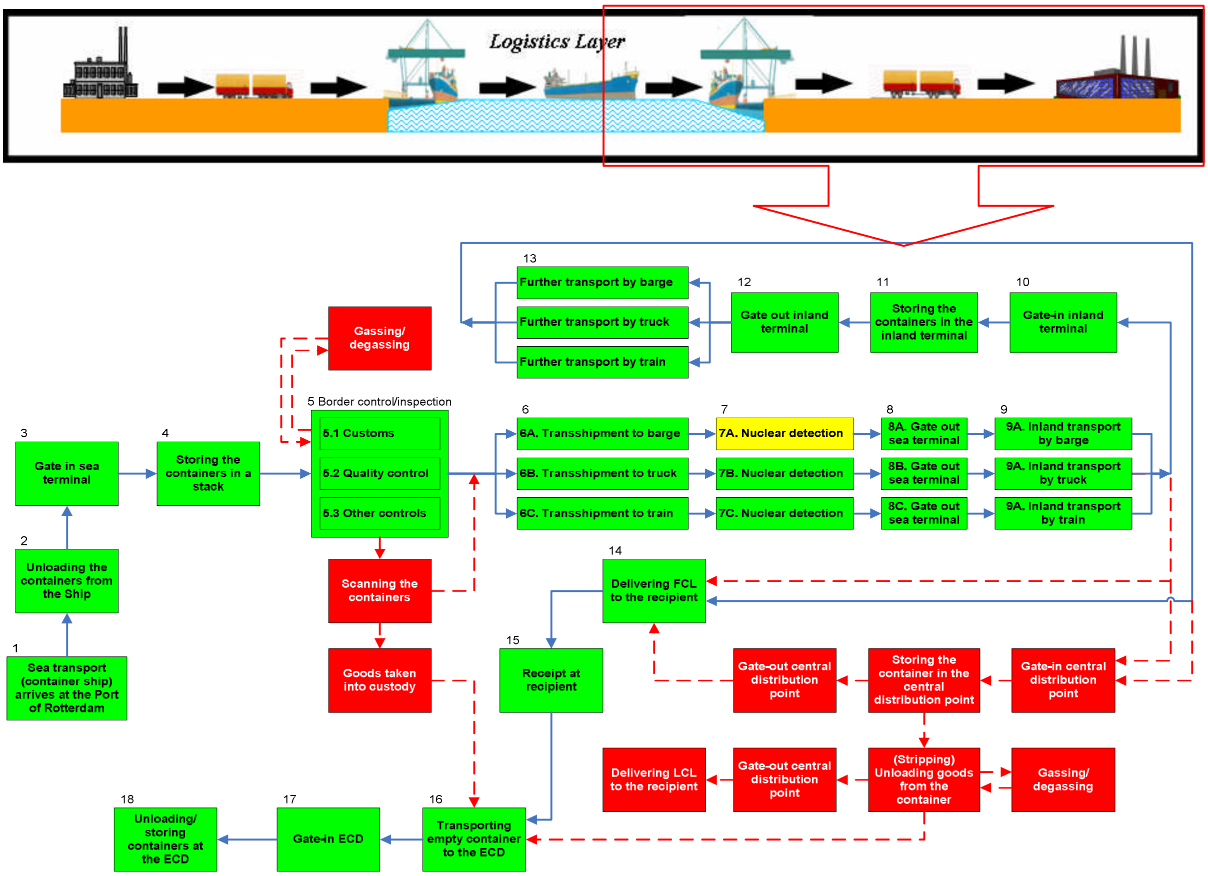

Logistics Layer
1 Sea transport (container ship) arrives at the Port of Rotterdam
2 Unloading the containers from the Ship
3 Gate in sea terminal
4 Storing the containers in a stack
5 Border control/inspection
5.1 Customs
5.2 Quality control
5.3 Other controls
Gassing/ degassing
Scanning the containers
Goods taken into custody
6
6A. Transshipment to barge
6B. Transshipment to truck
6C. Transshipment to train
7
7A. Nuclear detection
7B. Nuclear detection
7C. Nuclear detection
8
8A. Gate out sea terminal
8B. Gate out sea terminal
8C. Gate out sea terminal
9
9A. Inland transport by barge
9A. Inland transport by truck
9A. Inland transport by train
10 Gate-in inland terminal
11 Storing the containers in the inland terminal
12 Gate out inland terminal
13
Further transport by barge
Further transport by truck
Further transport by train
14 Delivering FCL to the recipient
15 Receipt at recipient
Gate-in central distribution point
Storing the container in the central distribution point
Gate-out central distribution point
(Stripping) Unloading goods from the container
Gassing/ degassing
Gate-out central distribution point
Delivering LCL to the recipient
16 Transporting empty container to the ECD
17 Gate-in ECD
18 Unloading/ storing containers at the ECD

Figure 9: Import scheme

2.2.1 Description of the import process scheme

In this subsection the complete import process shown in figure 9 is described in detail. Each green rectangle in the scheme represents one type of physical process that occurs regularly (standard processes). Each red rectangle in the scheme represents one type of physical process that does not occur regularly (alternative processes). Each yellow rectangle in the scheme represents one type of physical process that is related to transport modality Barge. The standard flow of containerized goods is numbered in order in which they follow each other. Normal lines (blue) represent the standard flow of containers and the dotted lines (red) represent the alternative processes. An enlarged version of the import scheme from figure 9 is to be found in appendix E.

1. *Sea transport (container ship) arrives at the Port of Rotterdam:* start of the import process and end of the export process;
2. *Unloading the containers from the Ship:* the containers that are on the discharge list, are unloaded from the container vessel;
3. *Gate in sea terminal:* this is the moment that the container enters the sea terminal (in Rotterdam);
4. *Storing the containers in a stack:* the containers are temporarily stored at the sea terminal for a while and waiting for the approval from the authorities to be allowed to enter further (inland) transport;
5. *Border control/inspection:* while the containers are temporarily stored at the sea terminal, the following (border) control activities take place:
    a. Customs: (nuclear scan), tax, control on dangerous goods, etc. These controls mostly take place at the sea terminal. After the approval from the customs the container can enter the following stage of transport;
    b. Quality control: brand control, food and consumer product safety control by (VWA), etc. These controls do not always take place at the sea terminal;
    c. Other controls: imported plants by (PD), imported animals, etc. These controls mostly take place out of the sea terminal;
    d. *Gassing/degassing:* these are optional processes that could occur while the controls a, b and c are curried out. Some containers are gassed in order to protect its content for different reasons. In order to be able to control the content of these kind of containers, they need to be degassed. After control, some times the containers need to be gassed again. This process takes place on a special location and conducted only by professional people;
    e. *Scanning the containers:* this is an optional process that could occur while the control is curried out. Containers (randomly) selected by the customs are going to scan facility. This is not nuclear scan but scan on smuggled goods and/or possibly people;
    f. *Goods taken into custody:* this is an optional process that could occur while the controls e is curried out. When for example smuggled goods are detected the goods are taken into custody by the related authorities and the empty container goes further in the SC (to the Empty Container Depot ECD).
6. Transhipment: after the border controls and inspections, the container is transhipped by one of the following three transport modalities:
    a. Barge;
    b. Truck;
    c. Train.
7. *Nuclear detection:* before the container goes out of the sea terminal, nuclear scan takes place:
    a. Barge: at the moment there are no facilities to scan the containers that are going to be transported by barge. This means that the containers that are transported by barge are not nuclear scanned;
    b. Truck: the containers that are loaded on trucks are going through the nuclear scan;
    c. Train: the containers that are loaded on a rail are going through the nuclear scan.
8. *Gate out sea terminal:* after the nuclear scan when no nuclear material detected, the container can be transported out of the sea terminal;

9. *Inland transport:* the containers can be transported to the inland by one of the three modalities;
10. *Gate-in inland terminal:* the containers can enter an in-inland or:
    a. Delivering FCL to the recipient (see 14) or
    b. Gate-in central distribution point (see 14.a).
11. *Storing the containers in the inland terminal:* the containers are transported to an in-inland terminal where they will be stored for a while (depending on the planning);
12. *Gate out inland terminal:* based on the planning, the containers are transported out of the inland terminal;
13. *Further transport:* depending on the planning and the destination for the container delivery, the containers are loaded from the inland terminal onto one of the three transport modalities;
14. *Delivering FCL to the recipient:* depending on the planning for the final destination of the container, the Full Container Load is delivered to its final recipient or:
    a. Gate-in central distribution point: the containers are transported to a CDP. This is an optional process;
    b. Storing the container in the CDP: the containers are stored at the CDP for a while (depending on the delivery planning). This is an optional process;
    c. Gate-out central distribution point: based on the delivery planning, the container is transported out of the CDP. This is an optional process. Or;
    d. (Stripping) Unloading goods from the container: the container is opened and the goods are unloaded. This is an optional process;
    e. Gassing/degassing: some containers are gassed in order to protect its content for different reasons. To be able to unload the content of the containers, they need to be degassed. This process takes place on a special location and conducted only by professional people. This is an optional process;
    f. Gate-out central distribution point: after the content of the container is unloaded, based on the delivery planning, the container is transported out of the CDP. This is an optional process;
    g. Delivering LCL to the recipient: after the contents of the container are unloaded, the Less then full Container Loads is delivered to its final recipient. based on the delivery planning, the container is transported out of the CDP. This is an optional process.
15. Receipt at recipient: the container is received by its final recipient. Due to time restriction, the truck driver mostly unloads the FCL and loads another empty container;
16. Transporting empty container to the ECD: the empty container is transported to the ECD;
17. Gate-in ECD: the empty container enters the ECD;
18. Unloading/storing containers at the ECD: the empty container is received by the ECD and unloaded from the truck. The empty container is ready for the export.

Key characteristics of the information flow related to import process:

Some of the key characteristics of import process are as follows:

1. *Information comes relatively early*: there are international security legislations and procedures for international transport. One of these international legislations is the so called “pre-arrival” information requirement. As the name “pre-arrival” indicates, the information regarding a shipment must arrive 24 hours prior to the import.

2. *Short timeframe for inspections at port*: due to the strict planning and the high volume of container flow, the necessary controls and inspections must take place in a relatively short timeframe.
3. *Confidentiality, Integrity, Availability and timeliness (CIA)*: depending on the country of origin and the country of departure, the CIA requirements of the cargo and the information (flow) could be vulnerable. Because not all countries have tight CIA inspections and control procedures. For example, data (values) can be different at different moments in time (e.g. goods description). It is not always easy to verify when the data is correct. This is an example of data integrity. (See section 2.4 Supply Chain Security (Definition) for detailed description of CIA)
   - *Accountability*: this point can be seen as a result from point 3 (CIA). When the integrity of the data (e.g. the transport history information) is not secure, it will not be easy to know which party (parties) in the SC is (are) to be taken responsible for a disruption of the SC (e.g. loss of goods).
   - *Dependencies on (timeliness and integrity of) data from previous parties in the chain*: this point can also be seen as a result from point 3 (CIA). When the integrity and availability of the data (e.g. the transport history information) is not secure, then the proceeding SC parties which are taking the transport over from the previous SC party will not be able to plan their processes accordingly. They are dependent on the information that they get.

2.3 Export

As mentioned earlier, the export process starts where the import process ends and visa versa. The following schemes show the focus on the export and the different physical processes that are involved. This scheme has been developed based on the instructions from the expert brainstorm sessions and literature research. The scheme is also validated during the field research.

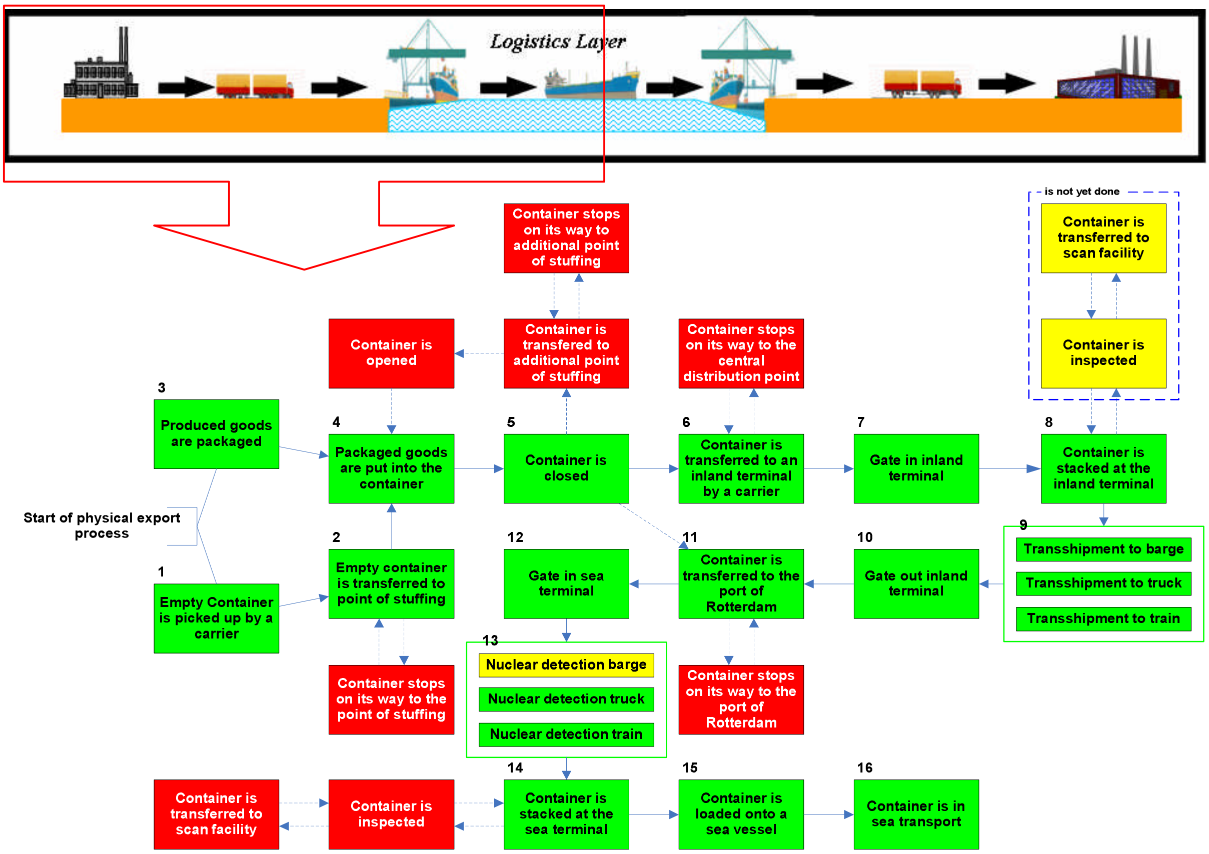

Logistics Layer
is not yet done
Container is transferred to scan facility
Container is inspected
Container stops on its way to additional point of stuffing
Container is opened
Container is transfered to additional point of stuffing
Container stops on its way to the central distribution point
3
Produced goods are packaged
4
Packaged goods are put into the container
5
Container is closed
6
Container is transferred to an inland terminal by a carrier
7
Gate in inland terminal
8
Container is stacked at the inland terminal
9
Transshipment to barge
Transshipment to truck
Transshipment to train
Start of physical export process
1
Empty Container is picked up by a carrier
2
Empty container is transferred to point of stuffing
12
Gate in sea terminal
11
Container is transferred to the port of Rotterdam
10
Gate out inland terminal
Container stops on its way to the point of stuffing
13
Nuclear detection barge
Nuclear detection truck
Nuclear detection train
Container stops on its way to the port of Rotterdam
Container is transferred to scan facility
Container is inspected
14
Container is stacked at the sea terminal
15
Container is loaded onto a sea vessel
16
Container is in sea transport

Figure 10: Export scheme [Meijer, 2007]

2.3.1 Description of the export process scheme

In this subsection the complete export process shown in figure 10 is described in detail. Each green rectangle in the scheme represents one type of physical process that occurs regularly (standard processes). Each red rectangle in the scheme represents one type of physical process that does not occur regularly (alternative processes). Each yellow rectangle in the scheme represents one type of physical process that is related to transport modality Barge. The standard flow of containerized goods is numbered in order in which they follow each other. Normal lines represent the standard flow of containers and the dotted lines represent the alternative processes. An enlarged version of the import scheme from figure 10 is to be found in appendix E.

1. *Empty Container is picked up by a carrier*: start of the export process and end of the import process;
2. *Empty container is transferred to point of stuffing*: the container is transferred to the POS by the truck driver. The empty container is almost never sealed;
   a. Container stops on its way to the point of stuffing: the empty container is not directly (non-stop) transported to the POS.
3. *Produced goods are packaged*: the goods are packaged (at the POS) and are made ready to be loaded into the container;
4. *Packaged goods are put into the container*: at the POS the packaged goods are put into the (empty) container. A container can go through more than one POS;
5. *Container is closed*: the packages are loaded into the container and the container is sealed at the POS or;
   a. Container is transferred to additional point of stuffing: container is sealed and it is not full. The container is transported to additional POS;
   b. Container stops on its way to additional point of stuffing: container is not directly (non-stop) transported to the additional POS;
   c. Container is opened: the seal is broken and container is opened at the additional POS. the packages are loaded into the container and the container is sealed again at the additional POS.
6. *Container is transferred to an inland terminal by a carrier*: the FCL of transported to an inland terminal by a currier (Barge, Truck or Train) or;
   a. Container is transferred to the port of Rotterdam (see 11);
   b. Container stops on its way to the central distribution point: container is not directly (non-stop) transported to the inland terminal.
7. *Gate in inland terminal*: the container enters the inland terminal;
8. *Container is stacked at the inland terminal*: the container is stored for a while before it is transported to the port of Rotterdam;
   a. Container is inspected: the container needs to be inspected;
   b. Container is transferred to scan facility: the container is transported to a scan facility (not nuclear scan).
9. *Transhipment*: after the possible inspections are completed, the container is transhipped by one of the following three transport modalities out of the inland terminal;
   a. Barge
   b. Truck
   c. Train
10. *Gate out inland terminal*: based on the planning, the container is transported out of the inland terminal;

11. *Container is transferred to the port of Rotterdam*: the container is transported to the port of Rotterdam for the further shipment;
    a. Container stops on its way to the port of Rotterdam: the container is not directly (non-stop) transported to the port of Rotterdam.
12. *Gate in sea terminal*: the container enters the sea terminal;
13. *Nuclear detection*: before the container enters the sea terminal, nuclear scan takes place
    a. Barge: at the moment there are no facilities to scan the containers that are transported to the sea terminal by barge. This means that the containers that are transported by barge are not nuclear scanned;
    b. Truck: the containers that are transported to the sea terminal by trucks are going through the nuclear scan;
    c. Rail: the containers that are transported to the sea terminal by train are going through the nuclear scan.
14. Container is stacked at the sea terminal: the container is stored for a while at the sea terminal before it is loaded onto the container ship (sea vessel);
    a. Container is inspected: the container needs to be inspected;
    b. Container is transferred to scan facility: the container is transported to a scan facility (not nuclear scan).
15. Container is loaded onto a sea vessel: the container is loaded onto a sea vessel and is ready to be shipped to an offshore country;
16. Container is in sea transport: container is on its way to the sea port of the offshore country.

<u>Key characteristics of the information flow related to export process:</u>

Some of the key characteristics of import process are as follows:

1. *Information comes relatively late*: the information about the shipment could change till the last container is loaded onto the container ship. This means that the information regarding the cargo arrives relatively late.

2. *Inspections at port is longer*: because containers are mostly stacked at the sea terminal (port) before they are loaded onto the sea vessel, the port authorities have relatively more time for the control and inspections.

3. *Confidentiality, Integrity, Availability and timeliness (CIA)*: the CIA requirements of the container (cargo) and the information are relatively secure. This is due to a relatively higher level of controls, inspections and the tight export procedures.

   – *Accountability*: this point can be seen as a result of point 3. Due to a higher level of controls, inspections and the tight export procedures, the integrity of the data (e.g. the transport history information) is secure, it will be easy to know which party (parties) in the SC is (are) to be taken responsible for a disruption of the SC (e.g. loss of goods).

   – *Dependencies on (timeliness and integrity of) data from previous parties in the chain*: this point can also be seen as a result of point 3 (CIA). When the integrity and availability of the data (e.g. the transport history information) is secure, then the proceeding SC parties which are taking the transport over from the previous SC party will be able to plan their processes accordingly. But they will always be dependent on the information that they get.

2.4 Supply Chain Security (Definition)

In most areas of life, people and organizations who work hard and spend money expect something in return, but with security, the pay-off is that nothing happens. Human psychology does not see this as a true reward. It can be a challenge to see the benefits of the resources invested. Indeed a good security manager oversees a site where nothing bad happens. Often, as time passes, people can begin to think that nothing bad will ever happen and be tempted to divert resources away from security. [Slay J., & Koronios A., 2006]

When searching for the exact meaning of security, the following definition is to be found:

Security *is the condition of being protected against danger or loss. In the general sense, security is a concept similar to safety. The nuance between the two is an added emphasis on being protected from dangers that originate from outside. Individuals or actions that encroach upon the condition of protection are responsible for the breach of security.* [www.wikipedia.org]

There are many different definitions of security in the context of supply chains. For example:

A secure supply chain *is a supply chain where various measures have been taken to guarantee a certain level of security. Security measures can be taken with regards to (a combination of) physical flows, information flows and/or money flows* [PROTECT, 2005a].

To assure a secure supply chain, security measures must be put in place. Most of these measures must have a preventive character. These measures have to ensure the confidentiality, integrity, availability/reliability of the entire SC and the information that flows among the entities directly and indirectly involved in the SC. Besides this the measures should also protect social (people and environment) and economic structures [Becker & Verduijn, 2005a, p. 13].

A reliable SC means: ***A reliable SC*** *ensures that the final customer receives the right product, at the right costs, at the right time, in the right condition, and in the right quantity* [Coyle, Bardi & Langley, 1996 quoted in PROTECT, 2005a].

Due to internal and external changes, which are related to the supply chain, the security measures that are put in place must be audited regularly. This auditing is needed because these measures can become obsolete because the security measures are directly linked to the global political changes/events (9-11, terrorist attacks, war, etc.), non-political threats (theft, illegal human traffic, smuggling drugs, etc.). But the question will still remain, how much security is needed and at what costs? Based on the nature of the changes, the measures must be amended, substituted or deleted.

Supply chain security needs to receive a lot of attention because security was, and it has become a very important issue for the governments and for the companies directly and indirectly involved.

A secure supply chain is a supply chain where up-to-date measures are taken to ensure both the physical and non-physical security of the logistic process. Security measures can be taken with regards to (a combination of) physical or information flows and preferably are preventive of nature.

Definition 4: Secure Supply Chain defined for work package 5.1

In this definition is mentioned that the security measures must be up-to-date and they must have preventive character. The reason behind these conditions is that the security measures must be audited on a regular basis because the measures must comply with the risks/threats that are present at the moment. In Dutch there is a saying “voorkomen is beter dan genezen” which means preventing is better than curing. The measures must prevent a certain threat/danger from happening instead of solving/correcting it after that it has happened. Mostly it is not possible to correct a damage that is already made (e.g. loss of human life). That focusing on the preventive character of the measures will, on the long term, be more beneficial compared to other measures.

Furthermore, in this thesis the security of SC is divided in physical security and non-physical (information) security.

A physical security state is a state where measures are taken to protect the supply chain against one of the following risks/threats:

1. *Terrorism:* (see Definition 5)
2. *Smuggle:* (see Definition 6)
3. *Theft:* (see Definition 7)

There are many different definitions for the term "terrorism". No single definition of terrorism has yet been accepted by all countries. This is because an act of terrorism has many different reasons and interpreted differently. But for the purpose of this thesis, terrorism is defined as: (Academic consensus definition)

> *"Terrorism is an anxiety-inspiring method of repeated violent action, employed by (semi-) clandestine individual, group or state actors, for idiosyncratic, criminal or political reasons, whereby - in contrast to assassination - the direct targets of violence are not the main targets. The immediate human victims of violence are generally chosen randomly (targets of opportunity) or selectively (representative or symbolic targets) from a target population, and serve as message generators. Threat- and violence-based communication processes between terrorist (organization), (imperilled) victims, and main targets are used to manipulate the main target (audience(s)), turning it into a target of terror, a target of demands, or a target of attention, depending on whether intimidation, coercion, or propaganda is primarily sought" (Schmid, 1988)* [www.unodc.org].

Definition 5: Terrorism

In the literature, smuggle is defined as any kind of illegal transport of people and/or goods without paying lawful customs charges or duties. In this thesis, it is important to know the non-financial risks of the smuggled people and/or goods. This is why for the purpose of this thesis, smuggling is defined as:

> *Smuggling is any form of unlawful transportation (import and export) of people and/or goods for the purpose of preparing and/or conducting a terrorist attack.*

Definition 6: Smuggle

In the literature, theft is defines as "*dishonest appropriation of goods belonging to another with the intention of permanently depriving the other (the owner) of it*" [Theft Act 1968 enacted by the British Parliament]. In this thesis, it is important to know the non-financial risks of the stolen goods. This is why for the purpose of this thesis, theft is defined as:

> *Theft is dishonest appropriation of goods belonging to another with the intention of permanently depriving the other (the owner) of it and using the stolen goods to prepare and/or conduct a terrorist attack.*

Definition 7: Theft

All these threats can be related to each other. For example drugs are smuggled to finance (the preparation for) a terrorist attack. Some countries are under the UN embargo for importing or exporting some goods (e.g. nuclear martial) because these goods could be used (as mean) for terrorist attack. Or goods are stolen either to be used as a mean for terrorist attack or to be soled in order to finance (the preparation for) a terrorist attack.

An information security state is a state where measures are taken to ensure the information (flow) in regard to one of the following aspects:

1. *Confidentiality:* A characteristic of information such that it is available only to those authorized to view;
2. *Integrity:* A characteristic of information such that the information and any change to it are accurate and complete;
3. *Availability:* A characteristic that information assets or a service and the components that make it up can be accessed and used when needed. [*Slay J. & Koronios A., 2006*]

2.5 Supply chain actors

In the SC, many organizations (both commercial and non-commercial) are involved in the transport of a container from shipper to consignee. Wagenaar (1992) [cited in Oosterhout et al., 2000] defines the following 5 groups of actors:

- Customer group; the final customers of the SC;
- Organizing group; responsible for the organization of the physical transport and supporting information documents.
- Physical group; this group is responsible for the physical processes in the SC.
- Authorizing group; this group is composed of organizations responsible for public infrastructure and of regulatory authorities that monitor if the SC companies observe the rules and regulations that apply to them.
- Financial group; this group supports the financial transactions between the different organizations in the SC.

In this thesis, the following terms are used to represent the different types of actors in the SC:

When the term "supply chain organizations" or "supply chain actors" is used, all groups, except the financial group, are meant. This is because the financial group and the associated information exchanges are left out of the scope of analysis.

When the term "supply chain companies" is used, all groups, except the financial group and the authorizing group are meant.

When the term "regulatory authorities" is used, the authorizing group is meant.

Definition 8: Terminology used in this thesis [adopted from Meijer 2007]

In the groups, different actors can be distinguished. The following table contains a list of actors which are active in the container transport:

Customer group	Shipper / exporter Consignee / importer
Organizing group	Forwarder (merchant haulage) Shipping line agent (carrier haulage) Ship broker
Physical group	ECD operator Pre- or on-carrier - Barge operator - Rail operator - Road carrier Central distribution point / container freight station Inland terminal Sea terminal Shipping line / sea carrier
Authorizing group	Customs Environmental office (SCMR) Food and consumer product safety authority (VWA) Ministry of transport, public works and water management (V&W) Plant health department (PD) Port authorities Seaport police

Table 2: Supply chain actors (Oosterhout et al. (2000)) [Meijer, 2007]

The shipper and the consignee are the final customers of the SC. The SC always starts with an importer receiving or ends with an exporter sending the goods packaged in a container. In the logistic process of transporting a container, the responsibility for the container and the contents of the container is often contractually devolved to the actors in the physical group or to the actors in the organizing group that may devolve the responsibility to the physical group in their turn.

The authorizing group represents a special type of actor responsible for public safety and the inspection of compliance with (international) law. The interest of the other groups is to transport a container as efficiently as possible from one point to the other. The authorizing group tries to ensure public safety and checks the compliance with (international) law with the least disruption to the logistic process. For scanning the container, for example, the container has to be taken out of the chain. Customs tries to minimize the time delay caused by the scanning of the container [Björkencrona, 2006].

In appendix A, the different actors involved in the logistic process are defined and described in more detail. In Figure 11, a quick overview of the SC for the SC companies is depicted. The scope of the actors in the export process is shown on the left-hand side of the figure and the scope of the actors in the import process is shown on the right-hand side of the figure. For every SC company the place of acceptance is denoted by the letter “A” and the place of delivery is denoted by the letter “D”. Between the place of acceptance and the place of delivery the corresponding SC company is responsible for the (contents of) the container [Oosterhout et al, 2000].

