ERASMUS UNIVERSITEIT ROTTERDAM

PROTECT

Transumo

Supply Chain Security in Container Transport

Recommendations towards an Improved Information System Architecture

PROTECT work package 5.2

Master's thesis Informatics & Economics

Date:	January 16, 2007
Author:	Mark Meijer (272972)
Contributions:	Dutch Tax and Customs Administration Erasmus University Rotterdam Port infolink Port of Rotterdam Authority TNO Built Environment and Geosciences
Supervisors:	dr. ir. J. van den Berg (Erasmus University Rotterdam) drs. S. Krupe (TNO)
Co-reader:	dr. F. Frasincar

Preface

This Master's thesis results from a seven-month internship at TNO Built Environment and Geosciences at the business unit Mobility and Logistics. During this period, I met many interesting people and I encountered several fascinating projects at this outstanding research institute. Besides enabling me to do my research, I enjoyed the pleasant work atmosphere and the involvement in some projects (although mainly at the surface) at TNO. The research presented in this thesis is part of a research project called PROTECT. In this project, many organizations cooperate doing research in the field of supply chain security.

The research was divided into two parts (work package 5.1 and 5.2) of which the second part relies highly on the first part. It was my assignment to focus on the research objective of work package 5.2. In the first period of my internship, however, I mainly cooperated in research of work package 5.1 (both in methodology and in execution). This included interviews and participation in brainstorm sessions to identify the user requirements for security relevant information. At the moment of writing this thesis, the research in 5.1 is not concluded. This thesis, therefore, leans on preliminary outcomes of work package 5.1 as well as on relevant literature on the subject.

I would not have been able to accomplish my research without the involvement of so many people around me. I thus want to express a word of gratitude for all those who supported the development of this thesis.

First, I want to thank my former coach Thierry Verduijn and final coach Sandra Krupe from TNO for their input on preliminary versions and research direction. Without their vision and involvement, this thesis would not have reached its level. I also want to thank the TNO project manager Egbert Guis for his participation in discussions and for his useful insights. Furthermore, I want to thank Cyril, Marjolein and Igor for the pleasant work atmosphere and their many encouragements during the process of writing this thesis.

Second, I want to thank the many people from the project that were involved in the two weekly brainstorm sessions at RSM Erasmus University Rotterdam. I want to thank Marcel van Oosterhout for his useful input on preliminary versions and his planning and execution of the brainstorm sessions. I also want to thank Iwan van der Wolf for his participation and useful insight in the area of port community systems and future directions of information systems used in container transport. I also want to address many thanks to Jurjen Duintjer and Bauke Padding for their contributions to the brainstorm sessions.

Special thanks go out to Nawid Popal for his cooperation that contributes to research outcomes presented in this thesis. Thank you for the pleasant teamwork, the preparation and execution of the interviews and the many hours of collaboration at RSM and TNO.

In addition, special thanks go out to Jan van den Berg, my coach from Erasmus University, who is now working at TU Delft. I could not have reached this quality without your input on research methodology and direction. I want to thank you for your participation in the brainstorm sessions and the comments on research findings presented in this thesis. Your enthusiasm has inspired me enormously and I hope on a continued cooperation, together with Marcel van Oosterhout and Nawid Popal, in publishing research findings from this project.

Furthermore, on a more personal level, I want to thank my fellow students for the enjoyable years that preceded this Master's thesis. I especially want to thank Moniek and Frank for the cooperation in the Master's phase and the many enjoyable meetings besides the academic obligations. I also want to thank Dennis, Edwin, Faried, Lonneke, Matthijs and Maurice for the pleasant academic atmosphere. I would very much enjoy if we can keep on meeting each other in academic and non-academic settings for many years to come.

Finally yet importantly, I want to thank my parents, Monique and Willem, for their support 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 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. Public 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 something in return like logistic advantages and lower lead-times.

In the supply chain for container transport already numerous information systems are used for the exchange of digital information between the organizations in the supply chain. Different categories that are distinguished are:

- Neutral or open community systems – these systems are used by the supply chain organizations to exchange security and non-security relevant information. An example of such a system is the port community system of Port infolink used in the port of Rotterdam;
- Authority systems – these systems are used by the regulatory authorities. Examples of these systems are the Customs systems and the seaport police systems;
- Container integrity systems – these systems are used to exchange information about the integrity of the container throughout the logistic process;
- Business (community) systems – these systems are used by the individual supply chain companies to exchange information about supply chain operations.