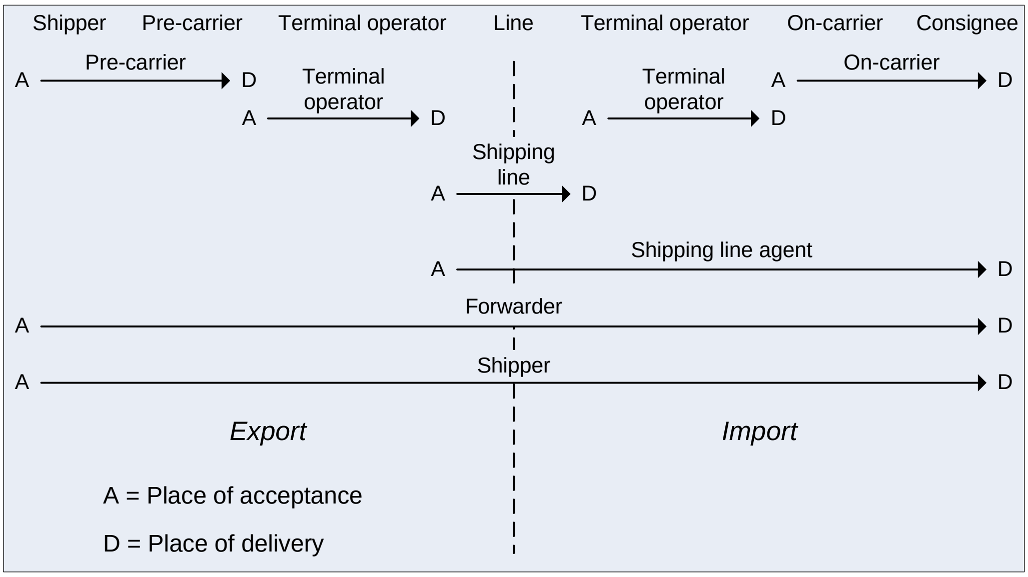


Figure 11: Scope of supply chain companies (Oosterhout et al. (2000)) [Meijer, 2007]

2.6 Conclusion

In this chapter, the SC for the container transport is introduced. A basic SC consists of five different activities. Since the focus of this thesis is only on the container transport activity of the entire SC, that's why the supply chain is defined as the network of organizations that are involved, through upstream and downstream linkages, in the different container transport related processes and activities that produce value in the form of products and services in the hands of the ultimate consumer (shipper or consignee).

Also a graphical representation of the SC definition is provided. Based on this, the schemes for the physical processes involved in import and export of containers are developed and briefly described. Also the key characteristics of the information flow related to both, import and export process are described.

Then, the SCS in the container transport is defined. It clarified what is meant by the SCS in relation to the container transport. Also the three types of threats (*Terrorism, Theft and Smuggle*) are defined.

Further, the actors that are active in the SC are described in more detail. This is done to create a consistent definition of the actors in the SC throughout the analysis. The actors are divided into four groups namely the customer group, the organizing group, the physical group and the authorizing group. The financial group is not considered in the analysis because financial information is left out of scope.

The findings from this chapter will be used as input for the next chapter (Chapter 3). In chapter 3 the threats and risks involved in the SC, as described in this chapter, are defined.

3 SCS threats and risks

This chapter is about the SCS threats and risks. This chapter provides a clear view of the most important risks and the SC links that are the most vulnerable.

This chapter is outlined as follows: section 3.1 describes why it is important to identify the SCS threats and risks. It also describes the factors contributing to the SC risks. Section 3.2 defines the most important SCS threats and risk for both import and export process. It describes the criteria based on which the threats and risks are identified. Finally the identification of the weakest security links in the SC is done in section 3.3. It also provides reasoning for the security strength or weakness of the SC links for both physical and information security.

3.1 Introduction

Before going into details, it is important to define what is meant by the term "risk". There are many different interpretations of risk in the academic literature. Amongst the most widely cited are variance-based definitions drawn from classical decision theory, where risk is the "*variation in the distribution of possible outcomes, their likelihoods and their subjective values";* or the hazard focussed interpretation, common in risk management, which is more likely to present risk in terms of: "*Risk = Probability (of a given event) x Severity (negative business impact)"* [March, J.G. & Shapira, Z. (1987)]. In this work we use risk in line with common usage in the sense that it relates to supply chain vulnerability, as *"at risk: vulnerable; likely to be lost or damaged"* [Christopher, M. & Peck, H. (2004)].

Security risks exist in all transport modalities. These risks are not all covered by security legislations and rules (measures). The security level differs per transport modality. Some of the modes are more vulnerable than others and the security of some of the land and water based transportation (e.g. transport of dangerous goods) is covered by strict security legislations and procedures, other land and water based transport modalities are still very vulnerable for security threats.

The consequences of a threat that occurs could be enormous and could have different effects. Some of the possible effects are on:

- EU population - A misuse of the supply chain could result in possible thousands of injuries and fatalities. For example when the threat (transport) reaches all 456 million inhabitants of the EU.
- Economy - the EU industrial base. All economic activities in the supply chain are at risk. Everyday cargo is shipped and transported to serve the needs for industry and consumers. Possible terrorist intervention can result in billions of Euros economic damage to the EU. It is estimated that the maximal cost of any terrorist attack on a European corridor cost maximal 2% of the original investment. Even so the economic damage could tally up as high as 6.6 billion Euros for major existing transport corridors by taking out a single piece of infrastructure. However, a misuse of the transport supply chain to conceal and transport weapons of mass destruction to industrial and densely populated conglomerates can result in even higher economic damages. Nuclear detonation in a major port city could have a calculated economic damage of 200 to 500 billion Euros [DNV Consulting, 2006].
- Environment – Using the SC for conducting an attack on a nuclear facility would not only result in thousands of fatalities but it would also have a negative long term effect on the regional environment and nature. A large area could no longer be used for agricultural purposes. People who live (have lived) in the effected area could develop new diseases like it was the case after the explosion at the nuclear facility of Chernobyl in Ukraine. Some of the children born in that area after the explosion are currying the so called Chernobyl disease and these kids are called the "Chernobyl children".

<u>Factors contributing to supply chain risk</u>

Whilst SC risk has always been present, there are a number of factors which have emerged in the last decade or so which might be considered to have increased the level of risk. These include:

1. *A focus on efficiency rather than effectiveness*: businesses have become more focused on efficiency. For example the JIT business models. This made the businesses more dependent on the SC (planning and coordination) and made the impact of a SC risk (disruption) even bigger.
2. *The globalisation of supply chains*: globalization and outsourcing mostly results in contribution from more locations (countries) in order to have a final product. This leads to more border crosses and possibly increased SC vulnerability.
3. *Focussed factories and centralised distribution*: factories are focused on centralized manufacturing and distribution due to the benefits like the economy of scale. This makes the factories less flexible because they focus on producing few products (small product range) with high volume and the products has to travel great distances and often cross many borders before it gets to its final destination. This could increase the SC vulnerability.
4. *The trend to outsourcing*: at a practical as well as a theoretical level, outsourcing has many attractions (e.g. spreading the financial risks, using third parties to offer new products and cervices, creating a network organization). But the risk of outsourcing for the SC is the loss of control. Disruptions in supply can often be attributed to the failure of one of the links in the SC and – by definition - the more complex the SC network the more links there are and hence the greater the risk of failure.
5. *Reduction of the supplier base*: companies intend to decrease the number of their suppliers. Even though there are many benefits to supplier base reduction it has to be recognised that it brings increased risk with it. This made the businesses/companies more dependent on supplier(s) and vulnerable for the disruption to the processes of the supplier(s).
6. *Volatility of demand*: the demand for products and goods in the market is very volatile. This makes it more difficult for the companies to optimally plan their stocks. This means low stokes (JIT) which again leads to more dependency on the suppliers and vulnerable for the disruption to the processes of the supplier(s).
7. *Lack of visibility and control procedures*: lack of confidence (visibility and control) in a SC leads to adds to the SC risk. SC visibility means, SC members being able to accurately follow the containers from the start till the end of the pipeline. Lack of SC visibility forces SC members to rely on forecast for their inventories. SC control means, SC members being able to respond to disturbances in appropriate way. [Summarized from Christopher, M. et al. (2002)].

The factors above confirm how vulnerable SC can be. That is why the organizations need to identify and be aware of the vulnerabilities and risks they could face, as the next paragraph explains.

3.2 The most important security threats and risks in the SC

Based on literature study [Goedhart, E.J. & Hulsebosch, B., (2001)] and recommendations from the expert brainstorm sessions, the security risks and threats are divided in three different types of security risks namely the physical security risks, the information security risks (non-physical security risks) and the financial risks. The first two types of security risks (physical and information) are discussed bellow but the third type of the risk (financial) is out of scope.

1. <u>Physical security risks:</u>

The following risks are meant by the physical security risks:

- Infrastructure risks: The terrorist has the objective to damage or destroy transport elements in order to disrupt the transport supply chain. The transport elements are in this case the terrorist’s target.

- Supply chain risks: The terrorist has the objective to misuse the transport supply chain as their means to create damage or fatalities. The transport elements are in this case not the target but the means. The misuse of the supply chain relate to:
    - The transport supply chain (cargo or mobile unit) is used as a means to conceal and transport various explosives, incendiary devices or nuclear devices to a location where they are unloaded or detonated;
    - The transport supply chain (cargo or mobile unit) is misused as a weapon [DNV Consulting, 2006].

2. Information security risks

Information security risks mean the risks to the CIA (Confidentiality, Integrity and Availability) requirements. The risks are that:

- The risk that the information about a transport (e.g. nuclear or chemical material) is available unauthorized personnel/people. This information can be used for planning to misuse the SC for terrorist attack and/or theft. This is information *confidentiality* risk.
- The risk that the information about a transport (e.g. nuclear or chemical material) is (deliberately) changed by (unauthorized) personnel/people. This manipulation of information can be used for planning to misuse the SC for terrorist attack and/or theft. This is information *integrity* risk.
- The risk that the information about a transport (e.g. nuclear or chemical material) is not available timely or (deliberately) made unavailable by (unauthorized) personnel/people. This interruption of information availability can be used for planning to misuse the SC for terrorist attack and/or theft. This is information *availability* risk.

In order to analyze the risks/threats that are related to the SC developed a security risk and information analysis tool using Microsoft Excel sheet is developed. This tool is based on the findings from the literature studies and the recommendations from the expert brainstorm sessions. The import and export schemes are used as the starting point for the analysis. More expert brainstorm sessions were needed to further develop the eventual security risk and information analysis tool. At each expert brainstorm session a draft version of the tool is presented and evaluated (commented) by the attendees of the sessions. The elements of this analysis tool – for both import and export – are the following ones:

1. *Processes*: all the physical processes involved in importing or exporting containers as mentioned on the import and export schemes are used;
2. *Actors involved*: the actors directly and indirectly involved in each of the processes are defined. This will provide a better view of the responsibilities that are forwarded from one actor to another. This also clarifies the weakest links in the SC;
3. *Signals:* for each process, the possible signals – which indicates unusual steps or issues that requires extra attention – are listed. A signal does not always lead to a threat but it could. For the purpose of this paper, the term signal can also be substituted by the term risk because as explained for signals, not every risk will lead to a certain threat but it could;
4. *Importance:* which signals could or couldn't lead to a threat is depending on the importance of the signal according to the actors directly and indirectly involved in the process. Three different importance levels are defined (*High, Medium and Low*). *High* importance signals lead to a direct threat or a threat in a short time. *Medium* importance signals lead to an indirect threat or a threat which will take a long time to occur. *Low* importance signals barely lead to a threat. These scores are verified during the field research (interviews).
5. *Threats:* based on these four criteria the threats are found. As described in Chapter 2, there are three different types of threats defined namely; Terrorism, Smuggle and Theft.

Table 3 shows an example of this part of the methodology which is used to analyze SC risks. A copy of the complete table is to be found at appendix G.

				Threats		
Processes	Actors involved	Signals	Importance (Low Medium High)	Terrorism	Theft	Smuggle
1. Container vessel arrives at the Port of Rotterdam	Directly involved: - Sea terminal operator (Haven meester) Indirectly invoved:	The container vessel/ cargo is coming from a suspicious country/ port of origin or shipper	h	x		x
		Vessel contains containers that are not on the pre-arrival container list	m	x		x
		Vessel contains containers with explosive/chemical/dangerous material	h	x		x
	Directly involved: - Sea Port Police - Ship Agent Indirectly invoved:	Unauthorized people are or have been on board. Container is being tempered by people/personnel on board	h	x	x	x
		On board incidents are reported	m	x	x	x

Table 3: Example of the SCS threats and risks analysis system

Because SC is a very dynamic sector, no guarantee about the completeness of this risk analysis could be given. This is also due to the fact that the data which is analyzed here can be different when time passes. Also the sources from where the information is gathered are broad but not deep. This means that the information is gathered from limited actors from a certain chain in the SC and not from more actors from a certain chain in the SC. This is due to the time and availability constrains.

This risk analysis is developed in close cooperation with Port infolink, Dutch customs, and Port authority (Havenbedrijf Rotterdam). These SC actors were actively involved in developing this risk analysis tool.

3.2.1 Import

The most important threats – related to importing containers – are defined by analyzing the level of importance of each signal. The level of importance (*Low, Medium or High*) for each signal is defined during the expert brainstorm sessions and the workshop. Because the focus is on the *most* important threats, only the signals with a *high* level of importance are considered to being (to lead to) the most important threats. The following table shows the list the most important threats related to import. A copy of the complete table is attached in appendix G.

			Threats		
Processes	Signals	Importance (Low Medium High)	Terrorism	Theft	Smuggle
1. Container vessel arrives at the port of Rotterdam	The container vessel/ cargo is coming from a suspicious country/ port of origin or shipper	h	x		x
	Vessel contains containers with explosive/chemical/dangerous material	h	x		x
	Unauthorized people are or have been on board. Container is being tempered by people/personnel on board	h	x	x	x
2. Unloading the containers from the container vessel	Unauthorized people are at the location. Container is being tempered by personnel	h	x	x	x
	Container is stolen	h	x	x	
3. Gate in Sea terminal	Container is not sealed	h	x	x	x
	Container contains goods to be smuggled	h	x		x
	Container contains goods to be used in a terrorist attack (disruption of logistic process)	h	x		x
4. Storing the containers in a temporary stack (Terminal)	Contents of container is stolen	h	x	x	
	Illegal material is put in the container	h	x		x
	Fake seal is used	h	x	x	x
5. Border control/inspections	Container is from a suspicious country of origin	h	x	x	x
	Container contains dangerous goods/material	h	x		x
7. Nuclear detection	The container contains nuclear material	h	x		x
9. Inland transport by a carrier	Container is stolen during transport	h	x	x	x
	Contents of container are stolen during transport	h	x	x	
	Contents of container is used in a terrorist attack	h	x		
10. Gate in inland terminal	Container contains illegal material	h	x		x
15. Receipt at recipient	Container is not sealed/seal is broken	h	x	x	x
	Conatiner is sealed but the seal (number) is different than expected	h	x	x	x
	Container containes unexpected dangerous material	h	x		x
	The content of the container is different than expected/goods are stolen	h	x	x	x
17. Gate in ECD	Container is not empty, contains goods used in terrorist attack	h	x		x
18. Unloading/storing containers at the ECD	Container is prepared to be misused for terrorist attack, theft, smuggle, ect (Dubbel bodem)	h	x	x	x

Table 4: Most important import related threats and risks

Table 4 proves that the threats are related to each other and one certain security signal could cause a threat which can lead to the cause of other threat. For example "Container is stolen" is an indication of theft. Depending on the contents of the container (e.g. nuclear or chemical material), this can be used as means for a terrorist attack. This is also applicable for the export process.

3.2.2 Export

Same as for the import process, the most important threats – related to importing containers – are defined by analyzing the level of importance of each signal. Also same as for the import process, the level of importance (*Low, Medium or High*) for each signal is defined during the expert brainstorm sessions and the workshop. Because the focus is on the *most* important threats, only the signals with a *high* level of importance are considered to being (to lead to) the most important threats. The following table shows the list the most important threats related to import. A copy of the complete table is to be found at appendix H.

			Threats		
Processes	Signals	Importance (Low Medium High)	Terrorism	Theft	Smuggle
1. Empty Container is picked up by a carrier (road / barge / rail)	Container not empty, contains goods to be smuggled	h	x		x
	Container not empty, contains goods used in terrorist attack	h	x		x
2. Empty container is transferred to point of stuffing (POS)	Illegal material is put into container	h	x		x
3. Produced goods are packaged	Illegal material is packaged	h	x		x
	Material packaged for terrorist attack	h	x		x
4. Packaged goods are put into the container	Packaged goods are goods to be smuggled or can be used in a terrorist attack	h	x		x
	Packaged goods are exchanged for illegal goods (e.g. by the loading personnel at POS)	h	x		x
	Packaged goods are stolen during loading of the container	h	x	x	
	Packaged goods are stolen by the truck driver	h	x	x	
5. Container is closed	Container is not sealed properly	h	x	x	x
6. Container is transferred to an inland terminal by a carrier	Container is stolen during transport	h	x	x	x
	Contents of container is stolen during transport	h	x	x	x
	Contents of container are used in a terrorist attack	h	x	x	
7. Gate in inland terminal	Container is not sealed	h	x	x	x
	Container contains illegal material	h	x		x
8. Container is stacked at the inland terminal	Container is stolen	h	x	x	x
	Contents of container is stolen	h	x	x	x
12. Gate in sea terminal	Container contains goods to be smuggled	h	x		x
	Container contains goods to be used in a terrorist attack (disruption of logistic process). Economic risk is higher than risk of loss of life. Especially interesting for offshore port because they don't have to scan (or are more sure about) the contents of the container.	h	x		x
16. Container is in sea transport	Container is used in a terrorist attack	h	x		

Table 5: Most important export related threats and risks

3.3 The weakest security related links in the SC

All transport is at risk [DNV Consulting, 2006]. This statement could be true, but some SC links are more at risk compared to others. This is also shown in the table 4 and 5 of the previous paragraph. The strength of a SC link also depends on whether it is involved in import or export of containers. Some SC links are equally vulnerable for both import and export process (e.g. Inland transport by a carrier: "*Container is stolen during transport*"), but there are also SC links that are more vulnerable during the import process (e.g. the sea port or border control: "*Container is from a suspicious country of origin*") or during the export (e.g. Point of Stuffing (POS): "*Illegal material is put into container*").

The strength of the SC links is also depending on the type of transport means (*Barge, Truck, and Rail*) is used for transporting containers. In this thesis, by the term "SC link" the points in the SC is meant where a container is transhipped from one transport modality to another and the security level of each transhipment point. For example, containers that are transported by barge are not nuclear scanned because there is no such nuclear scanning infrastructure at the port of Rotterdam. Barge could be a potential target for people with intention to smuggle nuclear material. But there are also arguments which make container transport by barge more secure compare to other transport means. Barge can transport more containers at once and the containers are loaded in such a sequence that it is not possible to open them during the transport. The barge operates on the waterways this means that they are not easily accessible by unauthorized people. Containers transported by other two transport means are nuclear scanned. This means that these containers will not be easy target to smuggle nuclear material.

Based on the analysis from the previous paragraph, the findings during the field research and the recommendations from the experts brainstorm sessions a differentiation is made between the weakest links in the physical layer of the SC (physical security) and the transaction layer of the SC (information security). Although these two layers are correlated with each other, they are two different processes. As a result the following links are characterized as being the *weakest* security related links in the SC:

I. Weakest links in the physical layer (physical security)

1. *Point of container stuffing & stripping*: this is the point where the goods are loaded into containers of unloaded from the container.
2. *Point of sealing*: this is the point where the container is closed and sealed.
3. Points of feeding and consolidation: this is the point where the containers are brought together and are stored.
4. *Transhipment points*: these are the points where the containers are exchanged from one modality to another (e.g. container is brought by a truck to an inland terminal and there it is loaded onto a barge for further transport).
5. *Stops of inland transport*: these are points where the containers are not moving.
6. *Point of End-user arrival*: this is the point where the container is delivered to its final destination.
7. *Handling of empty containers*: this is the point where the empty container is transported to the empty container depot (ECD).

II. Weakest links in the transaction layer (information security)

This part is related to the *information systems* that are used in the SC by different SC parties. The information flow, data and meta-data generated by the information systems is here the main focus. Under the meta-data is meant the information about the original data (e.g. the information about the frequency and the location of the changes to a certain data element). Proper measure for the CIA requirements could contribute to strengthening the weakest links in the transaction layer. The following points can be considered as the points that could contribute to strengthening the links in the transaction layer:

1. *The CIA requirements for booking information*: the booking information is the information by which a certain container transport starts and belongs to it during its entire “life cycle”. This is information could be crucial and that’s why the flow of it requires very tight CIA and security requirements.
2. *The CIA requirements for seal information*: the information regarding the seal (e.g. seal number, seal location, sealed by, seal status, etc.) offers information about the status of a container. This is why the flow of this information element requires high level of security and CIA requirements.
3. *Accountability*: the information about the responsibility of the container during its transportation is very important. Because this is the point where the claims (of threats or losses) are made. That is why the secure flow of this information needs additional attention.
4. *Dependency on (timeliness and integrity of) data from previous parties in the chain*: this is the point where the information is passed from one party to the other in the SC. its not only important that information is available on time but its also very important that the information is accurate and safe. This is why tight CIA and security requirements are inevitable.
5. *The meta-data*: the registration and control of meta-data is very important. It could provide an indication regarding the status of container and the security level of a container. For example if the booking information is changed or the seal information is changed more frequently than its usual, then it could be an indication of unlawful transportation and should trigger additional control by the responsible authorities. The meta-data could be found in the systems like the port community systems.

The information security is very important for enhancing the overall security level of the SC. During the interviews, this issue is mentioned repeatedly by the SC parties. The information security is not only important to enhance the SCS but it could also indirectly make the SC more efficient. For example, when the road operator has the information regarding the contents of a container – which is not always the case – it can plan the safest route to its final destination and it can take preventive security measures in case something happens to the container. But others (some of the SC parties from the interviews) suggest that providing the information regarding the content of the containers to the road operators has its cons too. For example, the information can leak to unauthorized people and they could misuse this information for conducting terrorist attack. The issue of CIA requirements for the information security in the SC is a very important issue and it is a good topic for further research.

Based on the results from the interviews and the recommendations from the expert brainstorm sessions, the weakest security links in the SC can be defined by:

A. Practical risks and the easiness by which a security breach can be created;

B. The implemented security measures;

C. The impact of a security breach.

Based on these criteria, the following table can be produced:

SC Link	A	B	C
Strong	Limited	Limited	Limited
Strong	Limited	High	Limited
Strong	Limited	High	High
Weak	Limited	Limited	High
Weak/Strong	High	High	High
Weak	High	Limited	High
Weak	High	Limited	Limited
Strong	High	High	Limited

Table 6: Strength / weakness of the SC links

Table 6 shows that for example if its easy to create a security breach and the there are limited security measures to prevent this security breach from happening and the impact of this security breach is high, then it’s a weak SC link (“A” = High, “B” = Limited, “C” = High).

3.4 Conclusion

In this chapter, the SCS threats and risks are introduced. It became clear that it is very important to identify the SCS threats and risks because the consequences of the threats that may occur – to the population, economy and environment – are tremendous and sometimes irrecoverable (e.g. loss of lives due to a nuclear attack using the SC). There are factors that contribute to the SCS risks. These factors make the SCS more vulnerable, for example due to the globalization of SC or lack of visibility and control of procedures.

Security risks exist throughout the entire SC. A number of most important SCS threats and risks are aggregated and put together in an analysis system. The results are validated by the parties directly and indirectly involved in the SC. These SCS threats and risks are characterized by its importance (*High, Medium or Low*). As a result it became clear that some security risks are more important than the others. For example, the risk related to a stolen container with the nuclear material is much more important than the risk related to a stolen empty container.

Another important point that has become clear is the strength of the different SC links. The strength of a SC link depends on the transport means (*Barge, Truck or Train*) used to transport a container, the process (*Import or Export*) a SC link is involved in and the security level of the SC link. Based on these criteria a number of SC links are identified which can be characterized as the *weakest* SCS links. The threats and risks identified in this chapter are certainly not all possible SCS risks.

The results from this analysis are used as input for the analysis in the next chapter (Chapter 4). In the next chapter the security measures are defined that are needed to prevent, eliminate or decrease the chances for the threats and risks identified in this chapter to occur and to strengthen the SCS weak(est) links in order to improve the (overall) level of SCS.

4 Security measures for enhancing the SCS and SC visibility

Based on the results from Chapter 3: SCS threats and risks, in this chapter the security measures are defined which could contribute to enhancing the SCS and the SC visibility.

This chapter is outlined as follows: Section 4.1 introduces the security measures (based on the literature research). This section describes the terms that are used further in this chapter and the different types of measures. Section 4.2 describes the security measures for the threats and risks that are identified in the previous chapter for both import ad export processes using the analysis system. Finally, section 4.3 introduces the "Sense and response model". This section describes the use of this model for the SC. It provides some examples which prove that this model is applicable for the SCS.

4.1 Introduction

In this thesis by the term "SCS measures" is meant not only the physical security measures (e.g. the technological security measures) but also non-physical security measures like reorganization of the business processes (e.g. the organizational security measures).

1. *Technological security measures*: these are the type of security measures where technology is used to enhance the SCS. <u>*Some*</u> examples of this kind of security measures are:
    a. Installing GPS systems (track and trance system) on the trucks in order to be able to follow the containers;
    b. Installing surveillance camera's at different locations (e.g. POS) to control the process of loading the goods into the containers;
    c. Using new information system for better exchange of the security relevant information among the parties involved in the SC;
    d. Embedding the containers with RFID chips;
    e. Using smart seals (Electronic seals). For more details see Meijer, 2007.
2. *Organizational security measures*: these are the type of security measures where some changes in the business processes are used to enhance the SCS. <u>*Some*</u> examples of this kind of security measures are:
    a. Redesigning the business processes. The current business processes are redesigned (or new processes are added or some processes are removed) in a way that it reduces the security threats;
    b. Introducing new requirements (e.g. identification cards for entrance or new access control regulations). This will provide more control and visibility in who is entering or exiting a certain area;
    c. Improved job descriptions to dedicate the responsibilities to each employee individually. This will help improve the involvement of the employees in the business processes and it will also increase the productivity;
    d. Providing better information about the possible risks related to the processes to the employees. This will increase the awareness which will positively influence the overall process security;
    e. Stimulating new security related cooperation's with other parties involved in the SC.

These security measures are classified as *preventive* (p), *detective* (d) and *corrective* (c). But to get a better perspective of the total security measures and their characteristics (e.g. what security measures are currently in place and what security measures are required in the future in order to enhance the overall SCS) two more characteristics are added namely *current* (cur) and *future* (f). The use of this classified security measures is visualized in figure 12.

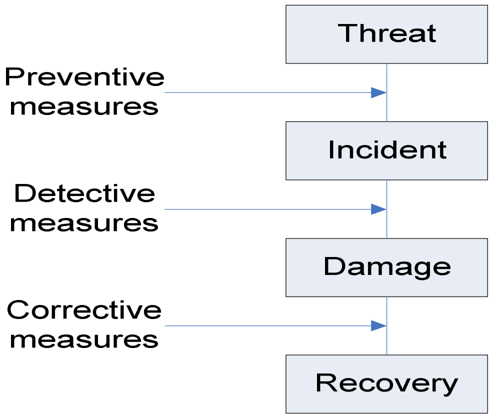


Figure 12 Measures (based on ISO 9000)

Figure 12 shows that the security measures must be put in place – first of all – to prevent a threat to become an incident. These are the so-called *preventive measures*. A simple example of preventive measure is safeguarding the area where the containers (with high value products) are stored by putting gates, high fences and surveillance camera's. This will make it more difficult for goods to be stolen from the containers.

When an incident occurs, the security measures must be put in place to minimize its damage. It should find the possible damage (e.g. to the SC). These are so-called *detective measure*. An example of detective measure is the (nuclear) scanning of containers. By scanning the containers, the possible dangerous goods that are put into containers (incident) will be detected. This will prevent an incident from causing damage (e.g. to the population of an area).

When an incident has resulted in damage, security measures must be put in place to correct the damage and recover the damaged SC. These are the so-called *corrective measures*. An example of a corrective measure is the presence of a Crisis Management Plan (*CMP*) [Slay J., Koronios A. (2006)]. CMP can be different per damage. For example if an empty container is stolen it will disrupt the SC process of the companies concerned. To recover this disruption, a new empty container must be brought in the SC and the search for stolen container must be started.

In the next sections, for each SCS measure it is also mentioned whether it is currently in place or it is an idea for the future from the authority's perspective.

4.2 Security measures

Based on exploratory research and field research the information analysis tool (mentioned in the previous chapter) is further developed. During a number of experts brainstorm sessions some idea's about the possible security measures for the threats that are defined in chapter 3 are proposed. The attendees of the expert brainstorm sessions reviewed each proposed security measure and presented their remarks and recommendations. These remarks and recommendations are used to further develop the eventual information analysis tool. The resulting security measures for import and export process are presented in section 4.2.1 Import and section 4.2.2 Export.

4.2.1 Import

After identifying the *most* important SCS threats and risks for container import process – as described in section 3.2.1 of chapter 3 – the possible measures (*Corrective*, *Detective and Corrective*) to deal with these threats and risks are defined. The measures are also characterized as currently in place or to be used in the future.

Table 7 shows an example of the measures that are identified. This table is an expansion on "Table 4 Most important import related threats and risks" from chapter 3. It also shows that for each possible threat and risk, there are one or more measures to be put in place. Table 7 shows only a part of the complete set of measures defined here. The complete table of measures is to be found in the appendix G.

Signals	Importance (Low Medium High)	Threats			Measures (p)reventive, (d)etective, (c)orrective, (cur)rent, (f)uture
		Terrorism	Theft	Smuggle	
The container vessel/ cargo is coming from a suspicious country/ port of origin or shipper	h	x		x	Handling the container vessel with exceptional care (Possible security allert) (p)
Vessel contains containers with explosive/chemical/dangerous material	h	x		x	Control at sea and routing the vessel to a pre-defined port (p)
Unauthorized people are or have been on board. Container is being tempered by people/personnel on board	h	x	x	x	Document control (authentication) (c) Check crew / passenger list (c) (p)
Unauthorized people are at the location. Container is being tampered by personnel	h	x	x	x	Access control (p) (d) (c)
Container is stolen	h	x	x		Verify person who picks up the container. Terminal proces & staff or automated (d) (c) Access control (p) (c) Physical security measures (gates, fences, cameras etc.) (p) (c) Tracking (d) (f) Motion detection (d) (f) Fences and Camera surveillance (c) (f) Background checks of personnel (Screening) (p) (c)
Container is not sealed	h	x	x	x	Container should be sealed after a risk analysis is conducted (possibly scanning the container to reduce the risk) (c) (cu)
Container contains goods to be smuggled	h	x		x	Check (electronic) seal status (d) (f) Verify person who delivers the container (d) (c) (cur) Random inspection at gate in (moment of descharge) (d) (f)
Container contains goods to be used in a terrorist attack (disruption of logistic process)	h	x		x	100% scanning of incoming containers with passive radiological scanning (d) (f) Checking of previous scan results (d) (f) Verify person who delivers the container (d) (c) (cur) Random inspection at the gate entrance (d) (f)
Contents of container is stolen	h	x	x		Motion detection inside container (d) (f) Motion detection compound (d) (c) Light sensors inside the containers (d) (f) Camera surveillance (c) (f) Access control (p) (c) Tracking of individual packaged goods (d) (f) Closing and sealing container (p) (c)
Illegal material is put in the container	h	x		x	Random checks (d) (f) + measures 1,2,3,4 and 6 from previous threat
Fake seal is used	h	x	x	x	Verify the seal number (p)(c)

Table 7: Security measures (Import)

4.2.2 Export

Same procedure of SCS measures identification as used for the container import process is also used for container export process. After identifying the *most* important SCS threats and risks for container export process – as described in section 3.2.2 of chapter 3 – the possible measures (*Corrective*, *Detective and Corrective*) to deal with these threats and risks are defined here. The measures are also characterized as currently in place or to be used in the future.

Table 8 shows an example of the measures that are identified. This table shows an expansion on “Table 5 Most important export related threats and risks” from chapter 3. It also shows that for each possible threat and risk, there are one or more measures to be put in place. Table 8 shows only a part of the complete set of measures defined here. The complete table of measures is to be found in the appendix H.

		Threats			
Signals	Importance (Low Medium High)	Terrorism	Theft	Smuggle	Measures (p)reventive, (d)etective, (c)orrective, (cur)rent, (f)uture
Container not empty, contains goods to be smuggled	h	x		x	Random inspection before leaving depot (d) (f) Weight comparison (d) (f) Assigning of containers to jobs should be done randomly (this ensures that people that want to smuggle goods are never sure where a certain container is going. This reduces the attractiveness of stuffing an empty container) (p) (c) Check information system (d) (f)
Container not empty, contains goods used in terrorist attack	h	x		x	Inspection (p) (c) + measures of previous threat
Illegal material is put into container	h	x		x	Locking container (p) (c) Motion detection inside container (d) (f) Inspection at POS (d) (f?)
Illegal material is packaged	h	x		x	Random checks (d) (f) Access control (p) (f?)
Material packaged for terrorist attack	h	x		x	Random checks (d) (f) Access control (p) (f?)
Packaged goods are goods to be smuggled or can be used in a terrorist attack	h	x		x	Random checks (d) (f) Access control (p) (f?) Scan the packaged goods (d) (f)
Packaged goods are exchanged for illegal goods (e.g. by the loading personnel at POS)	h	x		x	Truck driver checks if all goods are present (d) (c?) Contents of container is scanned when container is closed (d) (f) Access control (p) (f?) Camera surveillance (c) (f?)
Packaged goods are stolen during loading of the container	h	x	x		Weight comparison (d) (f) Truck driver checks if all goods are present (d) (c?) Contents of container is scanned when container is closed (d) (f) Access control (p) (f?) Camera surveillance (c) (f?)
Packaged goods are stolen by the truck driver	h	x	x		Verify person who is delivering the empty container and the person driving away with the loaded container (not necessarily the same person) (d) (c)

Table 8: Security measures (Export)

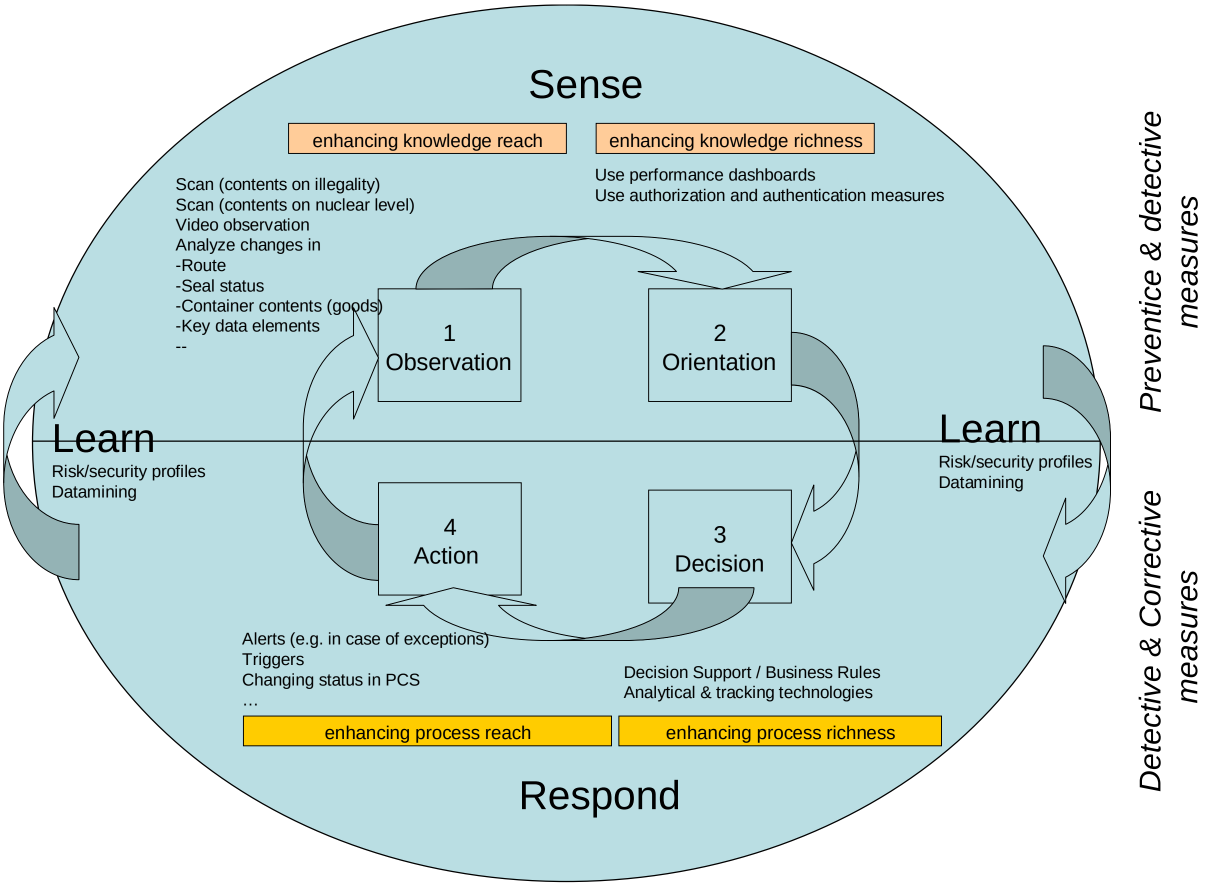
As mentioned earlier, the SCS measures for container import and export process, shown above, are only to deal with the SCS threats and risks. There also other security measures that are also identified but they are of a less urgent but they are also important and will contribute to enhancing the overall SCS security. This means that whether a certain SCS measure is selected to be used in practice or not, will depend on its level of importance for the SCS and also its level of coverage of CIA requirements.

By giving a classification (e.g. high, medium and low) that expresses how important the signals (threats) are for this particular case. This roughly allows selecting security measures by their strength. The classification will also give a rough indication how much money one wants to spend, which also helps in selecting the security measures further on [Goedhart, E.J., (2001)].

The SCS measures that are identified in this thesis are certainly not all the possible security measures that can be defined. Because of the dynamic character of SC and the changing requirements from the SC actors, new measures are

4.3 Sense and respond model

It is very important for the SCS measures not only to be preventive (sense), detective and corrective (respond) but they should also have a learning effect. This means that the measures must also enhance the knowledge and awareness of the SCS threats and risks among the SC parties. This will help prevent a certain threat or risk from repeating itself. In figure 13 the sense and respond model is presented. This model is usually used Information System Architecture (ISA) related projects for the SCS but – to a certain degree – it also fits in the context of SCS measures.


Sense
enhancing knowledge reach
enhancing knowledge richness
Scan (contents on illegality)
Scan (contents on nuclear level)
Video observation
Analyze changes in
-Route
-Seal status
-Container contents (goods)
-Key data elements
--
Use performance dashboards
Use authorization and authentication measures
1 Observation
2 Orientation
3 Decision
4 Action
Learn
Risk/security profiles
Datamining
Learn
Risk/security profiles
Datamining
Alerts (e.g. in case of exceptions)
Triggers
Changing status in PCS
…
Decision Support / Business Rules
Analytical & tracking technologies
enhancing process reach
enhancing process richness
Respond
Preventice & detective measures
Detective & Corrective measures

Adapted from Dove (2001), Canter (2000), Overby et al (2005)

Figure 13 Sense and respond model (Oosterhout 2006)

The idea behind the sense and respond model is that the implementation of different technologies and ICT initiatives for the SCS, all together form a part of the sense-respond-learn model. The main results of this could be that the SC will become safer.

4.3.1 Sense and respond model in the context of the SCS measures

In this section, the sense and respond model is briefly brought to attention. This model is not discussed in details because it is a model that is mostly used for ISA projects that are related to the SCS and this is why it is not fully applicable in the context of SCS measures. Nevertheless, it can be very useful to clarify the significance of the learning characteristics of the SCS measures. These characteristics are described by providing some clear examples.

When a threat is predicted or noticed (the sense part of the model), then the security measures are defined to detect and rather prevent from this threat to result in an incident (the respond part of de model). For example the “sense” is that when a “Container is from a suspicious country of origin” this could be a sign to predict SCS threats and risks. The respond to this sense is to stack the container at a separate location in order to prevent or minimize the possible damage and to send the container to a (nuclear) scan facility to be scanned for the possibility of nuclear, chemical, explosive or other kind of dangerous goods being inside the container. Or to send the container to a special location where it can be physically checked for possible smuggled goods (e.g. drugs).

The other way around is also possible. When a container is coming from a “safe” country of origin, and after a few random inspections, it appears to be not a safe country of origin because the containers are regularly misused (for smuggle or contents of the container are stolen) then this can be detected by e.g. the data mining techniques. Eventually this country can be removed from the list of “safe countries of origin” and be added to the list of suspicious countries of origin.

These examples have shown the “sense” and “respond” part of the model. The learning part of the model is an area between these two parts. By using different techniques – e.g. the data mining techniques as described or the profiling technique which grants statuses to containers based on their history, country of origin, security certifications etc. – improves the SC visibility. This could contribute to learning how to better and timely prevent, detect and correct a certain threat from according and minimize the possible damage.

4.4 Conclusion

In this chapter, the SCS measures are identified. The SCS measures can be either physical technological security measures (e.g., installing GPS systems “track and trance system” on the trucks in order to be able to follow the containers) or non-physical organizational security measures (e.g. redesigning the business processes) or a combination of both. The security measures are classified as being preventive, detective or corrective. Also whether a SCS measure is currently available (in use) or is it a SCS measure for the future.

The SCS measures related to the threats and risks identified in chapter 3 – have been presented during the experts brainstorm sessions. It became clear that there are one or more measures for each threat and risk (taking in account the preventive, detective and corrective nature of the measures). Which SCS measures could be selected is depending on their importance and also depending on their coverage of the CIA requirements.

The sense and respond model is briefly brought to attention. This model is not discussed in details because it is mostly used for ISA projects that are related to SCS. This means that it is not fully applicable in the context of SCS measures. Nevertheless, some examples are described which shows that this model can be very useful to clarify the significance of the learning characteristics of the SCS measures.

A general idea is that the best measure is to keep the containers and goods moving. Container and goods in motion reduces security risk because they are practically less easy to access and this contributes to reduce their vulnerability.

As mentioned earlier, this chapter has only identified the possible SCS measures. To implement these SCS measures, SCS relevant information is required. This issue is the subject of discussion in the next chapter (Chapter 5).

5 Information needs, availability and exchange for enhancing SCS and SC visibility

This chapter discusses the information needed to in order to apply the SCS measures as defined in the previous chapter (Chapter 4), it provides an overview of the total amount of information that is available and which information is currently being exchanged among the SC parties and what could be exchanged in the future in order to enhance the SCS and improve the SC visibility.

This chapter is outlined as follows: section 5.1 provides a general introduction to the topic of this chapter. Sections 5.2 describes the information that is needed in order to be able to implement the SCS measures defined in the chapter 4 for both container import and export processes. Section 5.3 discuses the level of information availability. It describes the total amount of information that is available and it also describes where the information is to be found. Finally, section 5.4 discusses the issue of information exchange among the SC parties. It shows which security relevant information is currently being exchanged among the SC parties and how could this information exchange be upgraded in order to enhance the SCS and improve the SC visibility. Also the information exchange gap is described.

5.1 Introduction

The SCS measures that are defined in previous chapter are of no use without the availability of the information that is needed for each of the measures. It should be made clear that there is a lot of data circling in the SC processes. Not all data available means information and not all the information is security relevant information. Whether an information element is security relevant or not depends on its nature, location, timing and importance. The last character (importance) is not necessarily the same for all SC parties. A security relevant information element can be of *high* importance for one party while for the other party it can be of *medium* or *low* importance. For example, the information regarding the TARRA of a container is of *high* importance for the customs and sea terminal because 500 kg’s more of less can be an indication of false content information. The difference in the TARRA of a container can be caused by smuggle of illegal or dangerous material instead of the goods mentioned on the pre-arrival or pre-departure list. The information about the TARRA of a container is of *low* to *medium* importance for a rail operator because 500 kg’s more or less will not much influence the business processes of a rail operator.

The security related information is only optimally uses for the SCS measures when it is available at the right place and at the right location and it must be reliable. The SC parties that are using each others information in order to start and/or finish their part of the import or export process must be 100 percent sure about the confidentiality, integrity and availability (CIA requirements) of the security relevant information, specially when the information is concerning the transport of nuclear, biological, chemical, explosive or other kind of dangerous and expensive martial and goods.

Not all of the SC parties have (all of) the security relevant information which is necessary in order to implement SCS measures, that could result in enhancing the SCS level and provide more visibility in the SC. But this can (only) be achieved when the SC parties better cooperate with each other and provide each other with the security information that is needed. In this thesis, this is called the information exchange among the SC parties. The level of cooperation and information exchange among the SC parties could provide an indication about the security level of the SC and they could be directly linked to each other. The level of cooperation or information exchange among the SC parties depends on the mutual trust (confidence) and (financial, organizational and/or process improvement) benefits and also depends on the requirements under which the parties are has come to a bilateral agreement.

5.2 Information needs

The SCS measures that are defined in chapter 4 require information in order to be implemented in practice. To find out what security relevant information is needed for each of these SCS measures, the information analyse system – that has been developed in the previous chapters – is further developed by adding a new column where the security relevant information needs for each SCS measure are mentioned. The security relevant information needs in this column is based on the field research and literature studies. After defining the information needs for each SCS measure, it is presented during the expert brainstorm sessions and based on the comments and suggestions from the experts, the security relevant information needs are further improved. The security relevant information needs are also based on the nature of the SCS measure (*preventive*, *detective*, *corrective*, *current* and *future*) and it is also depending on whether it is concerning a container import or export process. The lists of information needs are also presented during the workshop. This workshop also helped to further improve the security relevant information needs. It is very likely that the final lists of security relevant information needs can be different if more SC parties are involved in validating these lists, but so far the final lists of the security relevant information needs for import and export are defined as presented in appendix G for import and appendix H for export.

Table 9 provides an overview of a part of the security relevant information needs for container import process that is defied using the information analyse system.

		Threats				
Signals	Importance (Low Medium High)	Terrorism	Theft	Smuggle	Measures (p)reventive, (d)etective, (c)orrective, (cur)rent, (f)uture	Information needs
The container vessel/ cargo is coming from a suspicious country/ port of origin or shipper	h	x		x	Handling the container vessel with exceptional care (Possible security allert) (p)	- the country of departure - the history of country of departure - date of departure - date of (expected) arrival - complete route description - complete and detailed list of all BLs
Vessel contains containers with explosive/chemical/dangerous material	h	x		x	Control at sea and routing the vessel to a pre-defined port (p)	- total number of containers on board - type of material on board - sender of the container - beneficiary of the container
Unauthorized people are or have been on board. Container is being tempered by people/personnel on board	h	x	x	x	Document control (authentication) (c)	- pre-arrival information - number of people on board - nationalities/status
					Check crew / passenger list (c) (p)	- identity - nationality - how & when he/she got on board
Unauthorized people are at the location. Container is being tampered by personnel	h	x	x	x	Access control (p) (d) (c)	- access badges - validation - company he/she working for - known/unknown
Container is stolen	h	x	x		Verify person who picks up the container. Terminal proces & staff or automated (d) (c)	- identity of person/company who is picking up the container - genuine container pickup message
					Access control (p) (c)	- list of authorized personnel
					Physical security measures (gates, fences, cameras etc.) (p) (c)	- certification information - compliances
					Tracking (d) (f)	- location information (actual/supposed)
					Motion detection (d) (f)	- motion information (actual/supposed)
					Fences and Camera surveillance (c) (f)	- status information - begin and end time of storage - archive of footage
					Background checks of personnel (Screening) (p) (c)	- check in and check out time employees - date of last (updated) background check)

Table 9: Information needs (Import)

Table 10 provides an overview of a part of the security relevant information needs for container export process that are defied by using the information analyses tool.

		Threats				
Signals	Importance (Low Medium High)	Terrorism	Theft	Smuggle	Measures (p)reventive, (d)etective, (c)orrective, (cur)rent, (f)uture	Information needs
Container not empty, contains goods to be smuggled	h	x		x	Random inspection before leaving depot (d) (f)	- previous user container - risk profile users
					Weight comparison (d) (f)	- weight of container - actual weight of container
					Assigning of containers to jobs should be done randomly (this ensures that people that want to smuggle goods are never sure where a certain container is going. This reduces the attractiveness of stuffing an empty container) (p) (c)	- pool of available containers - pool of containers that can be used for the job (e.g. containers from a certain company)
					Check information system (d) (f)	- last inspection time - content - open/close time container
Container not empty, contains goods used in terrorist attack	h	x		x	Inspection (p) (c) + measures of previous threat	- suspected containers for "terrorist material" - last inspection time - content - open/close time container - weight of container
Illegal material is put into container	h	x		x	Locking container (p) (c)	- seal present - status information
					Motion detection inside container (d) (f)	- motion information interior actual - status information
					Inspection at POS (d) (f?)	- last inspection time - content - open/close time container - weight of container
Illegal material is packaged	h	x		x	Random checks (d) (f)	- administration of incidents - certification - weight information for comparison
					Access control (p) (f?)	- list of authorized personnel
Material packaged for terrorist attack	h	x		x	Random checks (d) (f)	- administration of incidents - certification - weight information for comparison
					Access control (p) (f?)	- list of authorized personnel

Table 10: Information needs (Export)

5.3 Information blocks and availability

This section of chapter 5 examines the issue of availability of the security relevant information in the SC. After defining the security relevant information needs, it is important to know whether the information exists or not. If yes, then where and how is this information to be founded.

5.3.1 Information blocks

In order to improve the visibility of the total amount of the security relevant information that is needed, the information that is defined in the previous section of this chapter is divided in “Information blocks”. The “information blocks” accumulates all the information elements and information options that are related to a certain information category. In this thesis by information categories is meant the information blocks. For this issue a top-down model is used.

In the top-down model an overview of the system is formulated, without going into detail for any part of it. Each part of the system is then refined by designing it in more detail. Each new part may then be refined again, defining it in yet more detail until the entire specification is detailed enough to validate the model [http://en.wikipedia.org]

Definition 9: Top-down model

This means first, a number of information blocks are defined which are related to the SC processes (both import and export). Then, these information blocks are furthers specified by defining the data elements that are related to each information block. Each data element has one or more options, that's why the data elements are further specified by defining the possible options and value of each data element. These information blocks are presented during the expert brainstorm sessions and they are detailed discussed and improved based on the comments and recommendations from the experts. All the information blocks are also presented and discussed during the field research except the highlighted ones. These are recommended by the experts during the expert sessions and added afterwards.

Table 11 provides an overview of the total number of information blocks defined in this thesis.

#	Category
1	Container (general)
2	Seal
3	Nuclear scan
4	X Ray scanning (container contents)
5	Operators (general)
6A	Road operator
6B	Truck details
6C	Truck driver details
7A	Rail operator
7B	Train details
8A	Barge operator
8B	Barge details
9	Shipping line/ship details
10	Personnel
11	Point of stuffing (STUF) or point of stripping (STRIP)
12	Cargo
13	Process information on timing STUF/STRIP
14	Process information on timing inland terminal
15	Process information on timing sea terminal
16	Process information on timing container vessel
17	Consignor (shipper)
18	Consignee (final recipient)
19	Ports
20	Sea terminal
21	Incidents

Table 11: Information Blocks

Description of the information blocks:

- Container (general) – this information block contains data elements about the container like the container number and the container status and some other container related data elements.
- Seal – this information block contains data elements about the seal that is used for the container. Examples of possible data elements are the location of sealing, the seal status and the seal number.
- Nuclear scan (detection) – in this information block information about the nuclear scan of the container is stored. Every container that is transferred by rail or road is scanned by the nuclear detection ports.
- Scanning or inspection (container contents) – information about the scanning or inspection of the container contents or the container in general is contained within this information block. Data elements within this block are, for example, the container scan type and the container scan results. These scans and inspections include both X-ray scanning and physical inspection by Customs, VWA or PD.
- Operators – this information block contains information about the operators that handled a specific container. This block contains information about the operator (contact information) and whether the operator is certified or not. For specific types of operators,

information that is more detailed may be stored to meet specific information needs. This information block is further specified and divided into Road operator, Rail operator and Barge operator.

- Ship details – this information block contains data elements about the ship that was used to transport certain containers.
- Personnel – this information block contains information about the employees of the different SC actors that are directly involved in the physical and non-physical SC processes. Data elements within this block are personnel ID and organization which are used for example to grant access rights in pre-defined areas.
- Point of stuffing (STUF) or point of stripping (STRIP) - this information block contains information about the location where the goods are being loaded into the container or the goods are unloaded from the container.
- Cargo – in this information block, data elements regarding the cargo inside of the container are stored. This information includes, for example, the bill of lading (B/L) number, the cargo value, a cargo description and cargo weight.
- Process information on timing – the timing details (STUF/STRIP, inland terminal, sea terminal, and arrival and time of departure of container vessel) of the container in the different SC processes is contained within this information block.
- Consignor (shipper) – this information block contains information about the shipper (sender) of a container. This information includes the Consignor ID to identify the shipper and Consignor certificate details. This is for the future use in order to know how reliable a certain shipper is.
- Consignee (final recipient) – this information block contains information about the final recipient (final receiver) of a container. This information includes the Consignee ID to identify the recipient and Consignee certificate details. This is for the future use in order to know how reliable a certain recipient is.
- Port information – this information block contains information about the port(s) that were passed by the container. This information includes some general port information (name, country etc.) and the port security level and the sea terminal through which the container is transported.
- Incidents – in this final information block, data elements about incidents concerning the container transport are stored. This information includes an incident description and an incident location [Meijer (2007)].

This method resulted in very detailed specification of data. Not all of the data elements and data options are relevant and necessary for enhancing SCS. Some data elements and data options are more important compare to the others. To distinguish this, more data characteristics are added. The additional characteristics are *Mandatory*, *Preferable* and *Importance*. These data characteristics specify whether a certain data element or data option is *mandatory* (e.g. the information regarding quality check of a cargo is required by authorities such as customs. This means that this data element is mandatory) or *preferable* (e.g. the information regarding the organization that has conducted the quality check on the cargo is not very important to know but its good to be somewhere accessible when needed. This means that this data element is preferable). Also the *importance* (High, Medium and Low) in the context of security threats of each data element or data options/value is defined (e.g. the information regarding the dangerous goods in the cargo is not only important for the authorities to know but it also has a high probability to be misused and cause security threat). By adding these characteristics to the data elements and data options, only the most important information can be "filtered" and the volume of the data can be limited. To better understand this method, the category "Container (general)" is shown in table 12 as example. The full analysis is to be found in appendix I.

				Characteristics of Data		
#	Category	Data element	Options / values	Mandatory	Prefer	Importance (Low, Medium, High)
1	Container (general)	container number		x		h
		booking number				
		container status	Empty (yes/no/residue)	x		
			Clean (yes/no)	x		
			Sealed (yes/no)	x		h
			Controlled (yes/no)		x	
			Controlled for		x	
			Controlled by		x	
			Damaged (yes/no)		x	
			Nuclear scanned (yes/no)	x		h
		container owner			x	
		ISO code	size.type	x		
		RFID tag (only for smart containers)	Yes/No/Active/Passive		x	
		scanned	Yes/No	x		h
		gassing	Gassed/degassed	x		
		gas-description		x		
		TARRA		x		h
		container integrity	Ok / not OK		x	h
		temperature changes	Yes/No		x	
		intrusion	Yes/No		x	
		light changes	Yes/No		x	

Table 12: Detailed information blocks

At this stage the information needs are more detailed described in the form of information blocks and related data elements and data options/values. But it is still not clear when and at which part of the SC are these information elements checked, at which moment in the SC are these information elements needed and on which means (documents) are these information elements to be found. It is also important to know in which (business) information systems are these information elements to be found and whether these data elements and data options/values are electronic available or not. Examples of these (business) information systems are the *Port Community System (PCS)*, *Container Integrity System (CIS)*, *Authority Systems (Customs, Port Authorities)*, and *Business (Community) Systems (BCS)*. A short description of these systems is provided below. More detailed description of these systems is to be found in Meijer (2007).

1. *Port community system* is an entity delivering information to supply chains operating in the port. The port community system is responsible for: data supply, data control, data distribution and data conversion (e.g. Port infolink);

2. *Container Integrity Systems* are used to monitor the integrity of the container, which means that these systems supply information whether the container has or has not been opened;

3. *Authority systems* are information systems or set of information systems that are used by authorities for numerous reasons. The main users of these systems are the customs and the seaport police;

4. *Business (community) systems* are the remaining category of information systems of the individual SC companies and the community systems set up by groups of SC companies systems (e.g. Forwarder systems, Shipping line systems, Terminal systems).

The information analyse system as mentioned in the previous chapters is now extended and this extended with the detailed specified information blocks and information characteristics as mentioned above. The findings from the field research are processed in this version of the information analyse system and it is presented during the experts brainstorm sessions and during the workshop. The comments and recommendations from the experts brainstorm sessions and the workshop is processed and the analysis system is also sent to all of the attendees of the workshop to be checked spartanly. The results are the following tables:

By selecting the elements and options with the *high* importance level, a selection of information can be provided which is needed for implementing the SCS measures. Table 13 provides an overview of a small part of this information. A complete version of this table is to be found in appendix J.

#	Category	Data element	Options / values	Characteristics of Data Mandatory	 Prefer	 Importance (Low, Medium, High)
1	Container (general)	container number		x		h
		container status	Sealed (yes/no)	x		h
			Nuclear scanned (yes/no)	x		h
		scanned	Yes/No	x		h
		TARRA		x		h
		container integrity	Ok / not OK	x		h
2	Seal	seal number		x		h
		location of sealing		x		h
		time of sealing			x	h
		sealed by	Consignor / Operator / Authority	x		h
		seal status/integrity	Ok / broken / damaged	x		h
			Broken	x		h
			Damaged	x		h
			Change history	x		h
3	Nuclear scan	location of scan	seaterminal, inland terminal etc	x		h
		results of scan	Ok / Not Ok	x		h
4	X Ray scanning (container contents)	container scan results	ok, not analyzed / ok, analyzed, not OK	x		h
5	Operators (general)	operator ID		x		h
		operator certificate details	Date/time of issue		x (future)	h
			Issuing authority		x (future)	h
			Valid utill		x (future)	h
6A	Road operator	operator ID		x		h
6C	Truck driver details	driver ID		x		h
7A	Rail operator	operator ID		x		h
7B	Train details	train ID/number		x		h

Table 13: Detailed information blocks with high importance

As this table a show, a data element or option/value which is of high security importance doesn't always needs to be characterizes as *mandatory*. A data element of option/value can also be characterized as *preferable* and still be of high security importance.

The Entity Relation diagram (ER) in figure 14 visualizes and helps understand the relation between the different information blocks and their data elements that are defined in the information analyse system of this research. The information blocks are denoted by the rectangles and the relationships are represented by the diamond shapes. For every relationship, the granularity is defined which means that, for example, for the booking-operator relationship several operators can handle a single booking or that an operator can handle different bookings. The different granularities are 1:N and N:M. 1:N means that one instance of an information block (entity) can have a relation with several instances of the second information block. The instance of the second information block, however, only has one instance of the first information block associated with it. The granularity N:M means that both entities can have several instances of the other entity associated with it. The values contained within the information blocks are depicted by the ovals. This figure represents the complete set of information that is identified to be relevant for SCS by the actors in the SC and by domain experts [Meijer (2007)].