The focus of this research is on the digital information exchange between the supply chain organizations to improve supply chain security. The goal of this thesis is to provide recommendations for a future information system architecture to exchange this information. Because the future requirements of the supply chain organizations are uncertain, a scenario approach is used. In these scenarios, the amount of data elements exchanged differs with the degree of market and government driver.

In the scenario where the market and government driver is low, the least amount of data elements are exchanged. Of these data elements, many are already available within the port community system of Port infolink (in the near future). By linking the port community system, the authority systems and the container integrity systems, a high degree of coverage in width can be obtained.

In the scenarios where more information is exchanged because of a high government or market driver a larger part of the information resides within business (community) systems. This information is more difficult to open up then information already available within the neutral or open community systems or the authority systems. Additionally, when the market driver is high, security relevant information becomes more competitive sensitive and thus another information system architecture is more appropriate.

Index

1 Introduction

In this chapter, the research presented in this thesis is introduced. First, the context in which the research is conducted is outlined. In section 1.2, the research objective is formulated and the approach to reach this research objective is described. Second, the content of the thesis is addressed. This is done by defining the scope of the thesis and by giving a brief description of the contents of each chapter.

1.1 Context

This thesis focuses on supply chain security (SCS) in container transport. The logistic process of transporting containers is vulnerable and deserves attention in order to improve the security in the supply chain (SC). Because 95% of the world trade is conducted using container transport, a disruption of the system will 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 field of interest of SCS.

The research conducted and presented in this thesis is part of a project called PROTECT (http://protect.transumo.nl). PROTECT is a TRANSUMO project (a knowledge development program transitioning towards sustainable mobility [Vrijenhoek, 2005]). The aim of PROTECT is to determine critical success factors that have an influence on international SCS and to determine to what degree organizations in the SC can manipulate these factors to create and sustain a secure SC.

This thesis represents work package 5.2 of the PROTECT project. In this work package, 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 an information system architecture (ISA) that the different actors can use to exchange security relevant information to improve SCS.

Participants in the PROTECT project are the Erasmus University Rotterdam, TNO, Port of Rotterdam Authority, Buck Consultants International, Dutch Customs, EVO, NDL, TLN and DNV.

Different factors that have an influence on a future ISA for SCS can be distinguished. A graphical representation of these factors is presented in Figure 1.

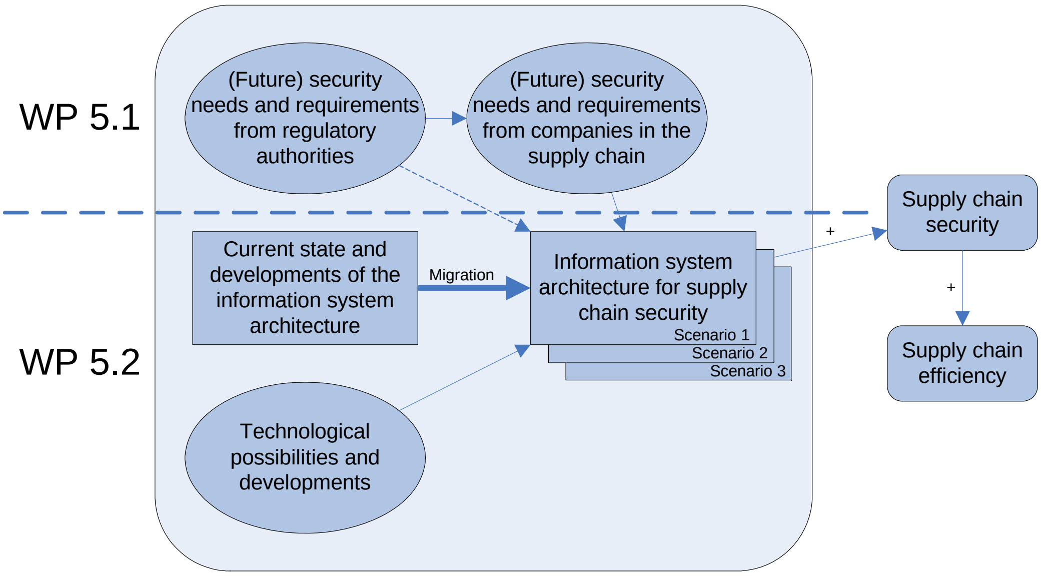

WP 5.1
WP 5.2
(Future) security needs and requirements from regulatory authorities
(Future) security needs and requirements from companies in the supply chain
Current state and developments of the information system architecture
Migration
Information system architecture for supply chain security
Scenario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

Figure 1: Factors influencing the ISA for SCS

In Figure 1, the factors are divided into two sections. The upper section of the figure presents the factors that are analyzed in the first part of the fifth work package of the PROTECT project (5.1). The lower section of the figure depicts the focus of the analysis performed within this thesis (5.2). The needs and requirements from the companies and the regulatory authorities are considered as given.

The reason for the development of an ISA for SCS comes forth from the basic assumption that by exchanging security relevant information SCS can be improved. Furthermore, the exchange of this type of information can ensure transparency and therefore provide collateral benefits to the SC companies investing in security [Rice & Spayd, 2005]. Companies in the SC will be more willing to gather and exchange security relevant information if it also delivers advantages to them. It is therefore important to look at win-win situations because this will increase the acceptance of the system.

1.2 Research objective

Information needs from both the organizations and the regulatory authorities create the need for an ISA transcending the organizational boundaries [Lee et al., 2000]. Because some security threats cannot be countered by individual organizations (e.g. terrorism), cooperation and information sharing in the SC is required. The focus of the ISA in the port of Rotterdam lay on exchanging messages between the different parties by fax or mail [Smit, 2004]. This changed in recent years to more and more digital information exchange. Adding security related information exchanges will alter the current ISA. In global supply chains, information systems are used by the actors involved in the logistic process to exchange information about the three flows in the SC – material, information and financial [Lee et al., 2000]. Adding information exchanges to enhance SCS will cause the current ISA to be extended (as simple as adding data fields to existing messages) or it will require a completely new ISA to be developed to support the new information exchange between multiple suppliers and receivers of data.

The research presented in this thesis has objectives that fit within the research question of the overall work package. The main question of the overall work package is described as follows: How can the security of the SC for container transport be improved with current and new information exchanges between the SC actors in order to enhance the reliability and efficiency of the logistic process?

This research question is not directly addressed in this thesis. However, this research question motivates the research objective of this thesis. Different elements of the research question deserve extra attention. First, in this research question, the assumption is made that current and new information exchanges can improve the security of the SC. It is important to note that there is information that has the potential to increase the security of the SC and that there is information that cannot be used to increase security. Second, with the SC actors 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 the different types of digital information exchanges.

Within work package 5.2 (addressed in this thesis), the general research objective is further specified into a research objective related to an ISA. The research objective of work package 5.2 is thus described as follows:

> *To provide recommendations to extend the current information system architecture in order to improve supply chain security.*

Definition 1: Research objective work package 5.2 (adapted from the original)

In work package 5.2, the main objective is to look at *digital information exchanges* between different organizations in the SC in order to improve SCS. The ISA used in this context means the overall information exchange model that is used in the SC. For specific information needs different information exchange models can be combined together in an overall ISA. Furthermore, scenarios are used to take into account the different possibilities for market and government driver for exchanging security relevant information. An ISA will have a more elaborate design if the market and government see great benefits in exchanging security relevant information, as apposed to the situation that both parties do not want to invest large amounts of money in SCS.

To reach the research objective of work package 5.2 different sub-questions arise:

(1) What are the (future) security information needs from the actors in the supply chain?

(2) What is the current state of the information system architecture for supply chain security?

(3) What relevant technological or architectural developments can be recognized with regard to supply chain security?

(4) What are possible recommendations to extend the current information system architecture with supply chain security relevant information in the scope of different future scenarios?

Definition 2: Research questions work package 5.2

These questions relate to different factors influencing the ISA for SCS as depicted in Figure 1. The first research question relates to the factors addressed in work package 5.1. The second research question pertains to the factor “Current state and developments of the ISA”. The third research question pertains to the factor “Technological possibilities and developments”. The fourth question relates to the migration from the current state of the ISA to a new state with an ISA for exchanging security relevant information in the SC. Because the extent of the future government and market driver are uncertain, different scenarios are developed. Within these scenarios, recommendations for an ISA for SCS are formulated.

1.3 Scope

The focus of analysis is on the transport of containers through the port of Rotterdam. As described earlier the needs for security relevant information from the organizations (companies and government) are considered as given for the analysis made in this thesis. The focus will be on how information can be shared between the different actors in the SC in order to fulfill these needs.

The information needs from the actors in the SC are considered as given in this thesis. They are the outcome of work package 5.1 and are depicted in Figure 2 [Popal, 2007]. From top to bottom, the scope is narrowed leading finally to information needs. Developing an ISA to facilitate the information exchange, following from the information needs, between the SC partners is the main target of the research presented in this thesis. The results from this thesis are thus valid within the scope defined in work package 5.1.