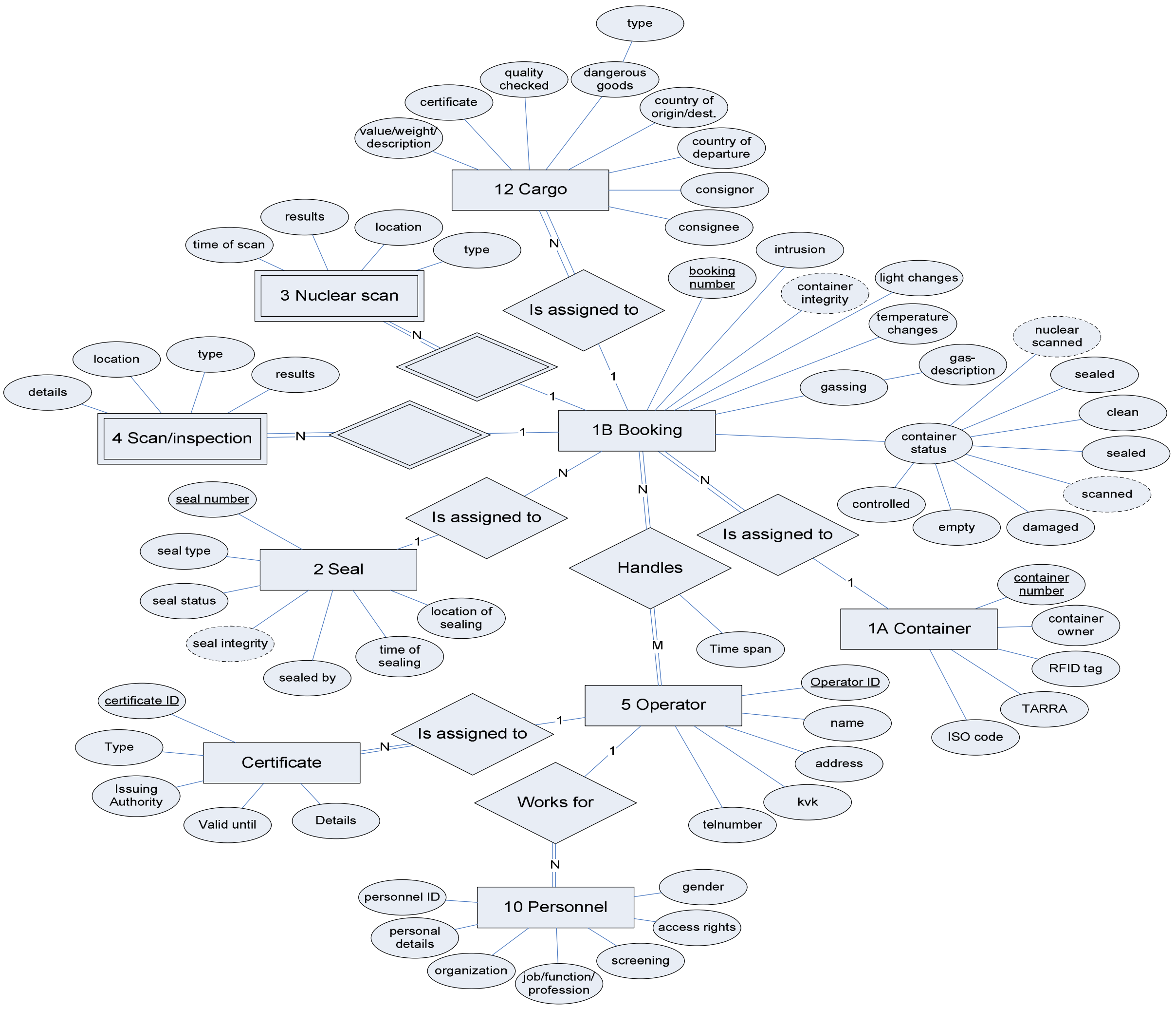


Figure 14 Entity Relation diagram for SCS relevant information

The information block “5 Operator” is more complicated and that is why it needs additional explanation as it is provided by figures 15 and 16. All the operators have the same data elements as the operator but have additional data elements specific to their function in the SC.

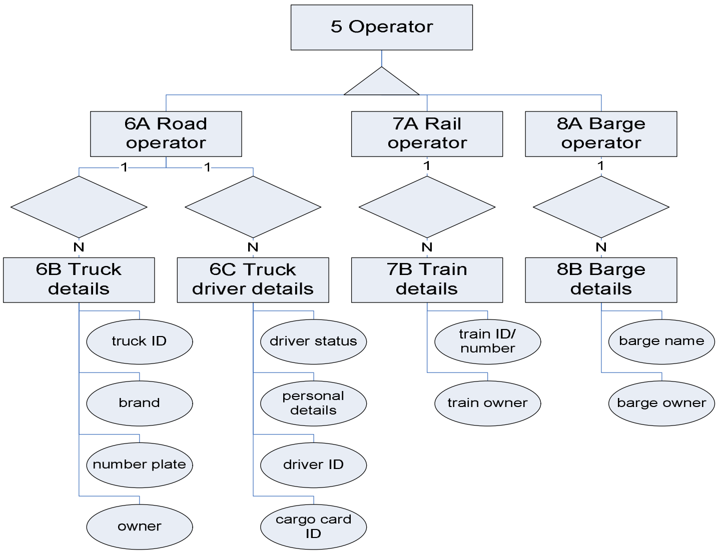


Figure 15 Entity Relation diagram for pre- and on-carrier

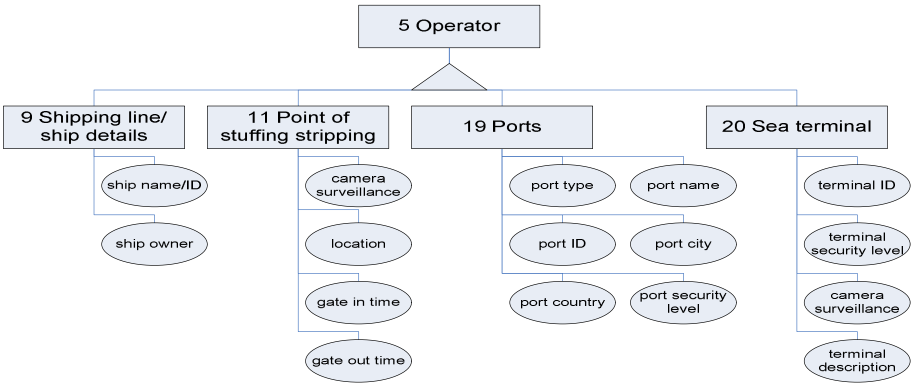


Figure 16 Entity Relation diagram for the remaining physical groups

5.3.2 Information availability

As shown in appendix I and appendix J, a lot of security relevant information is available. The information is in different systems and at different SC actors. It is not organized and exchanged efficiently to cover all of the possible SCS risks and threats. Table 14 shows the percentage of the total security relevant information availability and its place.

Import					Export				
PCS	Container Integrity System	Authority Systems (Customs, Port Authorities)	Business (Community) Systems	Electronic Availability	PCS	Container Integrity System	Authority Systems (Customs, Port Authorities)	Business (Community) Systems	Electronic Availability
64%	16%	55%	44%	82%	64%	16%	54%	33%	82%

Table 14: Percentage of total information availability (Import & Export)

Table 14 shows, 64% of the data elements are available in the PCS's (including availability in the future). CIS's have 16% of the data elements. Authority System's have 55% of the data elements and BCS's have 44% of the data elements. Overall 81% of the total data elements are electronic available.

Table 15 shows the availability of the security relevant information, which is characterized as being highly important for the SCS. It shows where this information is to be found and whether it is electronic available or not.

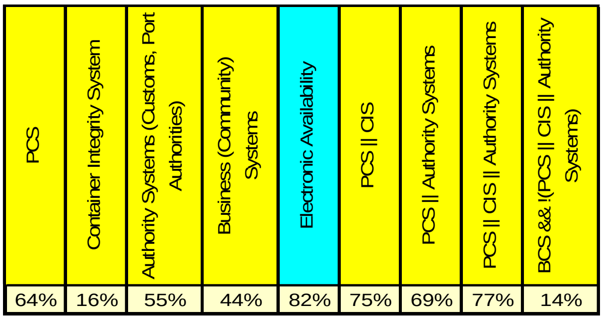
Import					Export				
PCS	Container Integrity System	Authority Systems (Customs, Port Authorities)	Business (Community) Systems	Electronic Availability	PCS	Container Integrity System	Authority Systems (Customs, Port Authorities)	Business (Community) Systems	Electronic Availability
79%	25%	63%	42%	91%	79%	25%	62%	33%	91%

Table 15: Percentage of high importance information availability (Import & Export)

Table 15 shows, 79% of the data elements are available in the PCS's (including availability in the future). CIS's have 25% of the data elements. Authority System's have 63% of the data elements and BCS's have 42% of the data elements. Overall 91% of the total data elements – which are characterized as being highly important – are electronic available.

According to the above two tables, there are a lot of security relevant information available. The problem is that the information is not available in one system and not all of it is electronic available. By a well organized cooperation among the different (information) systems, a much higher level of SCS information availability can be achieved. The following tables show the results of the level of SCS relevant information availability after linking different systems together. In the tables '&&' means 'and', '||' means 'or' and '!' means 'not'. 'PCS && Authority System' can thus be read as: 'information that is available in the Port Community System and the Authority System'.

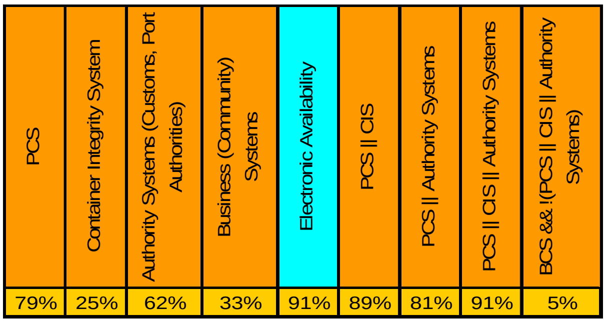
Table 16 and 17 shows some examples of linking the different information systems together and their results for obtaining the degree of coverage of the data elements.



PCS	Container Integrity System	Authority Systems (Customs, Port Authorities)	Business (Community) Systems	Electronic Availability	PCS || CIS	PCS || Authority Systems	PCS || CIS || Authority Systems	BCS && !(PCS || CIS || Authority Systems)
64%	16%	55%	44%	82%	75%	69%	77%	14%

Table 16: Degree of coverage of all information (Import & Export)

Table 16 shows the degree of coverage of all the SCS relevant information – for both export and export – that can be obtained by linking the "Port Community Systems" and "Container Integrity System" to each other the level of coverage could be up to 75%. By linking the "Container Integrity Systems" and "Authority Systems" to each other the level of coverage could be up to 69% and by linking the "Port Community Systems", "Container Integrity Systems" and "Authority Systems" to each other the level of coverage could be up to 77%. By combining all the systems together the level of coverage of 91% (77% + 14%) could be reached. The remaining 9% of the data elements are not electronically available in any of the information systems according to the information analyse system developed for this research.



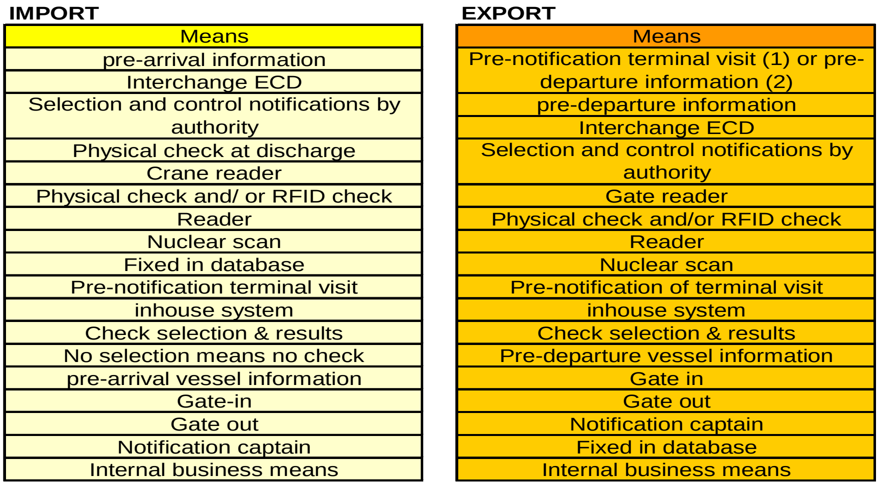
PCS	Container Integrity System	Authority Systems (Customs, Port Authorities)	Business (Community) Systems	Electronic Availability	PCS || CIS	PCS || Authority Systems	PCS || CIS || Authority Systems	BCS && !(PCS || CIS || Authority Systems)
79%	25%	62%	33%	91%	89%	81%	91%	5%

Table 17: Degree of coverage of information of high importance (Import & export)

Table 17 shows the degree of coverage of the information which is characterized as being highly important for the SCS– for both export and export – that can be obtained by linking the "Port Community Systems" and "Container Integrity System" to each other the level of coverage could be up to 89%. By linking the "Container Integrity Systems" and "Authority Systems" to each other the level of coverage could be up to 81% and by linking the "Port Community Systems", "Container Integrity Systems" and "Authority Systems" to each other the level of coverage could be up to 91%. By combining all the systems together the level of coverage of 96% (91% + 5%) could be reached. The remaining 4% of the data elements are not electronically available in any of the information systems according to the information analyse system developed for this research.

5.4 Information exchange

The previous section explained that there is a lot of SCS relevant information available but in different information systems and by linking different systems together, overall a higher level of SCS relevant information availability can be achieved. The next question is "how these systems could be linked to each other?" There are different possibilities to do this. A detailed scenario based approach answer to this question is defined in Meijer (2007) where three different scenario's of data exchange is explained. But one of the ways to exchange information among the different SC actors is by using the current information exchange means. Based on the literature study, field research and the recommendations from the experts brainstorm sessions a list of means is developed (table 18) by which the information is currently exchanged among the SC actors.



IMPORT

Means
pre-arrival information
Interchange ECD
Selection and control notifications by authority
Physical check at discharge
Crane reader
Physical check and/ or RFID check
Reader
Nuclear scan
Fixed in database
Pre-notification terminal visit
inhouse system
Check selection & results
No selection means no check
pre-arrival vessel information
Gate-in
Gate out
Notification captain
Internal business means

EXPORT

Means
Pre-notification terminal visit (1) or pre-departure information (2)
pre-departure information
Interchange ECD
Selection and control notifications by authority
Gate reader
Physical check and/or RFID check
Reader
Nuclear scan
Pre-notification of terminal visit
inhouse system
Check selection & results
Pre-departure vessel information
Gate in
Gate out
Notification captain
Fixed in database
Internal business means

Table 18: Information exchange means

These are the information exchange means that are currently being used for exchanging information among the different SC actors. Either the contents of these information exchange means can be changed or new information exchange means can be developed in order to achieve a higher level of SCS relevant information exchange. The next two sections describe which information is exchanged currently and which information exchange means is used for it. Also the future (desirable) information exchange is described.

5.4.1 Current information exchange

In order to get a better view of the current state of the data exchange among the SC actors, a matrix is developed where all the SC actors are mentioned and this matrix is presented during the experts brainstorm sessions. According to the data collected during the field research and provided by the attendees of the experts brainstorm sessions (e.g. Port infolink), the current state of information exchange is as follows:

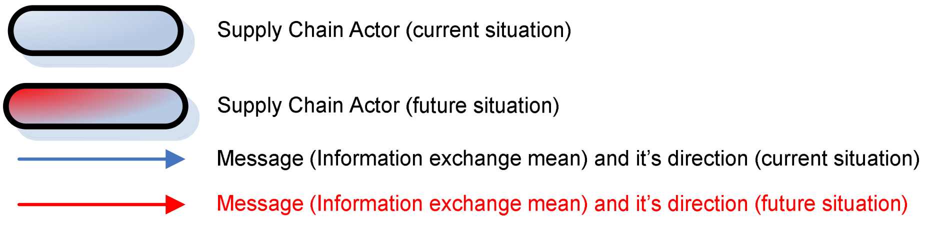

Supply Chain Actor (current situation)
Supply Chain Actor (future situation)
Message (Information exchange mean) and it's direction (current situation)
Message (Information exchange mean) and it's direction (future situation)

Figure 17 Notations used in chapter 5

A light blue "oval" is used to denote the SC actor which is currently involved in information exchange. A light blue/red "oval" is used to denote the future SC actors added to the SC actors which are currently involved in information exchange. A light blue line arrow is used to denote the message (information) exchange means and the direction of the information (from actor – to actor) for the current information exchange in place. A red line arrow is used to denote the message (information) exchange means and the direction of the information (from actor – to actor) for the future (desirable) information exchange possibility.

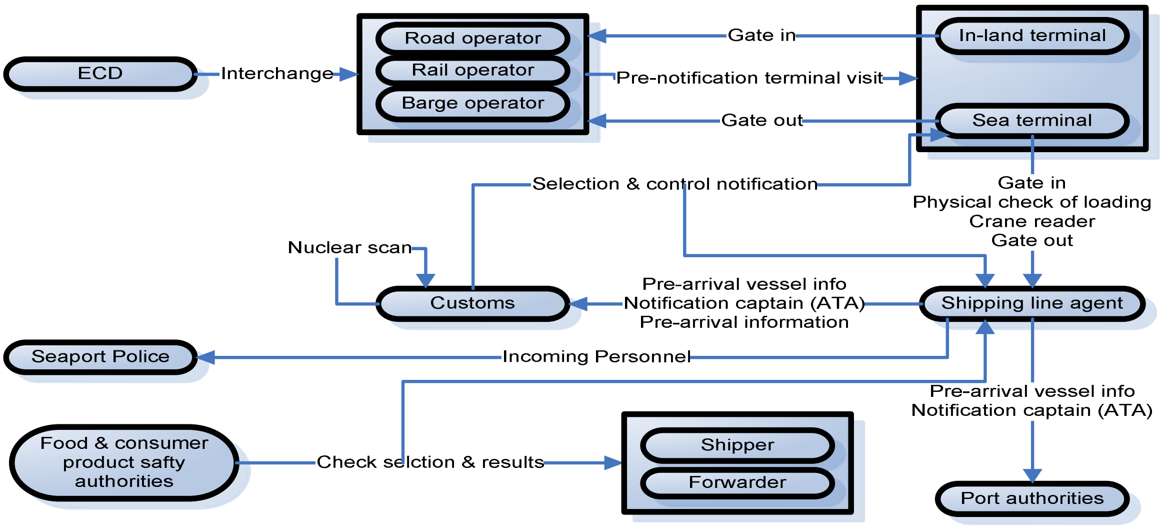


Figure 18 Current information exchange scheme (import)

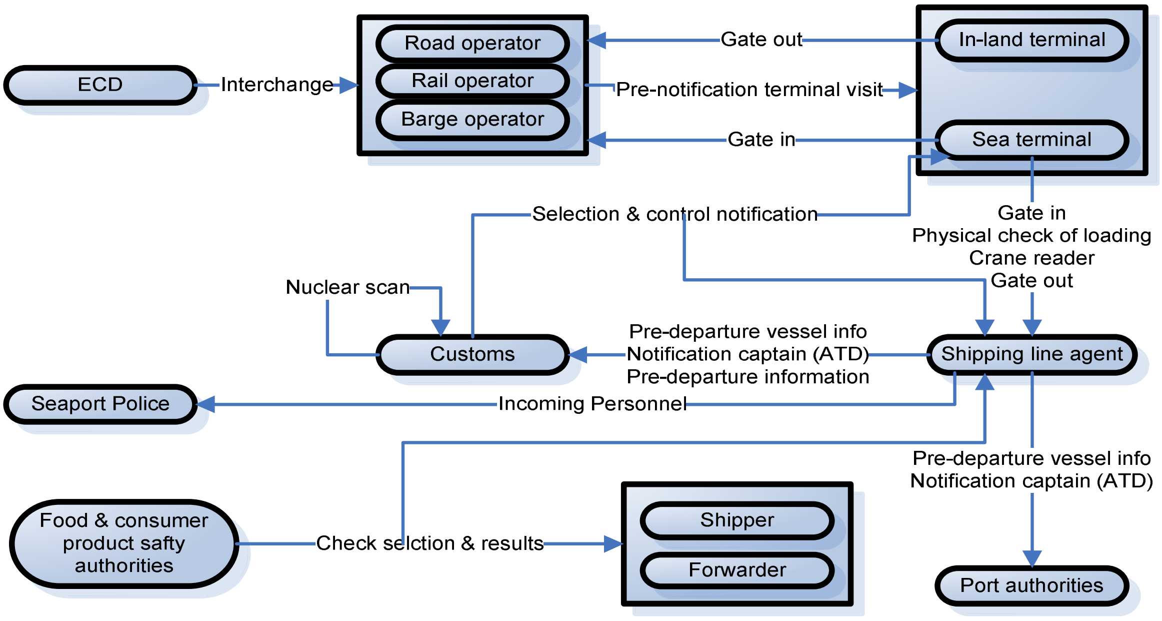

ECD
Interchange
Road operator
Rail operator
Barge operator
Gate out
Pre-notification terminal visit
Gate in
In-land terminal
Sea terminal
Selection & control notification
Gate in
Physical check of loading
Crane reader
Gate out
Nuclear scan
Customs
Pre-departure vessel info
Notification captain (ATD)
Pre-departure information
Shipping line agent
Seaport Police
Incoming Personnel
Pre-departure vessel info
Notification captain (ATD)
Food & consumer product safty authorities
Check selction & results
Shipper
Forwarder
Port authorities

Figure 19 Current information exchange scheme (export)

In appendix K is an overview of the data elements that are exchanged by the information exchange means (messages) as shown by these two figures provided. The SC actors that are not sending or receiving any information (according to the data collected during the field research and provided by the experts) are not mentioned in these two figures.

5.4.2 Future (desirable) information exchange

A figure that explains the future or desirable SCS relevant information exchange scheme with all the information needs that are defined in the beginning of this chapter will not be easy to develop but the next two figures are providing a simplified example of such information exchange schemes. These schemes are developed based also on the findings

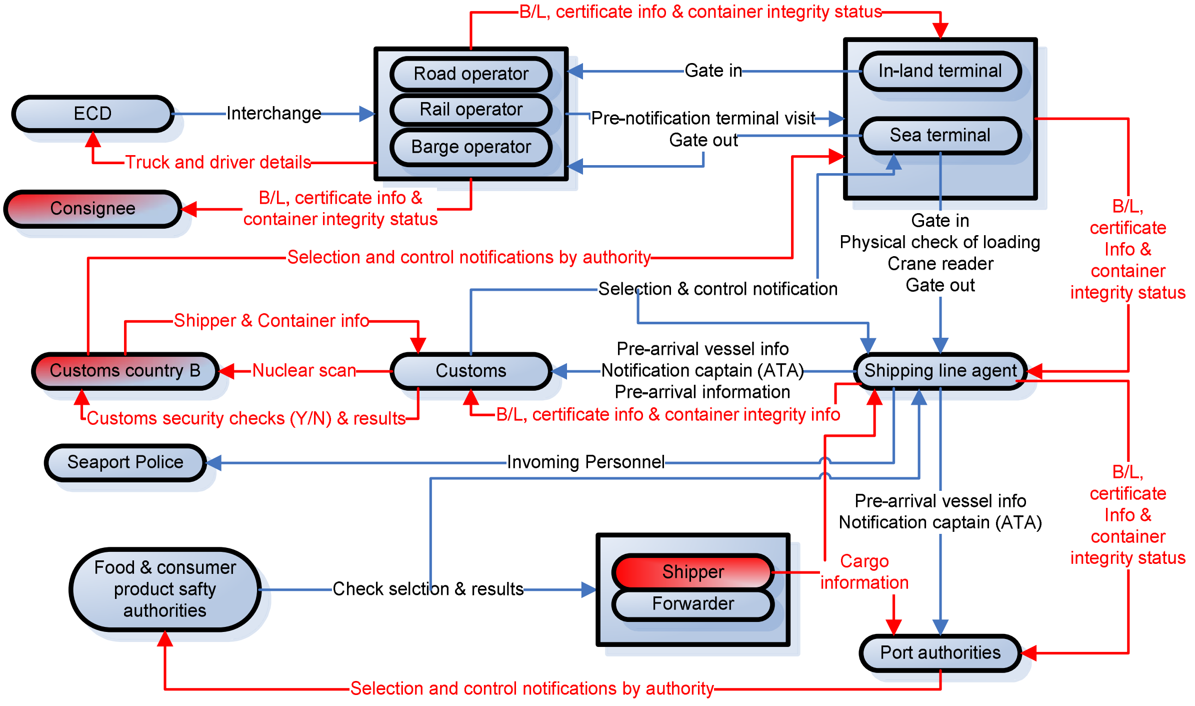

B/L, certificate info & container integrity status
Road operator
Rail operator
Barge operator
Gate in
In-land terminal
Sea terminal
ECD
Interchange
Pre-notification terminal visit
Gate out
Truck and driver details
Consignee
B/L, certificate info & container integrity status
Selection and control notifications by authority
Gate in
Physical check of loading
Crane reader
Gate out
B/L, certificate Info & container integrity status
Selection & control notification
Shipper & Container info
Customs country B
Nuclear scan
Customs
Pre-arrival vessel info
Notification captain (ATA)
Pre-arrival information
Shipping line agent
Customs security checks (Y/N) & results
B/L, certificate info & container integrity info
Seaport Police
Invoming Personnel
B/L, certificate Info & container integrity status
Pre-arrival vessel info
Notification captain (ATA)
Food & consumer product safty authorities
Check selction & results
Shipper
Forwarder
Cargo information
Port authorities
Selection and control notifications by authority

Figure 20 Future/desirable information exchange scheme (import)

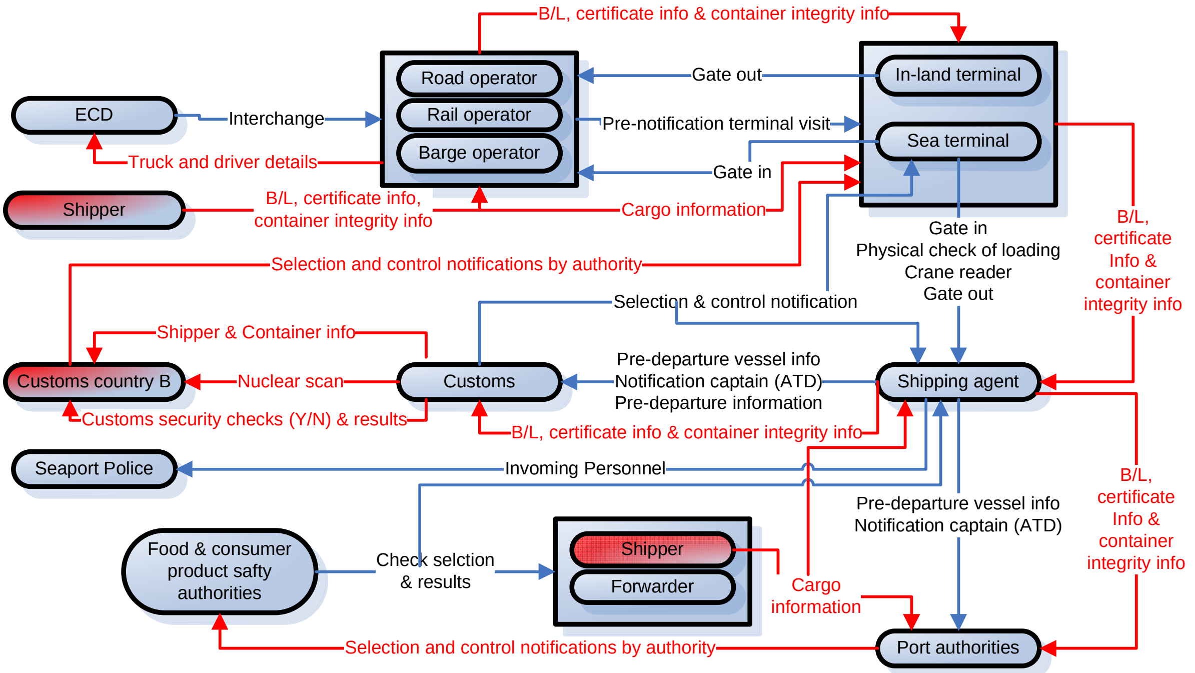

B/L, certificate info & container integrity info
Road operator
Rail operator
Barge operator
Gate out
In-land terminal
Sea terminal
ECD
Interchange
Pre-notification terminal visit
Truck and driver details
Gate in
Shipper
B/L, certificate info, container integrity info
Cargo information
Gate in
Physical check of loading
Crane reader
Gate out
B/L, certificate Info & container integrity info
Selection and control notifications by authority
Selection & control notification
Shipper & Container info
Customs country B
Nuclear scan
Customs
Pre-departure vessel info
Notification captain (ATD)
Pre-departure information
Shipping agent
Customs security checks (Y/N) & results
B/L, certificate info & container integrity info
Seaport Police
Invoming Personnel
B/L, certificate Info & container integrity info
Pre-departure vessel info
Notification captain (ATD)
Food & consumer product safty authorities
Check selction & results
Shipper
Forwarder
Cargo information
Port authorities
Selection and control notifications by authority

Figure 21 Future/desirable information exchange scheme (export)

5.4.3 The gap

Figure 20 and 21 are – obviously – not showing all the possible messages that could be exchanged among the different SC parties, but they clearly indicate that more messages and information must be exchanged or at least there must be some kind of (centralized or decentralized) system where the SCS relevant information is available for the authorized SC actors at the time when it is needed. Especially the information exchange with the country of origin of the containers and among the customs of different counties is important in order to make the SC more secure and at the same time more efficient. Initiatives like the World Customs Organization (WCO) are a good example such an international system. For more comprehensive research on the different information exchange system, see Meijer (2007).

The gap between the current and the future (desirable) information exchange could depend on a number of developments and changes in the SC. One of these developments is the technological developments. The technological developments like the smart seals, RFID chips, integrated business systems, etc. could – in the future – make it possible and affordable for the SC community to exchange more SCS relevant information. But examples of the gap in the SCS information exchange – as described for purpose of this thesis – is that the information regarding the security certificate of all the SC parties involved in transporting a container must be checked and validated. This information could be placed on the B/L. The container scan information must be shared by the customs in order to create more efficiency. The container integrity information must be available at any moment that is required. This includes the seal information (and its meta data).

5.5 Conclusion

In this chapter the SCS relevant information needs, the SCS relevant information availability and the exchange of the SCS relevant information possibilities are introduced with the intention of trying to enhance the overall SCS and to provide more visibility in the SC activities.

A short introduction is made to the SCS relevant information and described what is meant by the term “SCS relevant information”. Also the importance of the SCS relevant information and its availability is described.

Information is described which is needed to implement the SCS measures which are defined in the previous chapter. The process of getting to the total list of SCS relevant information needs and the process which leads to a short list of the SCS relevant information is described. The total SCS relevant information is accumulated as information blocks and the data elements related to each information block are characterized as *Mandatory* or *Preferable* and the level of importance (*High, Medium and/or Low*). By doing this, the information which is crucial for the SCS is “filtered”.

It has become clear that there is a lot of SCS relevant information available but it is not organized and not efficiently exchanged among the SC actors. The current and possibly future (desired) information exchange possibilities are discussed and the gap between them is shortly mentioned.

The risks, measures and the information needs are defined in this and other previous chapters. The challenges faced at the acceptance and implementation of the measures is the subject of next chapter (6).

6 Acceptance and implementation challenges

The goal of this chapter is to provide an overview of the challenges and difficulties that could be faced during the acceptance and implementation of the SCS measures.

This chapter is outlined as follows: Section 6.1 introduces the reality of the dilemma's that are expected to be faced during the acceptance and implementation of the SCS measures. It outlines the importance of this issue. Section 6.2 provides an overview of the main challenges that are to be faced to enforce (and encourage) the SC parties to accept and implement the SCS measures. Section 6.3 is a follow up on the previous section. It presents the possible solutions for the challenges described in the previous section. It depicts the criteria that must be taken in account at the development of SCS measures. Furthermore, a number of methods are described which could enforce the SC actors to accepting and implementing the SCS measures. After that, these methods are evaluated and recommendations are provided regarding this issue. In section 6.4 a conceptual framework model for accepting and implementing the SCS measures is developed. This model provides an overview of the possible benefits that are associated with the implementation of SCS measures. Finally, section 6.5 presents the field research that is conducted for the purpose of this thesis. It provides short overview of the SC actors that were interviewed.

6.1 Introduction

The acceptance and implementation of the SCS measures are expected to be faced with some resistance and challenges from the SC community. Depending on the actor, these resistance and challenges are based on different grounds and restrictions (e.g. financial, organizational, technical, etc.). During the field research for this thesis, the issue of acceptance and implementation of the SCS measures were characterized as a big concern. That is why this issue must be considered as a very important issue to be discussed. Different solutions were proposed by the SC actors (incentives) which are discussed later in this chapter.

Although the SCS threats, information needs and measures that are defined in the previous chapters are based on the daily practice and reality, still they could only be accepted and implemented by the SC parties if they are convincing and the (direct/indirect, short term/long term, financial/operational, individual/collateral) benefits are proven and to a certain level guaranteed. This approach is needed because the general view of the SC actors towards the implementation of SCS measures is negative. They would like to see the return on their investment in tangible results because as time passes they think that nothing bad will ever happen and they are tempted to divert resources away from investing in security [Slay J., Koronios A. (2006)].

There are a number of solutions to convince the SC actors to accept and implement the SCS measures. These solutions are further specified in this chapter. But before start providing solutions, the main challenges and difficulties that are expected to be faced, are discussed.

6.2 Main challenges

Based on the field research, it became clear that a lot of challenges are expected to be faced to convince the SC actors to accept and implement the SCS measures. The reasons for these difficulties and challenges are different per SC actor and individual company in the SC. Most of the challenges are related to the incentives that are expected by the SC parties in return for the implementation of the SCS measures. A category and subcategory based approach is used to provide a clear view of these challenges. Some of the main challenges are:

1. *Measures characteristics:*
    a. Relative advantage. The SCS measures that are implemented should result in relative advantage (e.g. quicker/more efficient business processes);
    b. Compatibility with business objectives and systems. The SCS measures that are implemented should be compatible with the current business objectives of the SC

actor and it must also be compatible with the business (information) system currently in use;

   c. Complexity. The SCS measures must not be too complex. The more complex the measures, the less interesting they are for the (smaller) SC actors;
   d. Tryability. It is preferable that the SCS measures are first tried for a while before implementation;
   e. Observability (benefits). The benefits of the SCS measures must be easily observed. Preferably in short term;
   f. Switching costs. The costs involved in switching to new SCS measures must be as low as possible.

2. *Organization characteristics:*
   a. Security awareness. Most of the organizations are not fully aware of the possible threats and risks that their processes could face or the threats and risks that their processes could cause to others due to insufficient security awareness;
   b. Size of the organization. The size of the organization is an important characteristic. Generally, due to the (financial and human resource) capacity large size organizations are easily implementing new SC measures compare to smaller size organizations;
   c. Flexibility. Not all organizations are structured the way that they are flexible to changes in their business processes caused by implementing SCS measures. These organizations mostly have a vertical organization structure with a lot of hierarchies and layers;
   d. Willingness to share information. Not all SC actors are willing to share the SCS relevant information which they have. This is due to different reasons but one of the reasons is the lack of trust and reliability;
   e. Willingness to implement security measures. Implementing new SCS measures are seen by some of the SC actors as unnecessary and unnecessarily making expensive investments and that is why they don’t want to implement any (more) SCS measures;
   f. Readiness to implement security measures. Some of the SC actors are not ready to implement SCS measures. This is due to budget, human capacity, size and/or organizational structure constrains;
   g. Value secure supply chain. The value a secure SC is for some SC actors very low. These are actors which are not directly affected by a security breach in the SC. These are mostly the SC actors which are indirectly involved in the SC processes;
   h. Security initiatives. The security initiatives are costly and so far only the large multi national organizations have had some investments in the SCS initiatives because they have a relatively large market share and the effect of the SCS initiatives and the return on investments are feasible. But in order to create an overall secure SC, also the smaller SC actors must be convinced of cooperating and investing in the SCS initiatives and they must be convinced of the benefits of their investments. Because the small SC actors are mostly the weaker links in the SC due to the lack investment in (new) security initiatives related to their businesses.

3. *External characteristics:*
   a. Market uncertainty/demand. Like any other businesses, the container transport actor is sensitive to the uncertainties in the market and depends on the demand from the market. This means the implementation of the SCS measures is not the first priority for the SC actors. But the market uncertainty and market demand can also be seen a tool of putting pressure on the SC actors to implement the SCS measures (e.g. the demand for a highly secure SC from the market);

b. Trading Partner Pressure. The pressure from the trading partner of a SC actor can have both negative and positive influences on implementing SCS measures by the SC actor;

c. Trust between trading partners. The trust between the trading partners is not always very good. This fact has become very clear during the field research which has been conducted for the purpose of this thesis. The issue of trust among the SC actors makes the implementation of a SCS measures (e.g. exchange of SCS relevant information among the SC actors/trading partners) is very difficult. But by implementing SCS measures more transparency can be created and this could eventually lead to increased trust among the trading partners;

d. Competitive pressure. Some SC actors are not implementing the SCS measures because it could const money and they could lose their competitive position to the other SC actors due to the (high) investment. Other SC actors are willing to gain competitive advantage by implementing SCS measures. This could provide more efficiency to their business processes which – in long run – could result in improved competitive position in the market;

e. Legal pressure/mandatory requirements. By legal pressure and/or mandatory requirements from the local or foreign authorities is one of the was to make the SC parties implement the SCS measures. But this approach is not widely preferred (supported) by specially the smaller SC actors which are included in the field research.

4. *Supply chain/Industry structures:*

   a. Power relation/position in the network. The power ratio and the position of a SCS actor (in other words: the market share) is a very decisive factor for implementing the SCS measures. This is due to the effectiveness of the SCS measures on the entire SC;

   b. Economic relations (collateral benefits). The economic incentives of the SCS measures are one of the most important factors for the SC actors to implement the SCS measures. This could be a challenge because the investment in SCS measures is not always resulting in tangible financial payoff in short run. The desired results of investing in SCS measures are that nothing happens. This is why to prove the benefits which could be gained by SC actors by implementing the SCS measures (collateral benefits) is a challenge;

   c. Corporate relations (partnership/trust). The corporate relation is an important issue which determines whether to implement SCS measures or not. If the partnership and trust among the SC actors is at stake, then it will not be easy to implement SCS measures.

6.3 *Solutions for the challenges*

Taking in mind the challenges and the difficulties mentioned in the previous section, some solutions can be developed to help easing these challenges and to encourage the SC actors to accept and to implement the SCS measures. In this section some possible solutions are discussed which are based on the incentives which the SC actors could expect in return on the investment they make in accepting and implementing the SCS measures.

6.3.1 Criteria for the development of the SCS measures

First of all, the SCS measures must be developed in a manner that the requirements from the SC community are taken into account as much as possible and the SCS measures must be examined on their feasibility. This is an issue which is discussed during the field research and during the expert brainstorm sessions. The level of coverage of the criteria for the SCS measures shown in figure 22, could be decisive for the SC parties to implement the SCS measures or not.

Figure 22, shows the basic criteria for development of SCS measures. These criteria are mentioned partly in Meijer (2007) for the purpose of the information system architecture (ISA) and partly in Rogers (1995). These criteria are meant to be used as guideline for the development of the SCS measures. The criteria are briefly explained.

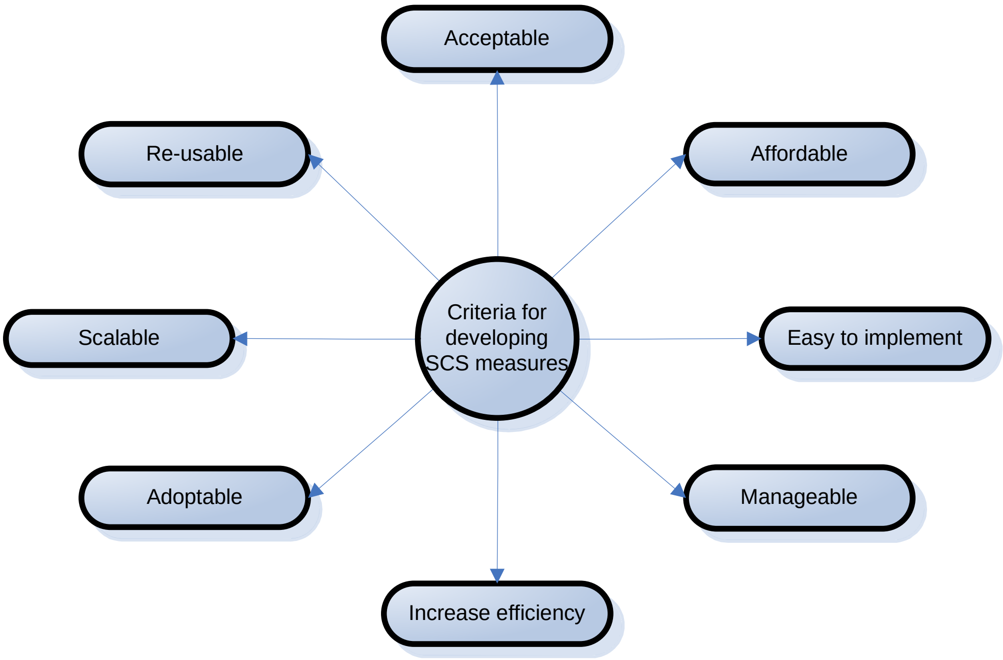


Figure 22 Criteria for development of the SCS measures

Acceptable

The first criteria for the SCS measures is the acceptability. For the context of this thesis, acceptable means that security measures should be flexible and it should fit into the company's business and comply with the overall objectives of the company. The acceptability of the SCS measures could be increased by the level of the CIA requirements that are met by the SCS measures. Also the coverage of the SCS measures is important for their acceptability. This means that the measures must be implemented by – preferably – all the SC actors. This will result in a higher overall level of SCS and increased collateral benefits. If only a (small) number of SC actors accept and implement the SCS measures, the SC will still be vulnerable and there still be some weaker links in the SC.

Taking in mind the issue of acceptability could result in anticipating of challenges such as compatibility with business objectives and system, complexity, observability (benefits), and flexibility.

Affordable

The second criteria for the SCS measures is the affordability. Affordability is a comparative term. Whether a SCS measure is affordable or not, depends on the size and the financial capacity of a company. But generally, the investment in SCS measures must be lower than (and it should never exceed) its return on investment (ROI). Protection against terrorist risks costs money. Large sized companies have – to some extent – implemented some security measures for their own supply chain operations. However, the majority of the medium and nearly all small sized companies in the supply chains, including their employees, have neither implemented security measures nor are fully aware of terrorist risks [DNV Consulting (2006)].

Taking in mind the issue of affordability could result in anticipating of challenges such as relative advantage, switching costs, and tryability.

Easy to implement

The third criteria for the SCS measures is that the measures must be easy to implement. By easy to implement is meant that the measures must be technically to implement. It shouldn't require lots of new technological changes. It must be accepted by the current systems in use and – of course – it must comply with the overall objectives of the company. The SCS measures shouldn't require very new business approaches and it should not result in redesigning the business processes in order to implement the measures. The measures should also not result in resistance from the employees to the changes. Because some SCS measures could force the employees to learn new working procedures and methods and it might require re-schooling.

Taking in mind the issue of easiness to implement could result in anticipating of challenges such as compatibility with business objectives and systems, complexity, tryability, and flexibility.

Manageable

The fourth criteria for the SCS measures is the manageability. This means that the SCS measures – once accepted and implemented – must be easy to manage and maintain. They must not require (a lot of) additional human and/or financial resources in order to be managed and maintained.

Taking in mind the issue of manageability could result in anticipating of challenges such as compatibility with business objectives and systems, and observability (benefits).

Increase efficiency

The fifth criteria for the SCS measures is the contribution to increase the efficiency. The SCS measure must help improve the efficiency of the business activities. Example of such improved efficiency is the controls that must take place during the import and export process of a container. By implementing the SCS measures, the frequency of these controls can get lower which means the container is not needed to be controlled at more locations at different moments in the SC.

Taking in mind the issue of efficiency could result in anticipating of challenges such as relative advantage, and observability (benefits).

Adoptable

The sixth criteria for the SCS measures is the adoptability. The adoptability of the SCS measures is very important. The SCS measures must be developed in a manner that they could be adopted for a new business process. Or – since the container transport is a very dynamic and vulnerable business – the SCS measures should make sure that the change in the information needs or changes in business process or other changes are implemented without (a lot of) additional efforts and additional investment of the financial and/or human resources.

Taking in mind the issue of adoptability could result in anticipating of challenges such as compatibility with business objectives and systems, complexity, and switching costs.

Scalable

The seventh criteria for the SCS measures is the scalability. It is very important for a SCS measure to be scalable. This means that if the quantity of the containers – transported by a SC actor – increases, the SCS measures should be capable of supporting this increase in the quantity of containers. Since the container transport is growing rapidly, the issue of scalability is very realistic and must be taken into a serious consideration during the development of the SCS measures.

Taking in mind the issue of scalability could result in anticipating of challenges such as compatibility with business objectives and systems, complexity, switching costs, and flexibility.

Re-usable

Finally, the eighth criteria for the SCS measures is the re-usability. It should be possible to re-use the SCS measures. Especially this should be the case for the more expensive SCS measures like the usage of expensive technical equipment (e.g. the GPS equipments on a container). From the financial perspective, the development of the re-usable SCS measures is a very welcome feature and the RIO would be easily prophesied.

Taking in mind the issue of re-usability could result in anticipating of challenges such as compatibility with business objectives and systems, complexity, switching costs, and flexibility.

6.3.2 Methods for accepting and implementing the SCS measures

Secondly, the SC actors could be put under pressure in order to make them accept and implement the SCS measures. A number of methods could be defined to put pressure on the SC actors and make them accept and implement the SCS measures.

Market (customers) pressure

The first method to enforce the SC actors to accept and implement SCS measures is the pressure form market and the customers. The demand from the market (thus from the customers) could pressure and enforce the SC actors to implement SCS measures. Most of the large SC actors which are interviewed (such as producers and shippers) are demanding for a very highly secure container transport chain. There are several reasons for this demand of high level of security.

Some of the goods to be transported are of high value (e.g. Philips products). In this case the financial consequences as a result of damage to the goods or theft of the goods are very high. Some other goods to be transported are highly dangerous (e.g. chemical and explosive material). In this case the financial consequences, the environmental consequences and the consequences for human fatalities as a result of a security breach in the transport could be very high. Others are concerned regarding the image of their company and brand. In this case, the financial consequences as a result of damage to the goods to be transported are not high but the financial consequences as a result of the damage to the name (image) of the company and its products are much higher. These are not always high value goods (e.g. Heineken).

The reasons mentioned above are some of the reasons why the market (the customers) demands for highly secure SC and demands from (put pressure on) the SC actors to implement the SCS measures in order to fulfil their SCS requirements. If the SC actors do not meet the security requirements from the market, the customers will go to another SC actor (the competitor). For this reason and for the continuity reason, the SC actors are forced to implement SCS measures.

Trading partners pressure

Most of the SC actors gradually become trading partners. They develop mutual trust and form a chain in which they operate on regular basis. When one or more (the majority of the) trading partners choose to accept and implement new SCS measures due to the demand from the market, the other trading partners are forced to follow in order to stay in that chain of trading partners. The implementation of the new SCS measures by the trading partners could be to become SCS certified and benefit from the incentives that are related to the certification. Later in this chapter, a number of incentives will be discussed and one of these incentives is related to the so called *Green Lane* idea which means that all the trading partners who are involved in transporting a certain container are SCS certified.

In order to maintain the mutual trust build and which has resulted in forming the trading partner’s chain and to benefit from the collateral benefits that are involved in becoming a green lane operator in the SC could be examples of the incentives and could encourage the SC actors to accept and implement the SCS measures.

Competitive pressure

As mentioned in the previous section of this chapter (6.3.1 Criteria for the development of the SCS measures), one of the criteria for the development of the SCS measures is that they should help increase the efficiency of the business processes of the SC actors which are implementing the SCS measures. More efficient business processes will lead to a more competitive advantage. This means that the SC actors which have implemented the SCS measures will have competitive lead compare to the SC actors which haven't implemented the SCS measures.

For the other SC actors in order to cutch up with the rest and to stay in the business, they must also implement the SCS measures. They can be encouraged by the competitive advantage that could be gained from implementing SCS measures. By this method the SCS measure could be accepted and implemented.

Authorities pressure (Mandatory Security Requirements)

Finally the pressure from the authorities is another method to force the SC actors to accept and implement the SCS measures. The governments and authorities could define SCS measures which determines a certain level of SCS. The governments and authorities could then impose the SC actors to implement those SCS measures in order to keep their business license and stay in business or other type of penalties could be defined. These mandatory SCS requirements could also be imposed by the foreign governments and authorities. The SC actors that are involved in the international container transport will have to implement the SCS measures developed by domestic and foreign governments and authorities in order to stay in business.

6.3.3 Evaluation of the methods for accepting and implementing the SCS measures

Security is a state responsibility. Leaving SCS fully to self-regulation by industry would be irresponsible for any state, as also concluded by the Heads of State (March 25, 2004). On the other hand supply chain management is an industry's responsibility and therefore public/private partnership is necessary [Eur-Lex (2007)]. This means a combination of security initiatives taken by the states and security initiatives taken by the industry must be created in order to enhance the overall level of SCS.

In the previous section of this chapter a number of methods are discussed to encourage (enforce) SC actors to accept and implement SCS measures. Which of the above methods are the most suitable and preferable for all parties involved in the SC, are a subject for further research. But the general focus should be on the bilateral benefits and a win-win situation must be created. The win-win situation could be created by finding the right balance between government security initiatives, implementation costs and supply chain efficiency. Also finding the optimum portfolio and pricing for supply chain security services and solutions is an important issue. Finally, finding security services and solutions which also contribute to supply chain efficiency is a method to create the win-win situation in a secure SC.

The (financial) incentives of a secure SC must become more visible. Some of the incentives which could encourage the SC parties to accept and implement the SCS measures in the remainder of this chapter as follows:

Collateral Benefits

By collateral benefits is meant other benefits – in addition to improved security which participating SC actors – derived from their security investments.

Studies [Peleg-Gillai, B. et al. (2006)] show that the majority of the parties which have invested in security reported a wide range of benefits. But some of the parties explained that since they already had robust security systems in place for many years, and/or have taken over the years numerous steps to improve the efficiency of their internal operations, they could report very few collateral benefits following the adoption in recent years of government regulations or voluntary initiatives. This means that these parties already had competitive advantage.

Some other parties explained that since they already had a robust security system in place for at least 10 years, and so hasn't experienced any fundamental shift in its security practices or in the impact they had on its business following 9/11. The major benefits they could report as a result of their C-TPAT certification were fewer and less intrusive inspections at the ports, which also provided less opportunity for damage to the imported goods. This is a clear example of the human psychology of explained by Slay J., & Koronios A., (2006) that in most areas of life, people and organizations who work hard and spend money expect something in return, but with security, the pay-off is that nothing happens. Human psychology does not see this as a true reward. It can be a challenge to see the benefits of the resources invested. Indeed a good security manager oversees a site where nothing bad happens. Often, as time passes, people can begin to think that nothing bad will ever happen and be tempted to divert resources away from security.

The field research – which has been conducted for the purpose of this thesis – also resulted in a number of clear examples of collateral benefits derived from the SCS initiatives and investments. One of these examples is Heineken. The largest market for Heineken is the USA. Products exported to the USA must meet the security requirements from the USA. Heineken always meets these security requirements and it also invests a lot in the new SCS initiatives. Amongst a number of benefits Heineken also mentioned the benefits like faster security inspection procedures for Heineken containers. Since the large number of containers exported to the USA, a faster security inspection procedure is a very important profit for Heineken.

While not an objective on its own, the increase of the quality of business performance due to implemented security programs can be considered a positive collateral benefit [DNV Consulting (2006)].

Visibility

Following the acceptance and implementation of SCS measures, the SC parties could improve their visibility to the location and condition of their goods as they move along the SC. Examples of improved visibility as a result of the implementation of the SCS measures are:

1. The accessibility to supply chain data could be improved which can lead to a better planning and management in container transport. Cost savings could be attributed to better planning and management in container transport;
2. The implementation of the SCS measures could also lead to an improvement in the timeliness of shipping information which could also be seen as important for a better planning and management of container transport. Cost savings could also be attributed to the timeliness of information;
3. A better data accuracy or data/information integrity could be as a result of the implementation of SCS measures. This could result in a more accurate container transport process which will decrease the number of accidents and mismanagements and prevent the loss of financial assets and even lives;

Efficiency

The efficiency as a result of implementing the SCS measures can be related to both process improvements as well as improvements in transportation and in the customs clearance process.

The process improvement can be seen as increased automated product handling and reduction in the number of times a product is handled. Such improvements are likely to lower the number of working hours required for these activities, and to reduce the chances for errors in the process or damage to the goods. Also increased process compliance is likely to be achieved as an effect of improvements in the processes. Also reduced process deviations and increase in process predictability can be achieved as a result of process improvement. Process improvement also means reduction in the number of steps in the supply chain process and reduction of the cycle time (measured as the time from order receipt until it is shipped). This is very likely to result in higher customer satisfaction in addition to internal benefits.

Process improvements as mentioned could result in higher productivity and this eventually could result in reduction in required personnel. Reduction of personnel and the processing benefits mentioned above are likely to result in cost saving.

Resilience

The implementation of the SCS measures could result in more resilient SC. By more resilient SC is meant the relationship between the SCS measures taken by the different SC actors and their ability to identify, respond to and resolve problems – especially problems that are related to breaches in security or to delays and other issues SC actors may face while their goods are in transportation.

As a result of a more resilient SC the identification time of a problem can be reduced. also the response time to a problem can be reduced and the problem resolution time is likely to be shortened. Cost savings could be realized and be attributed to these improvements

Customer Relations

The SC actors who implement the SCS measures are very likely to be able to improve the relationship with their customers and improve customer satisfaction. This could be achieved by offering more reliable and transparent services related to container transport. By doing so more customer satisfaction and confidence can be achieved. This can also be seen as promotion for the transport services of these SC actors and it is likely to result in increase in the number of new customers.

Furthermore, the implementation of SCS measures could result in more and better communication with the customers and increase in the number of joint customer activities, which indicates a tighter relationship with these customers.

6.4 Exploratory research results

As mentioned in the previous chapters, a field research is conducted for the purpose of this thesis. At least one interview is done with each type of SC actors. Table 19 shows a list of the SC actors that are interviewed. This table also provides an overview of the responses from the different actors on the questions asked during the interviews. The questions which are asked during every interview were related to the effect of four major characteristics on every SC actor namely; the measures characteristics, the organization characteristics, the external characteristics, and the supply chain/Industry structures [Oosterhout, M. & Moonen, H. (2006)]. The effects of these characteristics for each actor are examined. These effects are either “high/large/positive/important” which are denoted by “+”, or non which are denoted by “0”, or “low/small/negative/not important” which are denoted by “–”. The SC actors that are interviewed are divided in three categories namely; authorities, business (supply chain) parties, and technology providers and others. A complete list of the SC actors which are interviewed is to be found at appendix C.

			Measures characteristics						Organization characteristics								External characteristics					Supply chain/Industry structures		
	Categories of actors		Relative advantage	Compatibility with business objectives & sys	Complexity	Triability	Observability (benefits)	Switching costs	Security awareness	Size of the organization	Flexibility	Willingness to share information	Willingness to implement security measures	Readiness to implement security measures	Value secure supply chain	Security initiatives	Market uncertainty/demand	Trading Partner Pressure	Trust between trading partners	Competitive pressure	Legal pressure / mandatory requirements	Power relation/position in the network	Economic relations (collateral benefits)	Corporate relations (partnership/trust)
	Authorities																							
1	Customs	Customs	0	0	0	0	+	0	+	+	0	+	+	0	+	+	0	+	+	0	+	+	0	0
2	Seaport Police	Police	0	0	0	0	+	0	+	+	0	+	+	0	0	+	0	0	0	0	+	0	0	0
3	Port Of Rotterdam	Port of Rotterdam Authority	+	0	0	0	+	0	+	+	0	+	+	0	+	+	0	+	+	+	+	+	0	0
	Business (supply chain) Parties																							
4	ECT	Sea terminal	+	+	0	0	+	0	+	+	0	+	+	0	+	+	0	+	+	+	+	+	0	0
5	Heineken	Shipper	+	+	0	0	+	0	+	+	0	+	+	0	+	+	0	+	+	+	+	+	0	0
6	International Transport Overbeek (operator & depot)	Road operator	+	0	0	0	-	0	0	-	0	+	-	0	+	-	0	+	0	+	-	-	0	0
7	Centraal Burea voor de Rijn- en Binnenvaart (CBRB)	Barge operator	+	0	0	0	+	0	+/0	+	0	+	+/0	0	+	+	0	+	0	+	0	+	0	0
8	Rail Service Center Rotterdam	Rail operator	+	+	0	0	+	0	+	-	0	+	+	0	+	+	0	+	+	0	+	+	0	0
9	Keune & Nagel	LSP	0	0	0	0	-	0	+/0	+	0	+	+/0	0	+	+	0	+	+	+	0	+	0	0
10	Maerskline	Shipping line (agent)	+	0	0	0	+	0	+	+	0	+	+	0	+	+	0	+	+	+	+	+	0	0
	Technology providers and others																							
11	Port infolink	Solution provider	+	+	0	0	+	0	+	-	+	+	+	0	+	+	0	+	+	+	+	+	0	0
12	Siemens (CommerceGard)	Technology provider	+	+	0	0	+	0	+	+	0	+	0	0	0	+	0	+	0	+	0	+	0	0
13	Aon Risk management	Insurance	0	0	0	0	0	0	+	+	0	+	0	0	+/0	0	0	+	0	0	+	0	0	0

+	High/large/positive/important
0	Non
-	Low/small/negative/not important

Table 19: Evaluation of the interviews

The analysis in table 19 shows that 69% of the SC actors (9 out of the 13) are expecting to gain relative advantage by implementing the SCS measures. 77% of the SC actors (10 out of the 13) are expecting to have a better observation of their business (processes) by implementing the SCS measures. The security awareness within the organization is considered by 92% of the SC actors (12 out of the 13) as being highly important. 77% of the SC actors are large size organizations. The size of the organization is considered to be very important for implementing the SCS measures. The small size organizations also consider the SCS measures important as long as they are affordable. All actors were willing to share information if that could lead to improved SCS. 69% of the SC actors were willing to new implement SCS measures and these were mostly the large size organizations. 85% of the SC actors (11 out of 13) consider a secure SC as being highly important for their business (processes). 85% of the SC actors were actively involved in new SCS initiatives. 92% of the SC actors were defining the trading partner pressure as being the highly important to implement the SCS measures. 62% of the SC actors (8 out of 13) were considering that maintaining the trust between trading partners as being an important reason for implementing the SCS measures. 69% of the SC actors were considering the competitive pressure also an important reason to implement SCS measures. Equal percentage of the SC actors were considering the legal pressure / mandatory requirements as being an important reason for implementing the SCS measures. 77% of the SC actors were arguing that power relation/position in the network of an organization/SC actor – same as the size of it – determines the level of SCS initiatives and the level of implementing the SCS measures.

6.5 Conceptual framework model for SC

Based on the findings from all the previous sections of this chapter, findings from the field research and the recommendations from the expert sessions, a conceptual framework model for accepting and implementing the SCS measures is developed as shown in figure 23.

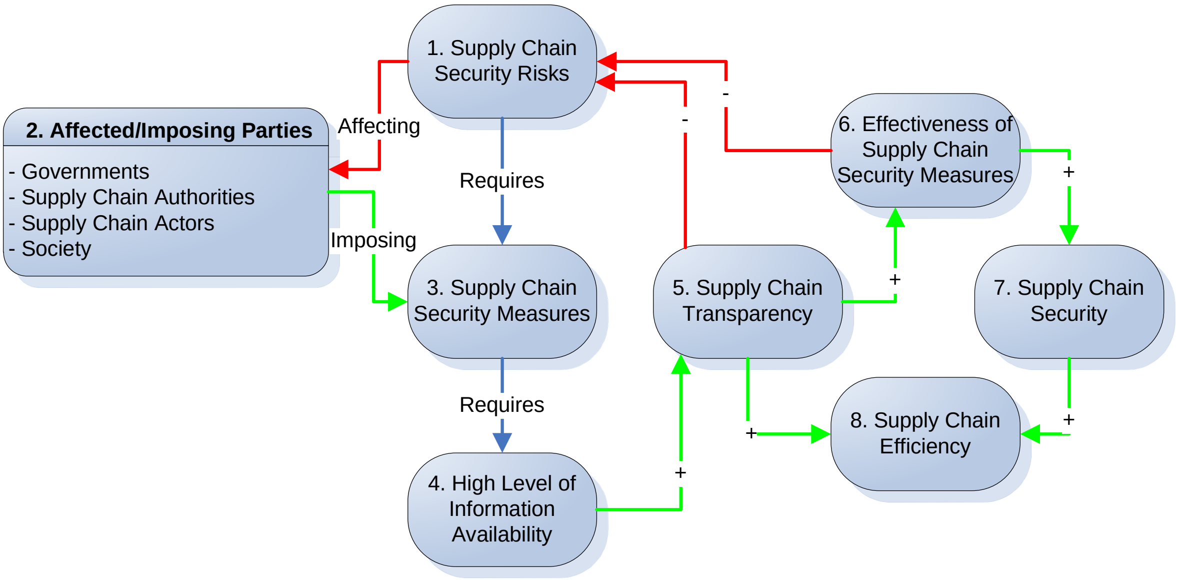

1. Supply Chain Security Risks
2. Affected/Imposing Parties
- Governments
- Supply Chain Authorities
- Supply Chain Actors
- Society
Affecting
Imposing
Requires
3. Supply Chain Security Measures
Requires
4. High Level of Information Availability
5. Supply Chain Transparency
6. Effectiveness of Supply Chain Security Measures
7. Supply Chain Security
8. Supply Chain Efficiency
-
-
+
+
+
+
+

Figure 23 Conceptual framework model for SC

Description of the model:

The SCS risks could affect the governments, the SC authorities, the SC actors and the society. This means that not only the SC benefits from a secure SC but also others. This is why the idea of developing and implementing the SCS measures doesn't necessarily come from SC actors that are directly involved in the SC. Thus in order to prevent a SCS risk from resulting in SCS threats, SCS measures are required to be developed and implemented. These SCS measures on their turn require SCS related information and its availability. The level of information availability depends on the willingness of the SC actors to share SCS related information. Sharing information will lead to a more transparent SC. SC transparency could have negative effects on the SCS risks because the people who want to misuse the SC for unlawful acts will have more information and it will make it easier for them to succeed. A transparent SC means that the processes are better visible and controlled. This could positively affect the SC efficiency. At the other hand a transparent SC will show and increase the effectiveness of certain SCS measures. The more SCS measure are effective the more secure a SC becomes and a secure SC could lead to more efficient SC and less SC risk.

This framework model provides a better view of the results of this research so far. It also provides a clear understanding of the benefits (e.g. SC transparency, SCS, and SC efficiency) for the SC actors as a consequence of implementing the SCS measures. Furthermore, it provides an overview of the possible methods to enforce (encourage) the SC actors to implement SC measures. It also mentions the parties that could be affected by certain SCS risks and the parties that require SCS measures.

6.6 Conclusion

In this chapter the challenges and the difficulties that could be faced during the acceptance and implementation of the SCS measures are discussed. Different reasons are mentioned which are used by the SC parties to challenge the acceptance and implementation of the SCS measures. Most of the reasons for challenging the acceptance and implementation of the SCS measures are based on financial grounds. Also the (financial) investment in technical and organizational changes are mentioned as being important reasons for SC parties to resist accepting and implementing the SCS measures.

The most preferred way to convince the SC parties to accept and implement the SCS measures is by come up with (financial) incentives which could be as a result of the implementation of SCS measures. Exampled of such incentives are building trust, enlarging the business network, increased credibility, improved visibility of the business activities, etc. Also other ways to convince the SC parties to accept and implement the SCS measures are discussed such as the pressure from the governments (legal pressure), competitive pressure, etc.

The SCS measures must be developed according to the requirements from the SC actors (SC community). This will make it easy for the SCS measures to be accepted and implemented by the SC parties. Then the method which is used to for accepting and implementing the SCS measures are discussed. Finally the methods used must be evaluated on their results.

A conceptual framework is developed which provides a better view of the results/benefits that can be achieved by accepting and implementing the SC measures. It also demonstrates the possible negative effects of the SCS measures. Finally in this chapter are the results from the exploratory research briefly analysed.

The most important conclusion from this chapter is that in order to achieve a desired level of information availability, the SC parties should undergo a transition. This transition is expected to be faced with acceptance and implementation challenges that are related to SCS measures. The transition can be redesigning the business processes, exchanging and providing additional security related data (information), getting the security certificates, the use of new IT application, etc. Depending on the type of the SC measure, the SC actors are confronted with different kind of challenges.

Next chapter (Chapter 7) provides the results from the validation workshop for work package 5.1 (and work package 5.2).

7 Validation

This chapter describes the findings from the validation workshop that was organized for discussing and validating the findings from the work package 5.

This chapter is outlined as follows: Section 7.1 introduces the validation workshop. It describe the purpose of the validation workshop. Section 7.2 presents the findings and feedback on work package 5.1. Work package 5.2 is also mentioned briefly and this chapter ends with a conclusive summary of the validation workshop.

7.1 Introduction

As part of the research methodology used in this thesis a validation workshop was organized to discuss research findings from both work package 5.1 and 5.2. In this workshop, experts from different domains participated and were able to express their remarks on results presented in preliminary versions of the research papers and presented during the workshop itself. A list of participants can be found in appendix D. These people represent expert opinions from three category of actors that were examined in this research such as authorities, business (SC) parties, technology providers and the PROTECT project team.

For the validation workshop, two and a half ours were available which were roughly cut in half for the two work packages. The two sessions started with the presentation of results after which the audience was given the opportunity to react on the results presented.

7.2 Work package 5.1

During the validation of work package 5.1, the information analysis as presented in this thesis was the primary focus of discussion. In the reactions, it was addressed that the importance of the different data elements deserves extra attention. A point of discussion was the importance of the data elements from the SCS point of view and whether data elements were mandatory or preferable. Some of the participants offered to view all the data elements and mention the level of importance from their own perspectives. Later on the data elements are sent to the individual experts and the experts valuated the data elements.

Furthermore, the risk analysis was a point of discussion. It was discussed that when considering theft, the risks involved in the transport of the container by truck were underexposed. For terrorist attacks, it was discussed that all containers have essentially the same chance of being a target, thus focusing on one of the modalities is not warranted from this point of view. Within the scope defined in this thesis, it is best to look at all modalities with equal concern.

Other point of discussion was the current and future information exchange among the SC actors. The remark was that the figures presented in this thesis depicting this point are too simplified. Although the figures are too simplified, they do represent the exchange of the most important information and the most important SC actors involved but in the real world, there are much more SC actors involved and much more information is being exchanged and in the future is desired to be exchanged in order to improve the level of SCS.

Also the issue of the coverage of this research is discussed. It is mentioned that the presented findings doesn’t represent the complete SC because of the lack of information from more actors (examples) from the same category. It is made clear that the time constrains and the unwillingness of the different actors to participate in this research has caused this lack of information.

In the second half of the workshop work package 5.2 is presented by Mark Meijer and the audience got the opportunity to react on the findings that were presented. A more detailed report on this is to be found in Meijer (2007).

7.3 Conclusion

Whether the SCS measures which are defined in this thesis and presented during the workshop will result in increased SCS is not easy to evaluate during such a workshop. It can only be evaluated if these SCS measures are used in a pilot project. But the methodology which is used to analyse the security issue in the SC and the needs for measures and information is discussed and generally approved. The main problem that is identified during this workshop was the importance of the different data elements. To deal with this issue, all the attendees have received a copy of the original analysis tool with all the elements that are presented. The attendees are requested to go through the data elements and valuate the importance of each data element from their own point of view. Some of the attendees did valuate the data elements and the results are processed in the risk analyses which is presented in this thesis.

8 Conclusions and recommendations

In this last chapter the main conclusions of the research are presented. Besides this, the recommendations for further research based on these findings are identified.

This chapter is outlined as follows: section 8.1 the main results from this research are presented followed by section 8.2 where the recommendations for further research are presented. Finally the research limitation are mentioned in section 8.3.

8.1 Conclusions

This conclusion takes us back to the main objective of this research which was formulated as to find out "*Which information is needed to improve the SCS and how can this information be exchanged among the parties, directly and indirectly, involved in the SC?"*. In order to provide an answer to this research objective, five research questions were formulated. By answering these research questions the answer to the main objective of this research (thesis) is provided. These research questions are discussed one by one in the reminder of this section.

Which security threats and risks do the parties involved in the logistic process, consider important with respect to the security of the SC?

Chapters 2 and 3 provide a more detailed answer to this question. In general, the security threats and risks that are considered important are divided in three types of security threats and risks; namely the physical security risks, the information security risks (non-physical security risks) and the financial risks.

The physical security risks are the risks of damage to the infrastructure and the SC means, and risks that the SC means are being used to create damage or fatalities. The information security risks are the risks that are related to the Confidentiality, Integrity and Availability (also known as CIA) of the SC information. The financial risks is out of scope of this research.

Which security measures can improve the security level of the SC?

Chapter 4 provides a more detailed answer to this question. The security measures which can improve the security level in the SC can be either physical security measures (e.g., improving the security of the SC means and channels and developing better facilities in order to prevent damage to the physical infrastructure of the SC), technological security measures (e.g., installing GPS systems "track and trance system" on the trucks in order to be able to follow the containers) or non-physical/organizational security measures (e.g. redesigning the business processes) or a combination of all three.

Having said this, it is obvious that there are many different security measures are created and can be created to improve the security level of the SC in general. It is worth saying that all the measures are either preventive, detective or corrective. Some of the SCS measures are currently available (in use) and some are created to be used in the future.

A general idea is that the best security measure for the SC is to keep the containers and goods moving. Container and goods in motion reduces security risk because they are practically less easy to be accessed and this contributes to reduction of their vulnerability.

What operational and security relevant information is needed to reduce SCS related risks and make the SC more secure?

Chapter 5 provides a more detailed answer to this question. The total SCS relevant information is accumulated as information blocks and the data elements related to each information block are characterized as *Mandatory* or *Preferable* and the level of their importance (*High, Medium and/or Low*). By doing this, the information which is crucial for the SCS is "filtered". This method has lead to a selection of the operational and security relevant information which is needed to reduce the SC risks and improve the SCS. Its is still a relatively large list of information. This list of information is related to either import process or export process only, but most of the information is needed for both processes. All parties that are involved and interviewed for the purpose of this research, agreed that the most important operational and security relevant information are related to consignor (shipper), consignee (final recipient), container (general), seal, nuclear scan (detection), scanning or inspection (container contents), operators, ship details, personnel, point of stuffing (STUF) or point of stripping (STRIP), cargo, process information on timings, port information and the information regarding the possible incidents.

It has become clear that there is a lot of SCS relevant information available but it is not organized and not efficiently exchanged among the SC actors.

How can current information exchange among the SC parties be characterized and which factors hinder or stimulate the adoption of security relevant information sharing?

As mentioned in section 5.4 of chapter 5, the current state of the information can be characterized as static. There is a fixed and predefined information flow in use, compared to the future (desirable) information exchange. The information which is exchanged is limited compared to the future (desirable) information exchange.

There are many factors which hinder the exchange of information amongst the SC actors. Some of the factors which are hindering the exchange of information amongst the SC actors are: business secrets, competition, technology, costs, (labour) capacity, interruption in the business processes, (governmental) restrictions, etc. Many more factors which discourages the exchange of the security related information are mentioned in chapter 6.

There are also many factors which encourages the exchange of information amongst the SC actors. These factors are based on the incentives which are expected in return for exchanging more information. Some of the factors which encouraging the exchange of information amongst the SC actors are: collateral (financial/operational) benefits, more visibility in the business processes, efficiency, etc. Many more factors which encourage the exchange of the security related information are mentioned in chapter 6.

What is the gap between the current information availability and the desired information availability with regards to SCS and what are recommendations to bridge this gap?

Although due to the uncertain nature of the SCS information needs in the future an exact gap between the current and the future information availability can't be provided now, but chapter 5 provides a clear answer to this question. In this chapter it has become clear that a lot of security related information is already available in different (information) systems of the SC actors that are directly and indirectly involved in the SC. But the available information is not organized. The expectation is that in the future more and new (technology generated) information will become available which can't be predicted now.

Thus the gap between the current information availability and the desired information availability with regards to SCS is that currently a lot of SCS relevant information is hidden in different (information) systems of the SC actors. This information is not always used during the transport of a container.

This gap can be bridged by making multilateral agreements with most (preferably all) of the SC actors and develop a centralized system or use existing facilities (e.g. Port infolink) to collect and distribute the SCS relevant information. There are also other technology based solutions (see Meijer, 2007) to bridge this gap. Also other procedural solutions (e.g. mandatory requirements for providing certain types of information) can help bridge the gap.

Having answered all the research questions, the answer to our main question of this research (*Which information is needed to improve the SCS and how can this information be exchanged among the parties, directly and indirectly, involved in the SC?*) is that there is a lot of information available in different stages of the SC and in different SC systems. But not all of the available information is equally important for the security of the SC. The most important information which is related to the SCS, is mentioned in the previous page. The information which is mentioned here is needed to implement the measures by which the SCS can be improved. The SCS measures are either preventive, detective or corrective from nature.

Identifying SCS related information only, is not enough to secure the SC. It is very important that by using the modern technology, the information is exchanged among the SC actors across the entire SC. This sharing and exchange of SCS related information should take place based on protocols inline with the international standards. In fact, currently a lot of information is being exchanged but not all the information identified in this research. Figure 20 and 21, section 5.4.2 from chapter 5 provides a clear overview of the current and future (desirable) information exchange. It shows that it is desirable that more security related information is timely exchanged and more SC actors are involved in information exchange. It is important that governments, World Customs Organization (WCO) and other regulating authorities are involved in developing the SC exchange standards and protocols.

It is worth mentioning that by no means is this the only list of information that can be considered as important for the SCS. This conclusion is based on the findings during this research.

8.2 Recommendation for further research

One of the recommendations for further research is to review the risk analysis tool used for the purpose of this thesis. To make the results from this analysis system more representatives for the entire SC, more interviews must be done with more than one example of a SC actor and the results from these interviews must be processed in the analysis tool.

It is also recommendable to run a pilot project in which the findings from this thesis are tested in practice. This can be done by finding some SC actors to voluntarily implement some of the SCS measures that are described in this thesis and to monitor their effects on the (improved) visibility of the business processes, the efficiency, the collateral benefits, the shorter processing time, and other positive results and also monitor the negative effects as a result of implementation of the SCS measures for example financial investment and ROI, redesigning the business processes and the procedures, the negative effects on the productivity and efficiency etc.

Also in this pilot the role of an external party such as Port infolink as an example of centralized solution for collecting and distributing of the SCS relevant information exchange can be examined.

A very important issue for further research is to find out the most preferable and applicable methods to encourage and to make the SC actors accept and implement SCS measures. This can be done by interviewing different types of SC actors and presenting the possible methods. After that collecting their opinions regarding each of the methods that are presented. Finally based on the findings from the field research and literature a conclusion can be made about the most preferable and applicable method to make the SC actors accept and implement the SCS measures.

More resurch is recommended to explore the new information system architectures by which the SCS relevant information can be exchanged among the SC actors. For example more research on the Service-Oriented Architecture (SOA) is recommendable to see how the different types of information systems of the SC actors can be linked to each other in order to improve the communication and exchange important security related information.

8.3 Research limitations

Because of the limited coverage of the research which is conducted for the purpose of this thesis, the results are not representative for the entire SC. It only represents the results from the parties that are interviewed and the parties that were actively involved in this research. This is because of the time constrains and the unwillingness of some SC actors to participate in this research. Nevertheless, the results in this thesis presents very realistic image of the issues regarding the security in the SC and the information needs, requirements and exchange in order to improve the level of security in the SC.

A. Appendix: Supply chain actors

Barge operator / Inland shipping operator (binnenvaart / vrachtvaarder / rederij)	- Operator of inland shipping vessels. [Oosterhout, 2000] - The inland shipping operator is a logistic service provider focused on the broad service offering in container transport between seaports and inland terminals via inland vessels. They aim to offer frequent reliable services with large vessels between the large number of terminals in the seaport and one or more inland terminals in the hinterland, this in conjunction with pre and post transport. They seek for optimal occupancy of their vessels with full load containers. They often rent vessels and sail fixed cycles past the terminals. Fast handling of the vessels and tight tuning of loading and unloading at the seaport and the inland terminals is in the main interest of the captains. A barge operator can be a pre-carrier or an on-carrier.
Consignee / importer (importeur)	The consignee (or importer) is the party to which the goods are consigned. This might be someone else than the final recipient. [Oosterhout, 2000]
Central distribution point (container freight station)	A facility at which (export) LCL cargo is received from merchants for loading (stuffing) into containers or at which (import) LCL cargo is unloaded (stripped) from containers and delivered to merchants. [Oosterhout, 2000]
Customs (douane)	Customs is a regulatory authority for controlling the import, export and transit of goods. Customs performs both administrative and physical controls and is primarily focused on container and bulk transport.
Empty container depot (lege container opslag)	The place designated by the carrier where empty containers are kept in stock and received from or delivered to the container operators or merchants. [Oosterhout, 2000]
Forwarder (expediteur) (merchant haulage)	The party performing the task of organizing the dispatch of goods including the necessary documentation. A forwarder can act as an agent for the shipper or the consignee. A forwarder has to arrange transport, Customs formalities, and insurance of goods during transport, etc. on behalf of a shipper or consignee. [Oosterhout, 2000]
Inland terminal operator (Inland terminal operator)	The development of an inland terminal is often related to the presence of a large shipper in the region. The ability to offer high frequency reliable services for the transport of large numbers of containers via inland shipping from and to seaports is for a shipper of main importance. Besides the inland terminal might act as a depot for storing (empty) containers and by flexibly anticipating on the timelines that shippers need their containers.
On-carrier (transporteur) Pre-carrier	Carrier (road / barge / rail) that performs the on-carriage from terminal in port of discharge to consignee. [Oosterhout, 2000] Carrier (road / barge / rail) that performs the pre-carriage from shipper to terminal in port of loading. [Oosterhout, 2000] For export a container goes from a shipper thru a pre-carrier to the sea terminal. From the sea terminal the shipping line takes the container to the foreign port from where the on-carrier takes the container to the consignee. For import the roles are reversed.
Rail operator (spoorweg maatschappij)	Operator of rail container transport. Rail operators sometimes have their own rail terminals for loading and unloading of containers onto or from the trains. A rail operator can be a pre-carrier or an on-carrier.

Regulatory authorities	Group of organizations not directly involved in the physical process of transporting containers. These organizations have a supervisor role and (continuously) monitor the physical and/or information flow in order to detect unlawful acts that could harm the security, safety and/or reliability of the SC.
Road carrier / Road hauler (wegvervoerder)	Their main interest is the optimal allocation of their fleet by combining runs and preventing “empty runs”. The road carrier is the first or final link in the chain from the shipper to the receiving party and therefore it will be confronted most heavily with waiting times. Communication with the terminals is therefore essential. A number of road carriers have started various inland terminals in order to create thick and frequent flows of containers to be shipped by inland vessels and to have a full occupied road fleet. A road carrier can be a pre-carrier or an on-carrier.
Sea terminal operator / Stevedore (terminal / stuwadoor)	A party running a business of which the functions are loading, stowing and discharging vessels. The terminal operator has to perform the physical handling of the cargo, related to vessels. This means that the terminal operator has to load the goods into a vessel. The vessel, into which the goods have to be loaded, is instructed by the liner-agent. Before any loading can take place, the terminal operator has to be informed of the delivery of the goods at his gate. This is the responsibility of the forwarder: he sends the terminal operator a Pre-Arrival, announcing which pre-carrier will deliver the goods at the terminal operator's premises. The receipt of the pre-arrival is a condition for acceptance of the goods. Given the pre-arrival and the load instruction, the goods can be loaded on the vessel if it is present at the quay. A vessel is either a general cargo vessel or a container vessel and should be loaded accordingly. It is the responsibility of the forwarder to arrange for Customs clearance. [Oosterhout, 2000]
Ship broker (cargadoor)	(Local) representative of shipping companies. They act as an intermediary between the shipping companies and the charterer. One ship broker can represent one large shipping company or can represent different smaller shipping companies.
Shipper / exporter (verlader / exporteur)	The merchant (person) by whom, in whose name or on whose behalf a contract of carriage of goods has been concluded with a carrier or any party by whom, in whose name or on whose behalf the goods are actually delivered to the carrier in relation to the contract of carriage. Synonym: Consignor, Sender. The shipper (or exporter) is the party which by contract sends goods from one place to another. [Oosterhout, 2000]
Shipping company / ship-owner (rederij)	Owner of the ships that transports the containers from port to port. Often the shipping line and the shipping company are the same organization.
Shipping line / sea carrier (scheepvaart maatschappij / rederij)	A company transporting goods over sea in a regular service. [Oosterhout, 2000]
Shipping line agent / logistic service provider (expediteur) (carrier haulage)	In shipping, a shipping line agent is a corporate body with which the shipping line has an agreement to perform particular functions on behalf of the shipping line at an agreed payment. A shipping line agent is either a part of the shipping line’s organization or an independent body. [Oosterhout, 2000]

[Adopted from Meijer 2007]

B. Appendix: Attendees experts brainstorm sessions

In the following table, the people who were regularly attending the expert brainstorm sessions are listed.

Category	Organization type	Organization name	Participant
Authorities	Customs	Dutch Customs	Mr. Bauke Padding
	Port authority (HBR)	Havenbedrijf Rotterdam	Mr. Jurien Duintjer
Technology providers	Port community system	Port infolink	Mr. Iwan van der Wolf
PROTECT project team	University	(RSM) Erasmus University Rotterdam	Mr. Marcel van Oosterhout
	University	TU Delft	Mr. Jan van den Berg
	Knowledge Institute	TNO	Mr. Thierry Verduijn and later on Ms. Sandra Krupe

Table 20: List of the attendees of expert brainstorm sessions

C. Appendix: Interviewed supply chain actors

In the following table, the organizations in the different categories that were interviewed for the research in work package 5.1.

Nr.	Category	Organization name	Interviewee	Date
1	Port community system	Port infolink	Mr. Iwan van der Wolf	2006-07-25
2	Port authority (HBR)	Havenbedrijf Rotterdam	Mr. Gerard van Hasselt	2006-07-14
3	Sea terminal	ECT	Mr. Bart Vermeer	2006-08-01
4	Road operator	Intern. Transport Overbeek b.v.	Mr. Kees Overbeek Jr.	2006-08-08
5	Customs	Dutch Customs	Mr. Henry Nugteren and Mr. Bauke Padding	2006-08-29
6	Insurance company	Aon Risk Management	Mr. Evert J. van der Meer and Mr. Jasper van der Horst	2006-09-21
7	Seaport police	Zeehavenpolitie	Mr. Nico Dubois	2006-09-28
8	LSP	Kuehne+Nagel	Mr. Cor Bakker, Mr. Wilko van Wijk and Mr. Leo de Jong	2006-09-29
9	Shipping line (agent)	Maerskline	Mr. Partick Mertens	2006-09-29
10	Container integrity system	Siemens	Mr. Gijsbert Huygen and Mr. Robin de Gruijter	2006-10-03
11	Barge operator	Centraal Bureau voor de Rijn- en Binnenvaart (CBRB)	Ms. Maira van Helvoirt	2006-10-06
12	Shipper	Heineken	Mr. René Polfliet	2006-10-11
13	Rail operator	Rail Service Center Rotterdam	Mr. H. Knegt	2006-10-11

Table 21: List of the interviewed SC actors

D. Appendix: Attendees of validation workshop

In the following table, the participants of the validation workshop for work package 5.1 and 5.2 are summarized. The validation workshop was held at Port infolink and was primarily meant for discussing results from the information analysis from work package 5.1 and the results from work package 5.2.

Category	Organization type	Organization name	Participant
Authorities	Customs	Dutch Customs	Mr. Henk van Pelt, Mr. H. van der Kooij and Mr. Bauke Padding
	Port authority (HBR)	Havenbedrijf Rotterdam	Mr. Jurien Duintjer
Business (Supply Chain) Parties	Sea terminal	ECT	Mr. Bart Vermeer
Technology providers	Port community system	Port infolink	Mr. Iwan van der Wolf
	Container integrity system	Siemens	Mr. Gijsbert Huygen
PROTECT project team	The Ministry of Transport, Public Works and Water Management	Ministerie van Verkeer en Waterstaat	Mr. Thierry Verduijn
	University	Erasmus University Rotterdam	Mr. Marcel van Oosterhout
	University	TU Delft	Mr. Jan van den Berg
	Knowledge Institute	TNO	Ms. Sandra Krupe

Table 22: List of the attendees of the validation workshop

E. Appendix: Import and Export schemes

Following two figures are the import and export process schemes which are used as basis for the further analysis of the SCS in this thesis.

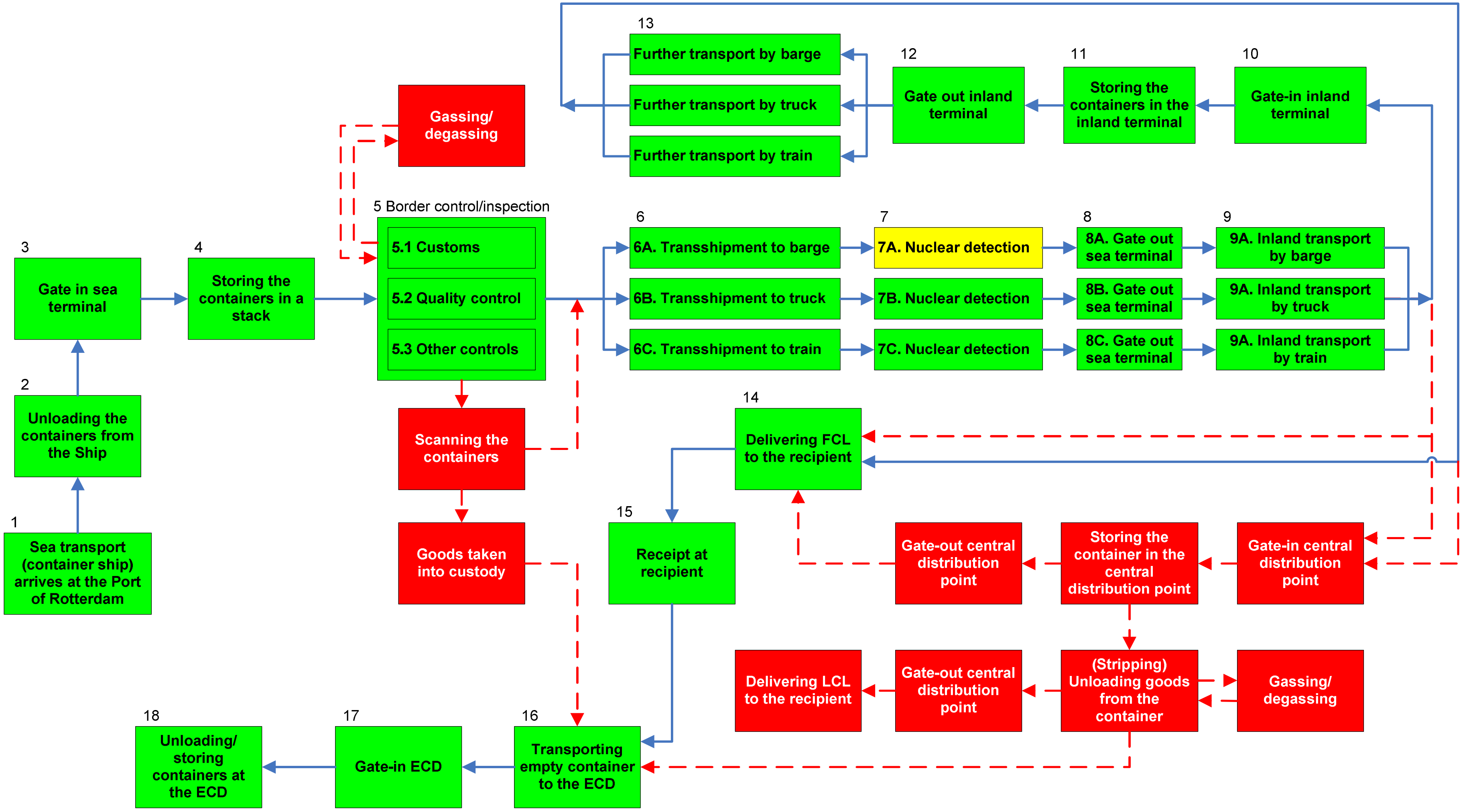

13
Further transport by barge
Further transport by truck
Further transport by train
12
Gate out inland terminal
11
Storing the containers in the inland terminal
10
Gate-in inland terminal
Gassing/ degassing
5 Border control/inspection
5.1 Customs
5.2 Quality control
5.3 Other controls
3
Gate in sea terminal
4
Storing the containers in a stack
6
6A. Transshipment to barge
6B. Transshipment to truck
6C. Transshipment to train
7
7A. Nuclear detection
7B. Nuclear detection
7C. Nuclear detection
8
8A. Gate out sea terminal
8B. Gate out sea terminal
8C. Gate out sea terminal
9
9A. Inland transport by barge
9A. Inland transport by truck
9A. Inland transport by train
2
Unloading the containers from the Ship
Scanning the containers
14
Delivering FCL to the recipient
1
Sea transport (container ship) arrives at the Port of Rotterdam
Goods taken into custody
15
Receipt at recipient
Gate-out central distribution point
Storing the container in the central distribution point
Gate-in central distribution point
Delivering LCL to the recipient
Gate-out central distribution point
(Stripping) Unloading goods from the container
Gassing/ degassing
18
Unloading/ storing containers at the ECD
17
Gate-in ECD
16
Transporting empty container to the ECD

Figure 24: Carriage of goods import

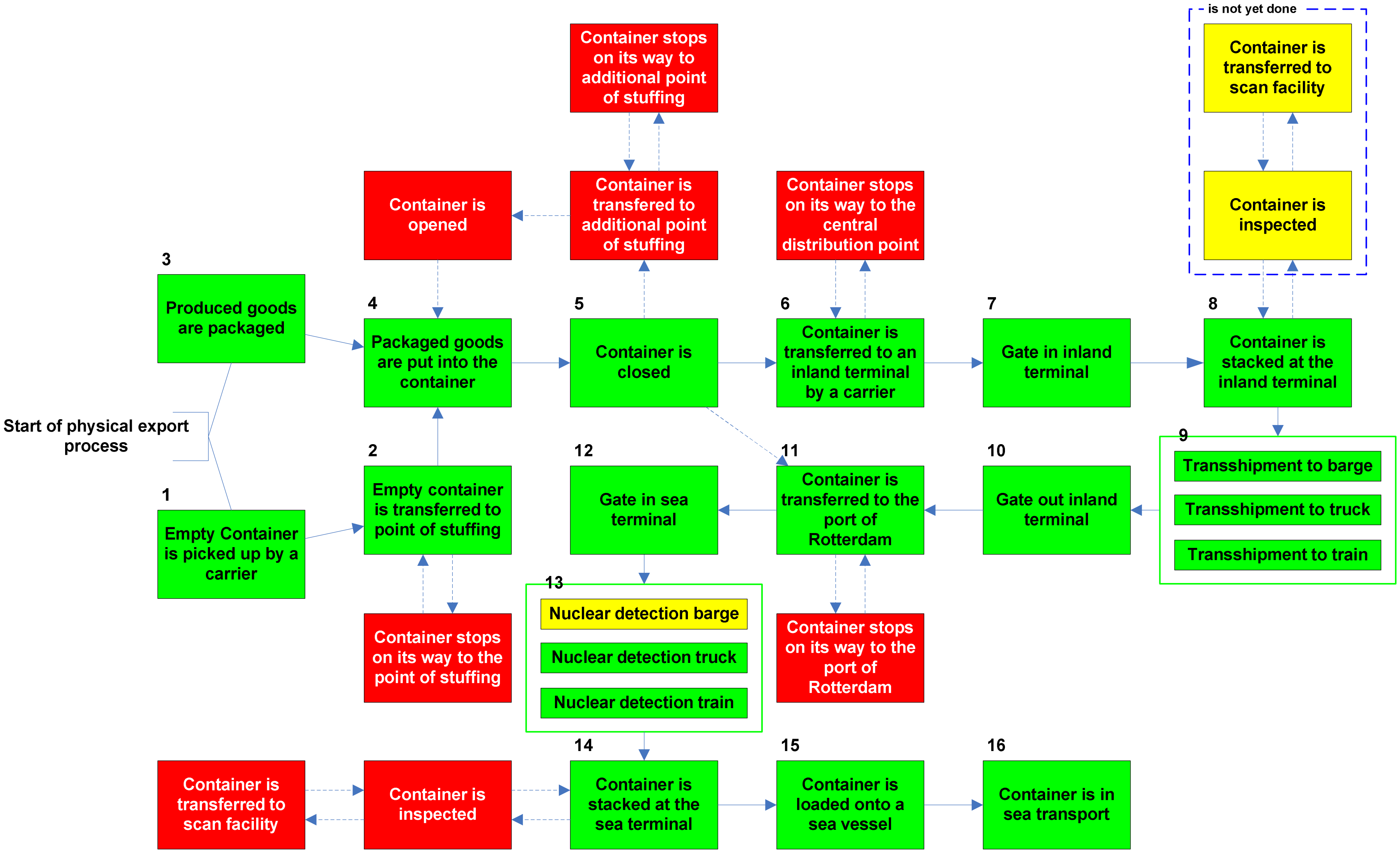

is not yet done
Container is transferred to scan facility
Container is inspected
Container stops on its way to additional point of stuffing
Container is opened
Container is transfered to additional point of stuffing
Container stops on its way to the central distribution point
3
Produced goods are packaged
4
Packaged goods are put into the container
5
Container is closed
6
Container is transferred to an inland terminal by a carrier
7
Gate in inland terminal
8
Container is stacked at the inland terminal
Start of physical export process
2
Empty container is transferred to point of stuffing
12
Gate in sea terminal
11
Container is transferred to the port of Rotterdam
10
Gate out inland terminal
9
Transshipment to barge
Transshipment to truck
Transshipment to train
1
Empty Container is picked up by a carrier
Container stops on its way to the point of stuffing
13
Nuclear detection barge
Nuclear detection truck
Nuclear detection train
Container stops on its way to the port of Rotterdam
14
15
16
Container is transferred to scan facility
Container is inspected
Container is stacked at the sea terminal
Container is loaded onto a sea vessel
Container is in sea transport

Figure 25: Carriage of goods export

F. List of abbreviations

CIS	Container Integrity System
CSD	Container Security Device
DCMR	DCMR Milieudienst Rijnmond
DNV	Det Norske Veritas
ECD	Empty Container Depot
EVO	Eigen vervoerders organisatie (Private transporters organization)
FCL	Full Container Load
GPS	Global Positioning System
IT	Information Technology
LCL	Less then full Container Load
PCS	Port Community System
PD	Plantenziektekundige Dienst (Plant Health Division)
POS	Point Of Stuffing
RFID	Radio Frequency Identification
SC	Supply Chain
SCS	Supply Chain Security
TNO	Nederlandse Organisatie voor toegepast-natuurwetenschappelijk onderzoek (Dutch organization for scientific research)
TLN	Transport and logistiek Nederland (Dutch transport and logistic organization)
V&W	Ministerie van Verkeer en Waterstaat (Ministry of transport, public works and water management)
VWA	Voedsel en Waren Autoriteit (Food and consumer product safety authority)

G. Appendix: Analysis of threats and risks, measures and information needs (import)

The following table presents the analysis for threat and risks, measures and the information which is needed. This analysis is based on import process.

				Threats				
Processes	Actors involved	Signals	Importance (Low Medium High)	Terrorism	Theft	Smuggle	Measures (p)reventive, (d)etective, (c)orrective, (cur)rent, (f)uture	Information needs
1. Container vessel arrives at the Port of Rotterdam	Directly involved: - Sea terminal operator (Haven meester) Indirectly invoved:	The container vessel/ cargo is coming from a suspicious country/ port of origin or shipper	h	x		x	Handling the container vessel with exceptional care (Possible security allert) (p)	- the country of departure - the history of country of departure - date of departure - date of (expected) arrival - complete route description - complete and detailed list of all BLs
		Vessel contains containers that are not on the pre-arrival container list	m	x		x	Install active RFID readers in the container cranes (d) (f)	- containers with RFID tags - origin of the container - sender information - destination of the container - beneficiary information ???
		Vessel contains containers with explosive/chemical/dangerous material	h	x		x	Control at sea and routing the vessel to a pre-defined port (p)	- total number of containers on board - type of material on board - sender of the container - beneficiary of the container
	Directly involved: - Sea Port Police - Ship Agent Indirectly invoved:	Unauthorized people are or have been on board. Container is being tempered by people/personnel on board	h	x	x	x	Document control (authentication) (c)	- pre-arrival information - number of people on board - nationalities/status
							Check (c) (p) crew / passenger list	- identity - nationality - how & when he/she got on board
		On board incidents are reported	m	x	x	x	Informing the parties to which it may concern (Police, Ambulance, Firefighter, Customs, etc.) (c) (p)	- the nature of incident - people involved - goods involved
2. Unloading the containers from the container vessel	Directly involved: - Sea terminal operator - Shipping line Indirectly involved: - ship broker - shipping line agent - shipping company	Unauthorized people are at the location. Container is being tempered by personnel	h	x	x	x	Access control (p) (d) (c)	- access badges - validation - company he/she working for - known/unknown
		Container is discharged while not on discharge/ pre-arrival list	l	x	x	x	Comparison discharge/ pre-arrival list with the discharged confirmation (p) (c)	- all descharged container numbers - total number of containers to be discharged (pre-arrival list) - total number of discharged containers - identity crane operator
		Container is stolen	h	x	x		Verify person who picks up the container. Terminal proces & staff or automated (d) (c)	- identity of person/company who is picking up the container - genuine container pickup message

3. Gate in Sea terminal	Directly involved: - Sea terminal operator Indirectly involved: - Sea Port Police	Container is not sealed	h	x	x	x	Container should be sealed after a risk analysis is conducted (possibly scanning the container to reduce the risk) (c) (cu)	- information relevant for scan decision - information about the sender and receiver
		Container is sealed just before departure to the Port of Rotterdam	m	x	x	x	Adding a time code to the seal ensures that the time the seal was affixed/closed can be monitored. Sealing the container just before departure to the Port of Rotterdam increases the risk of the container. (d) (f)	- closing time container - closing location container - closing authority container
		Container contains goods to be smuggled	h	x		x	Check (electronic) seal status (d) (f)	- seal status - seal affixed/close time
							Verify person who delivers the container (d) (c) (cur)	- identity of person/company who is delivering the container - genuine container delivery message
							Random inspection at gate in (moment of descharge) (d) (f)	- supposed contents - previous scan results - last inspection time - open/close time container Output: - Inspection result for future use
		Container contains goods to be used in a terrorist attack (disruption of logistic process)	h	x		x	100% scanning of incoming containers with passive radiological scanning (d) (f)	- scan status - previous scan results Output: - scan result for future use
							Checking of previous scan results (d) (f)	- previous scan results - last inspection time - content - open/close time container
							Verify person who delivers the container (d) (c) (cur)	- identity of person/company who is delivering the container - genuine container delivery message
							Random inspection at the gate entrance (d) (f)	- supposed contents - previous scan results - last inspection time - open/close time container Output: - inspection result for future use
4. Storing the containers in a temporary stack (Terminal)	Directly involved: - Sea terminal operator Indirectly invoved:	Container is stolen	h	x	x		Access control (p) (c)	- list of authorized personnel
							Physical security measures (gates, fences, cameras etc.) (p) (c)	- certification information - compliances
							Tracking (d) (f)	- location information (actual/supposed)
							Motion detection (d) (f)	- motion information (actual/supposed)
							Fences and Camera surveillance (c) (f)	- status information - begin and end time of storage - archive of footage
							Background checks of personnel (Screening) (p) (c)	- check in and check out time employees - date of last (updated) background check)
		Contents of container is stolen	h	x	x		Motion detection inside container (d) (f)	- motion information interior actual - status information
							Motion detection compound (d) (c)	- activity information (should there be activity in the section where the motion was detected)
							Light sensors inside the containers (d) (f)	- light information interior actual - status information
							Camera surveillance (c) (f)	- begin and end time of storage - archive of footage
							Access control (p) (c)	- list of authorized personnel
							Tracking of individual packaged goods (d) (f)	- location information of corresponding container (actual / supposed) - location information of individual packaged goods (actual / supposed)
							Closing and sealing container (p) (c)	- lock status (actual / supposed) - seal present - status information
		Illegal material is put in the container	h	x		x	Random checks (d) (f) + measures 1,2,3,4 and 6 from previous threat	- administration of incidents - certification - weight information for comparison
		Fake seal is used	h	x	x	x	Verify the seal number (p)(c)	- container seal number - container seal status - container seal time - person who sealed the container

5. Border control/inspections	Directly involved: - Customs - Quality control authorities - Other control authorities Indirectly involved: Seaport Police	Container is from a suspicious country of origin	h	x	x	x	Stack the container at a separate location (p) (c)	- type of container - sender information - beneficiary information
							Send the container to (nuclear) scan facility (p) (d) or a physical control	- content of the container - scan images - scan data
		Container contains dangerous goods/material	h	x		x	Instructions for further transport (c)	- route information - beneficialry information - carrier information
							Container/goods are checked (to be taken into custody) (d) (c)	- type of goods/materials - pre-arrival notification information - information about the party to further handle the goods that are taken into custody
6. Transshipment to a carrier	Directly involved: - Terminal operator - Carrier - Road operator - Barger operator - Rail operator Indirectly involved:	Container is picked up by wrong/unauthorized carrier	m	x	x	x	Access control (p)	- identity of the carrier operator - carrier - identification information - authentication information
7. Nuclear detection	Directly involved: - Sea terminal operator - Carrier - Road operator - Barger operator - Rail operator Indirectly involved: - Forwarder	The container contains nuclear material	h	x		x	Process is already a measure for detecting nuclear maretial in the container that can be used in a terrorist attack	all the information mentioned at process 1. Container vessel arrives at the Port of Rotterdam
8. Gate out Sea terminal	Directly involved: - Sea terminal operator - Cargo Agent - Carrier - Road operator - Barger operator - Rail operator Indirectly involved: - Forwarder	Container is stolen	h	x	x	x	Verify operator/ person who picks up the container (d) (c)	- pre-notification information - identity of person/company who is picking up the container - genuine container pickup message ??? - checked release order from cargo agent - check booking number
9. Inland transport by a carrier	Directly involved: - Pre-carrier - Road operator - Barger operator - Rail operator Indirectly involved: - Forwarder	Container is stolen during transport	h	x	x	x	Avoid transport stops (p) (f)	- planning information
							Tracking (d) (f)	- location information (actual / supposed)
							Locking container (the container is a less interesting target) (p) (c)	- seal present - status information
		Contents of container are stolen during transport	h	x	x		Locking container (p) (c)	- seal present - status information
		Contents of container is used in a terrorist attack	h	x			Avoid high-risk areas during transport (p) (f)	- location of high-risk areas - current scan status (if scanned thoroughly high risk areas do not have to be avoided
							Decentralized nuclear detection in key transport junctions (p/d) (f)	- current scan status - supposed contents of container - unique identifier of container
10. Gate in inland terminal	Directly involved: - Carrier - Road operator - Barger operator - Rail operator - Inland terminal operator Indirectly involved:	Container is not sealed	h	x	x	x	Container should be sealed after a risk analysis is conducted (possibly scanning the container to reduce the risk) (c) (f)	- information relevant for scan decision
		Container contains illegal material	h	x		x	Access control (p) (c)	- list of authorized personnel
							Verify operator/ person who delivers the container (d) (c)	- identity of person/company who is delivering the container - genuine container delivery message - pre/notificationterminal visit

11. Storing the containers in the inland terminal	Directly involved: - Inland terminal operator Indirectly involved:	Container is stolen	h	x	x	x	Access control (p) (c)	- list of authorized personnel
							Physical security measures (gates, fences etc.) (p) (c)	- certification information - compliances
							Tracking (d) (f)	- Location information (actual / supposed)
							Motion detection (d) (f)	- motion information (actual / supposed)
							Camera surveillance (c) (f?)	- status information - begin and end time of storage - archive of footage
							Background checks of personnel (p) (c)	- check in and check out time employees - date of last (updated) background check)
		Contents of container are stolen	h	x	x		Motion detection inside container (d) (f)	- motion information interior actual - status information
							Motion detection compound (d)	- activity information (should there be activity in the section where the motion was detected)
							Camera surveillance (c) (f)	- begin and end time of storage - archive of footage
							Access control (p) (c)	- list of authorized personnel
							Tracking of individual packaged goods (d) (f)	- location information of corresponding container (actual / supposed) - location information of individual packaged goods (actual / supposed)
							Locking container (p) (c)	- lock status (actual / supposed) - seal present - status information
		Container contains illegal material	h	x		x	Random checks (d) (f) + measures 1,2,3,4 and 6 from previous threat	- administration of incidents - certification - weight information for comparison
12. Gate out inland terminal	Directly involved: - Inland terminal operator - Carrier - Road opertator - Barger operator - Rail operator Indirectly involved: - Forwarder	Same as 8. Gate out Sea terminal	etc	x	x	x		
13. Further transport by a carrier	Directly involved: - Carrier - Road opertator - Barger operator - Rail operator Indirectly involved: - Forwarder	Same as 9. Inland transport by a carrier	etc					
14. Delivering FCL to the recipient	Directly involved: - Pre-carrier - Road operator - Barger operator - Rail operator - Recipient Indirectly involved:	The container arrived (too) late / lost the way	l	x	x	x	Install TT System (p) (f)	- departure time - expected/actual arrival time - carrier info - transport route
							Install navigation system (p) (f)	- departure address - destination address
		Same as 9. Inland transport by a carrier						
15. Receipt at recipient	Same as 14. Delivering FCL to the recipient	Container is not sealed/seal is broken	h	x	x	x	Send the container to (nuclear) scan/control facility (p) (d) (f)	- (expected) goods inside the container - (all) scan images - new scan images
							Verify the carrier information (c) (d)	- name (driver) - identification and authentication - company
							Request for TT information (f) (d) (c)	POS - sealed by (company/vesselper/person) - sealed at (location) - sealed on (date/time) - type of seal used - (planed) transport route - point(s) of detection - authorities that detected the container - authorities that controled/inspected the container
		Conatiner is sealed but the seal (number) is different than expected	h	x	x	x	Measures 1, 2 and 3 from previouse threats	- seal number - seal type - sealed by (company/vesselper/person) - sealed at (location) - sealed on (date/time) - (expected) material inside the container
		Container containes unexpected dangerous material	h	x		x	Measures 1, 2 and 3 from previouse threats	- same information as threat 1 and 2
		The content of the container is different than expected/goods are stolen	h	x	x	x	Measures 1, 2 and 3 from previouse threats	- same information as threat 1 and 2

16. Transporting empty container to the ECD	Directly involved: - Pre-carrier - Road operator - Barger operator - Rail operator Indirectly involved: - Forwarder	Empty container stolen	l	x	x	x	Avoid transport stops (p) (f)	- speed - reason for stopping (refuelling) - fuel prediction
							Tracking (d) (f)	- location information (actual / supposed)
		Illegal material is put into container	h	x		x	Locking container (p) (c)	- seal present - status information - weight
							Motion detection inside container (d) (f)	- motion information interior actual - status information
							Inspection of empty container (d) (p) (f?)	- last inspection time - content - open/close time container - weight of container
17. Gate in ECD	Directly involved: - Pre-carrier - Road operator - Barger operator - Rail operator - ECD Operator Indirectly involved:	Container not empty, contains goods to be smuggled	m	x		x	Random inspection before entering depot (d) (f)	- previous user container - risk profile users
							Weight comparison (d) (f)	- weight of container - actual weight of container
							Assigning of containers to jobs should be done randomly (this ensures that people that want to smuggle goods are never sure where a certain container is going. This reduces the attractiveness of stuffing an empty container) (p) (c)	- pool of available containers - pool of containers that can be used for the job (e.g. containers from a certain company)
							Check information system (d) (f)	- last inspection time - content - open/close time container
		Container is not empty, contains goods used in terrorist attack	h	x		x	Inspection (p) (c) + measures of previous threat	- suspected containers for "terrorist material" - last inspection time - content - open/close time container - weight of container
		Empty container stolen	l	x	x	x	Tracking (d) (f)	- location information (actual / supposed)
							Motion detection (d) (f)	- motion information (actual / supposed)
							Access control (p) (f?)	- list of authorized personnel
							Verify person who is delivering the container (p) (c)	- identity of person/company who is delivering the container - genuine container deliver message
18. Unloading/storing containers at the ECD	Directly involved: - ECD Operator Indirectly involved:	Container is prepared to be misused for terrorist attack, theft, smuggle, ect (Dubbel bodem)	h	x	x	x	Access control (p) (f?)	- access badges - validation - list of authorized personnel - registration
							Empty container seal (f?) (p)	- seal number - seal type - sealed on (date/time) - status (Controled?)
							Physical security measures (gates, fences, cameras etc.) (p) (c)	- certification information - compliances

Table 23: Analysis of threats and risks, measures and information needs (import)

H. Appendix: Analysis of threats and risks, measures and information needs (export)

The following table presents the analysis for threat and risks, measures and the information which is needed. This analysis is based on import process.

				Threats				
Processes	Actors involved	Signals	Importance (Low/Medium High)	Terrorism	Theft	Smuggle	Measures (p)reventive, (d)etective, (c)orrective, (cur)rent, (f)uture	Information needs
1. Empty Container is picked up by a carrier (road / barge / rail)	Directly involved: - Empty container depot - Pre-carrier - Road operator - Barger operator - Rail operator Indirectly involved: - Forwarder	Container not empty, contains goods to be smuggled	h	x		x	Random inspection before leaving depot (d) (f)	- previous user container - risk profile users
							Weight comparison (d) (f)	- weight of container - actual weight of container
							Assigning of containers to jobs should be done randomly (this ensures that people that want to smuggle goods are never sure where a certain container is going. This reduces the attractiveness of stuffing an empty container) (p) (c)	- pool of available containers - pool of containers that can be used for the job (e.g. containers from a certain company)
							Check information system (d) (f)	- last inspection time - content - open/close time container
		Container not empty, contains goods used in terrorist attack	h	x		x	Inspection (p) (c) + measures of previous threat	- suspected containers for "terrorist material" - last inspection time - content - open/close time container - weight of container
		Empty container stolen	l	x	x	x	Tracking (d) (f)	- location information (actual / supposed)
							Motion detection (d) (f)	- motion information (actual / supposed)
							Access control (p) (f?)	- list of authorized personnel
							Verify person who is picking up the container (p) (c)	- identity of person/company who is picking up the container - genuine container pickup message
2. Empty container is transferred to point of stuffing (POS)	Directly involved: - Pre-carrier - Road operator - Barger operator - Rail operator Indirectly involved: - Forwarder	Empty container stolen	l	x	x	x	Minimum speed (p) (f)	- speed - reason for stopping (refuelling) - fuel prediction
							Tracking (d) (f)	- location information (actual / supposed)
		Illegal material is put into container	h	x		x	Locking container (p) (c)	- seal present - status information
							Motion detection inside container (d) (f)	- motion information interior actual - status information
							Inspection at POS (d) (f?)	- last inspection time - content - open/close time container - weight of container

3. Produced goods are packaged	Directly involved: - Shipper Indirectly involved: - Forwarder	Illegal material is packaged	h	x		x	Random checks (d) (f)	- administration of incidents - certification - weight information for comparison
							Access control (p) (f?)	- list of authorized personnel
		Material packaged for terrorist attack	h	x		x	Random checks (d) (f)	- administration of incidents - certification - weight information for comparison
							Access control (p) (f?)	- list of authorized personnel
		Theft of material to be packaged	m	x	x	x	Random checks (d) (f)	- administration of incidents - certification - weight information for comparison
							Tracking (d) (f)	- location information of individual articles (within compound or globally)
							Security gate detection (d) (f?)	- identification of individual articles (are they allowed to leave or should they be on the premises)
							Access control (p) (f?)	- list of authorized personnel
4. Packaged goods are put into the container	Directly involved: - Shipper - Pre-carrier - Road operator - Barger operator - Rail operator Indirectly involved: - Forwarder	Packaged goods are goods to be smuggled or can be used in a terrorist attack	h	x		x	Random checks (d) (f)	- administration of incidents - weight information of consignments or even individual articles - supposed contents
							Access control (p) (f?)	- list of authorized personnel
							Scan the packaged goods (d) (f)	- administration of incidents - supposed contents
		Packaged goods are exchanged for illegal goods (e.g. by the loading personnel at POS)	h	x		x	Truck driver checks if all goods are present (d) (c?)	- unique identifier of cargo items or articles - consignment(s) information
							Contents of container is scanned when container is closed (d) (f)	- unique identifier of cargo items or articles - unique identifier of container - consignment(s) information
							Access control (p) (f?)	- list of authorized personnel
							Camera surveillance (c) (f?)	- begin time and end time of stuffing - archive of footage
		Packaged goods are stolen during loading of the container	h	x	x		Weight comparison (d) (f)	- weight information of consignments or even individual articles - weight of container
							Truck driver checks if all goods are present (d) (c?)	- unique identifier of cargo items or articles - unique identifier of container - consignment(s) information
							Contents of container is scanned when container is closed (d) (f)	- unique identifier of cargo items or articles - unique identifier of container - consignment(s) information
							Access control (p) (f?)	- list of authorized personnel
							Camera surveillance (c) (f?)	- begin time and end time of loading - archive of footage
		Packaged goods are stolen by the truck driver	h	x	x		Verify person who is delivering the empty container and the person driving away with the loaded container (not necessarily the same person) (d) (c)	- identity of person/company who is delivering and picking up the container - genuine container stuffing and pickup message

5. Container is closed	Directly involved: - Pre-carrier - Road operator - Barger operator - Rail operator Indirectly involved: - Forwarder	Container is not sealed properly	h	x	x	x	Remote monitoring of container seal (d) (f)	- seal status
							Procedural check of container seal (e.g. by truck driver) (d) (f?)	Output: - seal has been checked
6. Container is transferred to an inland terminal by a carrier	Directly involved: - Pre-carrier - Road operator - Barger operator - Rail operator Indirectly involved: - Forwarder	Container is stolen during transport	h	x	x	x	Minimum speed (p) (f)	- speed
							Tracking (d) (f)	- location information (actual / supposed)
							Locking container (the container is a less interesting target) (p) (c)	- seal present - status information
		Contents of container is stolen during transport	h	x	x	x	Locking container (p) (c)	- seal present - status information
		Contents of container are used in a terrorist attack	h	x	x		Avoid high-risk areas during transport (p) (c?)	- location of high-risk areas - current scan status (if scanned thoroughly high risk areas do not have to be avoided)
							Decentralized nuclear detection in key transport junctions (p/d) (f)	- current scan status - supposed contents of container - unique identifier of container
7. Gate in inland terminal	Directly involved: - Pre-carrier - Road operator - Barger operator - Rail operator - Inland terminal operator Indirectly involved: - Forwarder	Container is not sealed	h	x	x	x	Container should be sealed after a risk analysis is conducted (possibly scanning the container to reduce the risk) (c) (f)	- information relevant for scan decision
		Container contains illegal material	h	x		x	Access control (p) (c)	- list of authorized personnel
							Verify person who delivers the container (d) (c)	- identity of person/company who is delivering the container - genuine container delivery message

8. Container is stacked at the inland terminal	Directly involved: - Inland terminal operator	Container is stolen	h	x	x	x	Access control (p) (c)	- list of authorized personnel
							Physical security measures (gates, fences etc.) (p) (c)	- certification information - compliances
							Tracking (d) (f)	- Location information (actual / supposed)
							Motion detection (d) (f)	- motion information (actual / supposed)
							Camera surveillance (c) (f?)	- status information - begin and end time of storage - archive of footage
							Background checks of personnel (p) (c)	- check in and check out time employees - date of last (updated) background check)
		Contents of container is stolen	h	x	x	x	Motion detection inside container (d) (f)	- motion information interior actual - status information
							Motion detection compound (d) (c?)	- activity information (should there be activity in the section where the motion was detected)
							Camera surveillance (c) (f?)	- begin and end time of storage - archive of footage
							Access control (p) (c)	- list of authorized personnel
							Tracking of individual packaged goods (d) (f)	- location information of corresponding container (actual / supposed) - location information of individual packaged goods (actual / supposed)
							Locking container (p) (c)	- lock status (actual / supposed) - seal present - status information
		Illegal material in container	h	x		x	Random checks (d) (f) + measures 1,2,3,4 and 6 from previous threat	- administration of incidents - certification - weight information for comparison
9. Transhipment to inland transport	Directly involved: - Inland terminal operator - Pre-carrier - Road operator - Barger operator - Rail operator Indirectly involved: - Forwarder	Container is stolen	h	x	x	x	Verify person who picks up the container (d) (c)	- identity of person/company who is picking up the container - genuine container pickup message
10. Gate out inland terminal	Directly involved: - Inland terminal operator - Pre-carrier - Road operator - Barger operator - Rail operator Indirectly involved: - Forwarder	Container is stolen	h	x	x	x	Verify person who picks up the container (d) (c)	- identity of person/company who is picking up the container - genuine container pickup message

11. Container is transferred to the port of Rotterdam	Same as 6.	Same as 6.						
12. Gate in sea terminal	Directly involved: - Sea terminal operator - Pre-carrier - Road operator - Barger operator - Rail operator Indirectly involved: - Forwarder	Container is not sealed	h	x	x	x	Container should be sealed after a risk analysis is conducted (possibly scanning the container to reduce the risk) (c) (c)	- information relevant for scan decision
		Container is sealed just before entering the Port of Rotterdam	m	x	x	x	Adding a time code to the seal ensures that the time the seal was affixed/closed can be monitored. Sealing the container just before entrance of the Port of Rotterdam increases the risk of the container. (d) (f)	- close time container
							Monitoring of parking place surrounding gate in (d/c) (f)	- window of opportunity of affixing the seal or closing of container - archive of footage
		Container contains goods to be smuggled	h	x		x	Check seal status (d) (f)	- seal status - seal affixed/close time
							Verify person who delivers the container (d) (c)	- identity of person/company who is delivering the container - genuine container delivery message
							Random inspection at gate entrance (d) (f?)	- supposed contents - previous scan results - last inspection time - open/close time container Output: - Inspection result for future use
		Container contains goods to be used in a terrorist attack (disruption of logistic process). Economic risk is higher than risk of loss of life. Especially interesting for offshore port because they don't have to scan (or are more sure about) the contents of the container.	h	x		x	100% scanning of incoming containers with passive radiological scanning (d) (nearf)	- Scan status - Previous scan results Output: - Scan result for future use
							Checking of previous scan results (d) (f)	- previous scan results - last inspection time - content - open/close time container
							Verify person who delivers the container (d) (c)	- identity of person/company who is delivering the container - genuine container delivery message
							Random inspection at gate entrance (d) (f?)	- supposed contents - previous scan results - last inspection time - open/close time container Output: - inspection result for future use
13. Nuclear detection	Directly involved: - Sea terminal operator - Pre-carrier - Road operator - Barger operator - Rail operator Indirectly involved: - Forwarder	Process is already a measure for detecting contents of the container that can be used in a terrorist attack	h	x	x	x		
14. Container is stacked at the sea terminal	Directly involved: - Sea terminal operator	Same as 8.						
15. Container is loaded onto a sea vessel	Directly involved: - Sea terminal operator - Shipping line Indirectly involved: - Ship broker - Shipping line agent - Shipping company	Container is stolen	h	x	x	x	Verify person who picks up the container (d) (c)	- identity of person/company who is picking up the container - genuine container pickup message
16. Container is in sea transport	Directly involved: - Shipping line Indirectly involved: - Ship broker - Shipping line agent - Shipping company	Container is stolen	h	x	x	x	Tracking (d) (f)	- location information (actual / supposed)
							Background checks of personnel (p) (c)	- date of last (updated) background check)
		Container is used in a terrorist attack	h	x			Should actually be prevented in an earlier stage of transport (p)	- inspection/scan results - nuclear detection at earlier stage of export process
							Crisis management (c) (f?)	- crisis management plan

Table 24: Analysis of threats and risks, measures and information needs (export)

I. Appendix: Complete list of information blocks

The following table presents the complete list of the information blocks, their characteristics and data about the availability.

				Characteristics of Data			Timing																	
							Import									Export								
#	Category	Data element	Options / values	Mandatory	Prefer	Importance (Low, Medium, High)	PCS	Container Integrity System	Authority Systems (Customs, Port Authorities)	Business (Community) Systems	Electronic Availability	PCS || CIS	PCS || Authority Systems	PCS || CIS || Authority Systems	BCS && !(PCS || CIS || Authority Systems)	PCS	Container Integrity System	Authority Systems (Customs, Port Authorities)	Business (Community) Systems	Electronic Availability	PCS || CIS	PCS || Authority Systems	PCS || CIS || Authority Systems	BCS && !(PCS || CIS || Authority Systems)
1	Container (general)	container number		x		h	x	x	x	x	x	x	x	x		x (1&2)	x	x (2)	x	x	x	x	x	
		booking number			x		?	?	?	?	?					?	?	?	?	?				
		container status	Empty (yes/no/residue)	x			x		x		x	x	x	x		x		x		x	x	x	x	
			Clean (yes/no)	x																				
			Sealed (yes/no)	x		h	x	x	x		x	x	x	x		x (1&2)	x	x (2)		x	x	x	x	
			Controlled (yes/no)		x		x	?	x		x	x	x	x		x	?	x		x	x	x	x	
			Controlled for		x		x		x		x	x	x	x		x		x		x	x	x	x	
			Controlled by		x		x		x		x	x	x	x		x		x		x	x	x	x	
			Damaged (yes/no)		x																			
			Nuclear scanned (yes/no)	x		h			x									x						
		container owner			x		x	x	x		x	x	x	x		x (1&2)	x	x (2)		x	x	x	x	
		ISO code	size.type	x			x		x		x	x	x	x		x (1&2)		x (2)		x	x	x	x	
		RFID tag (only for smart containers)	Yes/No/Active/Passive		x			x			x	x		x			x			x	x		x	
		scanned	Yes/No	x		h	x		x		x	x	x	x		x		x		x	x	x	x	
		gassing	Gassed/degassed	x			x		x		x	x	x	x		x (1&2)		x (2)		x	x	x	x	
		gas-description		x			x		x		x	x	x	x		x (1&2)		x (2)		x	x	x	x	
		TARRA		x		h	x		x		x	x	x	x		x (1&2)		x (2)		x	x	x	x	
		container integrity	Ok / not OK	x		h		x			x	x		x			x			x	x		x	
		temperature changes	Yes/No		x			x	x		x	x	x	x			x	x		x	x	x	x	
		intrusion	Yes/No		x			x	x		x	x	x	x			x	x		x	x	x	x	
		light changes	Yes/No		x			x	x		x	x	x	x			x	x		x	x	x	x	
2	Seal	seal number		x		h	x	x	x		x	x	x	x		x (1&2)	x	x (2)		x	x	x	x	
		location of sealing		x		h		x			x	x		x			x			x	x		x	
		time of sealing			x	h		x			x	x		x			x			x	x		x	
		sealed by	Consignor / Operator / Authority	x		h	x		x		x	x	x	x		x (1&2)		x (2)		x	x	x	x	
		seal status/integrity	Ok / broken / damaged	x		h	x	x	x		x	x	x	x		x (1&2)	x	x (2)		x	x	x	x	
			Broken	x		h	x	x	x		x	x	x	x		x (1&2)	x	x (2)		x	x	x	x	
			Damaged	x		h	x	x	x		x	x	x	x		x (1&2)	x	x (2)		x	x	x	x	
			Change history	x		h	x	x	x		x	x	x	x		x (1&2)	x	x (2)		x	x	x	x	
		seal type	Physical, e Seal, Bold seal with RFID, Container security device		x		x		x		x	x	x	x		x (1&2)		x (2)		x	x	x	x	
3	Nuclear scan	location of scan	seaterminal, inland terminal etc	x		h			x		x		x	x				x		x		x	x	
		results of scan	Ok / Not Ok	x		h			x									x						
		type of scan	1st line / 2nd line etc		x																			

4	X Ray scanning (container contents)	container scan type	1st line (low capacity) / 2nd line (high capacity X Ray)	x					x									x						
		container scan location	sea terminal, inland terminal etc	x			x		x		x	x	x	x		x		x		x	x	x	x	
		container scan results	ok, not analyzed / ok, analyzed, not OK	x		h	x		x		x	x	x	x		x		x		x	x	x	x	
		scanning details	scan photo		x				x		x		x	x				x		x		x	x	
			scanning time/date	x			x		x		x	x	x	x		x		x		x	x	x	x	
5	Operators (general)	operator ID		x		h	x		x		x	x	x	x		x (1&2)		x (2)		x	x	x	x	
		operator details	name/address information		x		x		x		x	x	x	x		x (1&2)		x (2)		x	x	x	x	
		operator certified	Yes	x			x (future)		x		x	x	x	x		x (future)		x (2)		x	x	x	x	
		operator type of certificate	ISPS/AEO/--		x		x (future)		x		x	x	x	x		x (future)		x		x	x	x	x	
		operator certificate details	Date/time of issue		x (future)	h	x (future)		x		x	x	x	x		x (future)		x		x	x	x	x	
			Issuing authority		x (future)	h	x (future)		x		x	x	x	x		x (future)		x		x	x	x	x	
			Valid utill		x (future)	h	x (future)		x		x	x	x	x		x (future)		x		x	x	x	x	
6A	Road operator	operator ID		x		h	x			x	x	x	x	x		x				x	x	x	x	
		cargo card ID		x			x			x	x	x	x	x		x				x	x	x	x	
		driver ID		x			x			x	x	x	x	x		x				x	x	x	x	
6B	Truck details	truck ID		x			x			x	x	x	x	x		x				x	x	x	x	
		truck number plate		x			x			x	x	x	x	x		x				x	x	x	x	
		brand	Volvo, Mercedes Benz, Man, ---		x					x	x				x				x	x				x
		owner	Name (company)		x					x	x				x				x	x				x
			Address		x					x	x				x				x	x				x
6C	Truck driver details	driver ID		x		h	x			x	x	x	x	x		x				x	x	x	x	
		personal details	name/address information		x		x			x	x	x	x	x		x				x	x	x	x	
			Biometric details	x			x			x	x	x	x	x		x				x	x	x	x	
		driver status	OK/Black list	x			x			x	x	x	x	x		x				x	x	x	x	
7A	Rail operator	operator ID		x		h	x			x	x	x	x	x		x				x	x	x	x	
		train number		x			x			x	x	x	x	x		x				x	x	x	x	
7B	Train details	train ID/number		x		h	x			x	x	x	x	x		x				x	x	x	x	
		train owner	Name (company)		x		x			x	x	x	x	x		x				x	x	x	x	
			Address		x		x			x	x	x	x	x		x				x	x	x	x	
8A	Barge operator	operator		x			x			x	x	x	x	x		x				x	x	x	x	
		barge name / ID		x		h	x			x	x	x	x	x		x				x	x	x	x	
8B	Barge details	barge name / ID		x			x			x	x	x	x	x		x				x	x	x	x	
		barge owner	Name (company)		x					x	x				x				x	x				x
			Address		x					x	x				x				x	x				x
9	Shipping line/ship details	operator		x			x		x		x	x	x	x		x		x		x	x	x	x	
		ship name / ID		x		h	x		x		x	x	x	x		x		x		x	x	x	x	
		ship owner	Name (company)		x		x		x		x	x	x	x		x		x		x	x	x	x	
			Address		x		x		x		x	x	x	x		x		x		x	x	x	x	
10	Personnel	personnel ID		x		h	x			x	x	x	x	x		x			x	x	x	x	x	
		personal details	Name/address information		x		x			x	x	x	x	x		x			x	x	x	x	x	
			Biometric details	x			x			x	x	x	x	x		x			x	x	x	x	x	
		organisation		x		h	x			x	x	x	x	x		x			x	x	x	x	x	
		job/function/profession		x						x	?				x				x	?				x
		screening	Yes	x						x	?				x				x	?				x
		access rights		x						x	x				x				x	x				x
		gender	Male/Female		x					x	x				x				x	x				x
11	Point of stuffing (STUF) or point of stripping (STRIP)	STUF/STRIP camera surveillance	Yes / No		x			x		x	x	x		x			x		x	x	x		x	
		STUF/STRIP location			x	h		x		x	x	x		x			x		x	x	x		x	
		cargo B/L		x				?		x	?				x		?		x	?				x
		STUF/STRIP sealing		x		h		x		x	x	x		x			x		x	x	x		x	
		gate in time STUF/STRIP			x			x		x	x	x		x			x		x	x	x		x	
		gate out time STUF/STRIP			x			x		x	x	x		x			x		x	x	x		x	
		container number		x				x		x	x	x		x			x		x	x	x		x	
		operator ID		x				x		x	x	x		x			x		x	x	x		x	

12	Cargo	B/L number		x		h	x		x	x	x	x	x	x		x		x	x	x	x	x	x	
		cargo value		x		h	x		x	x	x	x	x	x		x		x	x	x	x	x	x	
		cargo weight		x		h	x		x	x	x	x	x	x		x		x	x	x	x	x	x	
		cargo description		x		h	x		x	x	x	x	x	x		x		x	x	x	x	x	x	
		cargo item		x			x		x	x	x	x	x	x		x		x	x	x	x	x	x	
		cargo number of colli			x		x		x	x	x	x	x	x		x		x	x	x	x	x	x	
		cargo code		x			x		x	x	x	x	x	x		x		x	x	x	x	x	x	
		cargo origin certificate	Yes / No		x		?x		x		?					?x		x		?				
			cargo origin certificate details		x		?x		x		?					?x		x		?				
		cargo export certificate	Yes / No	x			?x		x		?					?x		x		?				
			cargo export certificate details	x			?x		x		?					?x		x		?				
		cargo health certificate	Yes / No	x			?x		x		x		x	x		?x		x		x		x	x	
			cargo health certificate details	x			?x		x		x		x	x		?x		x		x		x	x	
		cargo quality checked	Quality check organisation ID		x																			
			Yes/No	x		h	x		x		x	x	x	x		x		x		x	x	x	x	
		dangerous goods	Yes/No	x		h	x		x		x	x	x	x		x		x		x	x	x	x	
		dangerous goods type	IMO code/Chemical/Nuclear/--	x			x		x		x	x	x	x		x		x		x	x	x	x	
		country of origin		x		h	x		x		x	x	x	x		x		x		x	x	x	x	
		country of departure		x			x		x		x	x	x	x		x		x		x	x	x	x	
		consignor / shipper ID		x			x		x		x	x	x	x		x		x		x	x	x	x	
		consignee ID		x			x		x		x	x	x	x		x		x		x	x	x	x	
		container track history		x		h	x	x	x	x	x	x	x	x		x	x	x	x	x	x	x	x	
13	Process information on timing STUF/STRIP	expected time STUF/STRIP		x		h		?		x	?				x		?		x	?				x
		actual time of STUF/STRIP		x		h		x		x	x	x		x			x		x	x	x		x	
		expected time of departure from STUF/STRIP			x			?		x	?				x		?		x	?				x
		actual time of departure from STUF/STRIP		x				x		x	x	x		x			x		x	x	x		x	
14	Process information on timing inland terminal	ETA at inland terminal		x		h	x			x	x	x	x	x		x			x	x	x	x	x	
		ATA at inland terminal		x		h	x			x	x	x	x	x		x			x	x	x	x	x	
		ETD from inland terminal			x					x	?				x				x	?				x
		ATD from inland terminal		x						x	?				x				x	?				x
15	Process information on timing sea terminal	ETA at sea terminal		x		h	x			x	x	x	x	x		x			x	x	x	x	x	
		ATA at sea terminal		x		h	x			x	x	x	x	x		x			x	x	x	x	x	
		ETD from sea terminal			x		x			x	x	x	x	x		x			x	x	x	x	x	
		ATD from sea terminal		x		h	x			x	x	x	x	x		x			x	x	x	x	x	
16	Process information on timing container vessel	ETA of container vessel			x		x			x	x	x	x	x										
		ATA of container vessel		x			x			x	x	x	x	x										
		ETD of container vessel			x											x			x	x	x	x	x	
		ATD of container vessel		x												x			x	x	x	x	x	
17	Consignor (shipper)	consignor ID		x		h	x		x		x	x	x	x		x		x		x	x	x	x	
		consignor details	Name/address information	x			x		x		x	x	x	x		x		x		x	x	x	x	
		consignor certified	Yes/No	x		h	x (future)		x		x	x	x	x		x (future)		x		x	x	x	x	
		type of certificate	AEO/C-TPAT/--	x			x (future)		x		x	x	x	x		x (future)		x		x	x	x	x	
		certificate details	Date/time of issue		x (future)		x (future)		x		x	x	x	x		x (future)		x		x	x	x	x	
			Issuing authority		x (future)		x (future)		x		x	x	x	x		x (future)		x		x	x	x	x	
			Valid till		x (future)		x (future)		x		x	x	x	x		x (future)		x		x	x	x	x	
18	Consignee (final recipient)	consignee ID		x		h	x		x		x	x	x	x		x		x		x	x	x	x	
		consignee details	Name/address information	x			x		x		x	x	x	x		x		x		x	x	x	x	
		certified	Yes	x		h	x (future)		x		x	x	x	x		x (future)		x		x	x	x	x	
		type of certificate	AEO/C-TPAT/--	x			x (future)		x		x	x	x	x		x (future)		x		x	x	x	x	
		certificate details	Date/time of issue		x (future)		x (future)		x		x	x	x	x		x (future)		x		x	x	x	x	
			Issuing authority		x (future)		x (future)		x		x	x	x	x		x (future)		x		x	x	x	x	
			Valid till		x (future)		x (future)		x		x	x	x	x		x (future)		x		x	x	x	x	
19	Ports	port type	Port of origin/ Port of destination/ Port of transit/ Port of loading (POL)/ Point of discharge (POD)	x		h	x		x		x	x	x	x		x		x		x	x	x	x	
		port name		x			x		x		x	x	x	x		x		x		x	x	x	x	
		port ID		x		h	x		x		x	x	x	x		x		x		x	x	x	x	
		port city		x			x		x		x	x	x	x		x		x		x	x	x	x	
		port country		x			x		x		x	x	x	x		x		x		x	x	x	x	
		port security level	CSI/ISPS/--	x		h	x		x		x	x	x	x		x		x		x	x	x	x	
20	Sea terminal	terminal ID		x		h	x		x		x	x	x	x		x		x		x	x	x	x	
		terminal description		x			x		x		x	x	x	x		x		x		x	x	x	x	
		terminal security level	ISPS/AEO/--	x		h	x		x		x	x	x	x		x		x		x	x	x	x	
		camera surveillance	Yes/No		x		x		x		x	x	x	x		x		x		x	x	x	x	
21	Incidents	incident ID		x						x	?				x				x	?				x
		incident type		x		h				x	?				x				x	?				x
		incident location		x		h				x	?				x				x	?				x
		incident description	Container number		x					x	?				x				x	?				x
			Booking number		x					x	?				x				x	?				x
		operator ID		x						x	?				x				x	?				x
		management ID(s)		x						x	?				x				x	?				x
		CMP		x						x	?				x				x	?				x

Table 25: Complete list of information blocks

J. Appendix: List of information blocks (high importance only)

The following table presents the list of the information blocks and their characteristics. This table represents only the data elements of *high* importance.

				Characteristics of Data			Import									Export						
#	Category	Data element	Options / values	Mandatory	Prefer	Importance (Low, Medium, High)	PCS	Container Integrity System	Authority Systems (Customs, Port Authorities)	Business (Community) Systems	Electronic Availability	PCS || CIS	PCS || Authority Systems	PCS || CIS || Authority Systems	BCS && !(PCS || CIS || Authority Systems)	PCS	Container Integrity System	Authority Systems (Customs, Port Authorities)	Business (Community) Systems	PCS || Authority Systems	PCS || CIS || Authority Systems	BCS && !(PCS || CIS || Authority Systems)
1	Container (general)	container number				high	x	x	x	x	x	x	x	x		x (1&2)	x	x (2)		x	x	
		container status	Sealed (yes/no)	x		high	x	x	x		x	x	x	x		x (1&2)	x	x (2)		x	x	
			Nuclear scanned (yes/no)	x		high			x									x				
		scanned	Yes/No	x		high	x		x		x	x	x	x		x		x		x	x	
		TARRA		x		high	x		x		x	x	x	x		x (1&2)		x (2)		x	x	
		container integrity	Ok / not OK		x	high		x			x	x		x			x				x	
2	Seal	seal number		x		high	x	x	x		x	x	x	x		x (1&2)	x	x (2)		x	x	
		location of sealing		x		high		x			x	x		x			x				x	
		time of sealing			x	high		x			x	x		x			x				x	
		sealed by	Consignor / Operator / Authority	x		high	x		x		x	x	x	x		x (1&2)		x (2)		x	x	
		seal status/integrity	Ok / broken / damaged	x		high	x	x	x		x	x	x	x		x (1&2)	x	x (2)		x	x	
			Broken	x		high	x	x	x		x	x	x	x		x (1&2)	x	x (2)		x	x	
			Damaged	x		high	x	x	x		x	x	x	x		x (1&2)	x	x (2)		x	x	
			Change history	x		high	x	x	x		x	x	x	x		x (1&2)	x	x (2)		x	x	
3	Nuclear scan	location of scan	seaterminal, inland terminal etc.	x		high			x		x		x	x				x		x	x	
		results of scan	Ok / Not Ok	x		high			x									x				
	X Ray scanning (container contents)	container scan results	ok, not analyzed / ok, analyzed, not OK	x		high	x		x		x	x	x	x		x		x		x	x	
5	Operators (general)	operator ID		x		high	x		x		x	x	x	x		x (1&2)		x (2)		x	x	
		operator certificate details	Date/time of issue		x (future)	high	x (future)		x		x	x	x	x		x (future)		x		x	x	
			Issuing authority		x (future)	high	x (future)		x		x	x	x	x		x (future)		x		x	x	
			Valid utill		x (future)	high	x (future)		x		x	x	x	x		x (future)		x		x	x	
12	Cargo	B/L number		x		high	x		x	x	x	x	x	x		x		x	x	x	x	
		cargo value		x		high	x		x	x	x	x	x	x		x		x	x	x	x	
		cargo weight		x		high	x		x	x	x	x	x	x		x		x	x	x	x	
		cargo description		x		high	x		x	x	x	x	x	x		x		x	x	x	x	
		cargo quality checked	Yes/No	x		high	x		x		x	x	x	x		x		x		x	x	
		dangerous goods	Yes/No	x		high	x		x		x	x	x	x		x		x		x	x	
		container track history				high	x	x	x	x	x	x	x	x		x	x	x	x	x	x	

Table 26: List of information blocks of high importance only

K. Appendix: List of means (import and export)

The following table shows the list of means that are used by the SC actors to exchange information currently of in the future.

IMPORT

Means	Data element
pre-arrival information	container number
	container status
	container owner
	ISO code
	gassing
	gas-description
	TARRA
	seal number
	sealed
	sealed by
	seal status
	seal integrity
	seal type
	operator-ID
	operator details
	operator certified
	B/L number
	cargo value
	cargo weight
	cargo description
	cargo item
	cargo number of colli
	cargo code
	dangerous goods
	dangerous goods type
	country of origin
	country of departure
	consignor#
	consignee#
	certified
	certified
Interchange ECD	container status
Selection and control notifications by authority	container status
	container scanned
	container scan type
	container scan location
	container scan results
	scanning details
Physical check at discharge	container status
Crane reader	RFID tag (only for smart containers)
Physical check and/ or RFID check	container integrity
	temperature changes
	intrusion
	light changes
	seal type
Reader	location of sealing
	time of sealing
Nuclear scan	Nuclear scanned
	Nuclear detection results
	Nuclear detection location

EXPORT

Means	Data element
Pre-notification terminal visit (1) or pre-departure information (2)	container number
	container status
	container owner
	ISO code
	gassing
	gas-description
	TARRA
	seal number
	sealed
	sealed by
	seal status
	seal integrity
	seal type
	operator-ID
	operator details
	Operator certified
pre-departure information	container status
	B/L number
	cargo value
	cargo weight
	cargo description
	cargo item
	cargo number of colli
	cargo code
	dangerous goods
	dangerous goods type
	country of origin
	country of departure
	consignor#
	consignee#
	certified
	certified
Interchange ECD	container status
Selection and control notifications by authority	container status
	container scanned
	container scan type
	container scan location
	container scan results
	scanning details
Gate reader	RFID tag (only for smart containers)
Physical check and/ or RFID check	container integrity
	temperature changes
	intrusion
	light changes
	seal type
Reader	location of sealing
	time of sealing
Nuclear scan	Nuclear scanned
	Nuclear detection results
	Nuclear detection location

Fixed in database	Operator type of certificate
	Operator certificate details
	type of certificate
	certificate details
	type of certificate
	certificate details
Pre-notification terminal visit	operator#
	cargo-card-ID
	driver ID
	truck ID
	truck number plate
	driver ID
	personal details
	driver status
	operator
	train number
	train ID/number
	train owner
	operator
	barge name/ ID
	barge name/ ID
	expected time of arrival (ETA) at In-land terminal
	expected time of departure from Sea terminal
	port-key ID
	personal details
	organisation
inhouse system	brand
	owner
	barge owner
Check selection & results	cargo quality checked
No selection means no check	cargo quality checked
pre-arrival vessel information	operator
	ship name/ID
	ship name/ID
	ship owner
	expected time of arrival (ETA) Sea terminal
	expected time of arrival (ETA) container vessel
	consignor-ID
	consignor details
	consignee-ID
	consignee details
	port name
	port ID
	port city
	port country
	port security level
	port name
	port ID
	port city
	port country
	port security level
	port name
	port ID
	port city
	port country
	port security level
	terminal-ID
	terminal description
	terminal security level
	camera surveillance
	POD name
	city
	country
	POD security level
	camera surveillance
	POL name
	city
	country
	POL security level
	camera surveillance
gate-in	actual time of arrival (ATA) In-land terminal
gate out	actual time of departure in-land terminal
	actual time of departure from Sea terminal
Notification captain	actual time of arrival (ATA) Sea terminal
	actual time of arrival (ATA) container vessel
Internal business means	incident-ID
	incident type
	incident location
	incident description
	operator-ID
	management-ID(s)
	CMP
?	order number
	STUF/STRIP camera surveillance
	STUF/STRIP location
	cargo B/L
	STUF/STRIP sealing
	gate in time STUF/STRIP
	gate out time STUF/STRIP
	container#
	operator#
	expected time of stuffing/stripping
	actual time of stuffing/stripping
	expected time of departure STUF/STRIP
	actual time of departure STUF/STRIP
	expected time of departure at In-land terminal
NA	expected time of departure (ETD) container vessel
	actual time of departure (ETD) container vessel

Pre-notification of terminal visit	operator#
	cargo-card-ID
	driver ID
	truck ID
	truck number plate
	driver ID
	personal details
	driver status
	operator
	train number
	train ID/number
	train owner
	operator
	barge name/ ID
	barge name/ ID
	expected time of arrival (ETA) at In-land terminal
	expected time of arrival (ETA) Sea terminal
	port-key ID
	personal details
	organisation
inhouse system	brand
	owner
	barge owner
Check selection & results	cargo quality checked
Pre-departure vessel information	operator
	ship name/ID
	ship name/ID
	ship owner
	expected time of departure from Sea terminal
	expected time of departure (ETD) container vessel
	consignor-ID
	consignor details
	consignee-ID
	consignee details
	port name
	port ID
	port city
	port country
	port security level
	port name
	port ID
	port city
	port country
	port security level
	port name
	port ID
	port city
	port country
	port security level
	terminal-ID
	terminal description
	terminal security level
	camera surveillance
	POD name
	city
	country
	POD security level
	camera surveillance
	POL name
	city
	country
	POL security level
	camera surveillance
gate in	actual time of arrival (ATA) In-land terminal
	actual time of arrival (ATA) Sea terminal
gate out	actual time of departure in-land terminal
Notification captain	actual time of departure from Sea terminal
	actual time of departure (ETD) container vessel
Fixed in database	Operator type of certificate
	Operator certificate details
	type of certificate
	certificate details
	type of certificate
	certificate details
Internal business means	incident-ID
	incident type
	incident location
	incident description
	operator-ID
	management-ID(s)
	CMP
?	order number
	STUF/STRIP camera surveillance
	STUF/STRIP location
	cargo B/L
	STUF/STRIP sealing
	gate in time STUF/STRIP
	gate out time STUF/STRIP
	container#
	operator#
	expected time of stuffing/stripping
	actual time of stuffing/stripping
	expected time of departure STUF/STRIP
	actual time of departure STUF/STRIP
	expected time of departure at In-land terminal
NA	expected time of arrival (ETA) container vessel

Table 27: List of means (import and export)

L. References

Papers and books

Babbie, E (2004), *The Practice of Social Research (10th Edition)*, Chapman University

Barnes, P. & Oloruntoba, R. (2005), *Assurance of Security in Maritime Supply Chains: Conceptual Issues of vulnerability and Crisis Management.* The Fox School of Business and Management.

BS 7799-1:1999 Information security management - Part 1: *Code of practice for information security management* (1999), BSI/DISC Committee BDD/2.

Becker, J. & Verduijn, T. (2005b), *Supply chain security PROTECT WP4 eindraport 2005*, TNO.

Christopher, M. et al. (2002), *Supply chain vulnerability*, Cranfield School of Management.

Christopher, M. & Peck, H. (2004), *Building the resilient supply chain*, Cranfield School of Management, International Journal of Logistics Management.

Dhillon, G. (2007), *Principles of Information System Security (Text and Cases)*, Virginia Commonwealth University.

DNV Consulting (2006), *(file name: 14325 DNV binnen_p4.pdf).*

Dresser, E.L. (2004), *The effectiveness and economic impact of enhancing container security*, Massachusetts institute of technology.

Everett, M. Rogers (1995), *Diffusion of Innovations*, fourth edition.

Eyefortransport (2006), *Cargo and supply chain security trends.*

Goedhart, E.J. & Hulsebosch, B., (2001), Virtuele Haven, *Risk Analysis of Container Import Processes*.

Henry, H. Willis, David S. Ortiz, 2004, by the RAND Corporation, *Evaluating the Security of the Global Containerized Supply Chain.*

Joshi, V. Y. (2000), *Information Visibility And Its Effect On Supply Chain Dynamics*, Mater thesis, Massachusetts Institute of Technology.

March, J.G. & Shapira, Z. (1987), *Managerial Perspectives on Risk and Risk Taking*, Management Science, Vol.33, No.11.

Meijer, M. (2007), *PROTECT D5.2 – Information System Architecture for Supply Chain Security in Container Transport,* Master's thesis (preliminary version), Erasmus University Rotterdam.

OECD (Organisation for Economic Co-operation and Development), Maritime Transport Committee (2003), *Security in maritime transport: risk factors and economic impact*, Directorate for science, technology and industry.

Oosterhout, M. et al. (2000), Virtuele Haven, *T2.D1a, Inventory of Flows & Processes in the Port*, Erasmus University Rotterdam / ERBS B.V.

Oosterhout, M. & Moonen, H. (2006), *Adoption and implementation of IOS*, Erasmus University Rotterdam.

Peleg-Gillai, B. et al. (2006), *Innovators in Supply Chain Security*, Stanford University.

PROTECT (2005a), *Supply chain security PROTECT D 1.2 – Definitions*, RSM Erasmus University Rotterdam.

Rogers, E. M. (1995), *Diffusion of Innovation (4th Edition).*

Slay, J. and Koronios, A. (2006), *Information Technology Security & Risk Management.*

Vrijenhoek, N.H. (2005), *Supply Chain Security - What you can do for supply chain security, and what supply chain security can do for you*, Mater thesis, RSM Erasmus University Rotterdam.

Internet

PROTECT (2006)	http://protect.transumo.nl (Accessed on 2006-12-20)
UNODC	http://www.unodc.org/unodc/terrorism_definitions.html (Accessed on 2007-02-14)
Wikipedia (2006)	http://en.wikipedia.org/wiki/Security (Accessed on 2006-12-08)
Wikipedia (2007)	http://en.wikipedia.org/wiki/Supply_chain (Accessed on 2007-01-30)
Wikipedia (2007)	http://en.wikipedia.org/wiki/Exploratory_research (Accessed on 2007-02-06)
Wikipedia (2007)	http://en.wikipedia.org/wiki/Constructive_research (Accessed on 2007-02-06)
Wikipedia (2007)	http://en.wikipedia.org/wiki/Empirical_research (Accessed on 2007-02-06)
Eur-Lex (2007)	http://eur-lex.europa.eu (Accessed on 2007-03-18)

M. List of figures, tables and definitions

Figures

Tables

Definitions