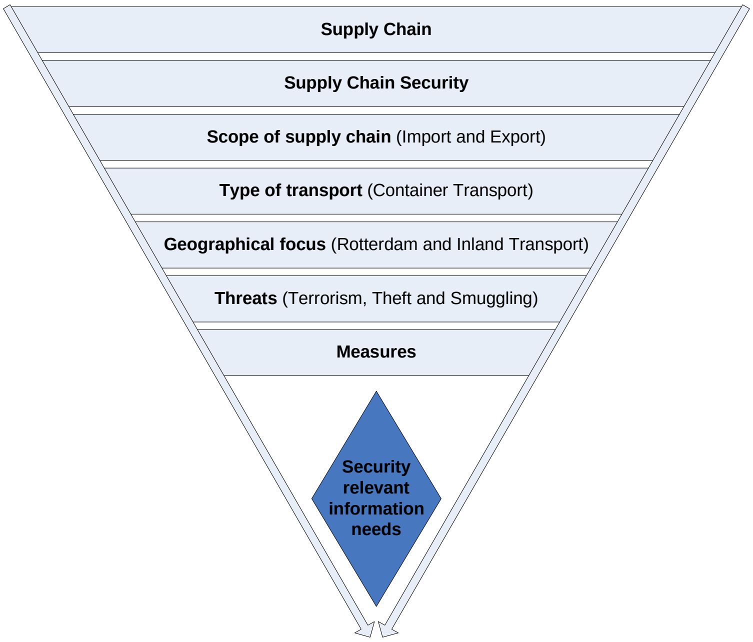

Supply Chain
Supply Chain Security
Scope of supply chain (Import and Export)
Type of transport (Container Transport)
Geographical focus (Rotterdam and Inland Transport)
Threats (Terrorism, Theft and Smuggling)
Measures
Security relevant information needs

Figure 2: Scope of work package 5.1

Additionally an ISA for SCS should fit with the current ISA used in the container transport. In this analysis low-level details about the ISA (e.g., which programming techniques should be used) are omitted. The analysis considers a high-level description of information coming from and going to different actors in the SC. The research also describes the methods that are used to exchange information between the different parties in the SC. The scope of this thesis is summarized in the following figure.

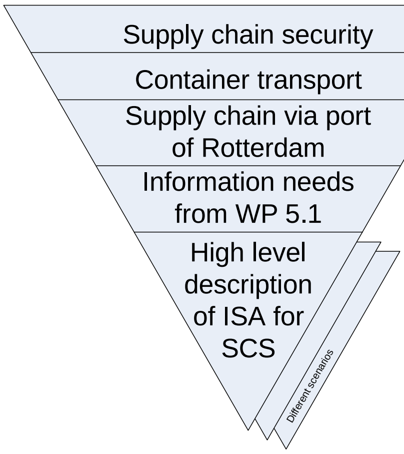

Supply chain security
Container transport
Supply chain via port of Rotterdam
Information needs from WP 5.1
High level description of ISA for SCS
Different scenarios

Figure 3: Scope of work package 5.2

The outcomes of this research are also limited within the scope of the factors that are considered to have influence on a future ISA for SCS. The factors, introduced in Figure 1, that have an influence on the future ISA for SCS are: (1) the needs for security relevant information from the regulatory authorities and the companies in the SC, (2) the current state of the ISA and (3) the technological possibilities and developments. Other factors are left out the scope of this analysis.

1.4 Methodology

In this research, the goal is to formulate recommendations for the development of an ISA to enhance SCS. To reach this goal different methods are used; a graphical representation of the methodology used can be found in Figure 4 (p. 14).

First, the processes in the import and export of containerized goods are defined and mapped. These maps are used as guidelines for the exploratory research [Wikipedia, 2007a] in work package 5.1.

Second, to identify the needs for security relevant information, interviews are conducted with SC actors. These interviews also serve as a validation for the process maps and they are used to identify processes where important risks occur.

After this, the concept of an ISA is researched. In this research, a conceptual framework is introduced based on a study on criteria to evaluate an ISA. This conceptual framework is used to develop the ISAs in different future scenarios.

The other factors, previously identified to have an influence on the future state of an ISA for SCS, are part of the exploratory research of work package 5.2. An ISA for SCS needs to be developed to be used in practice. Therefore, the scenarios are related to the way information exchange is currently organized. For this purpose, ISA experts have been interviewed on both security-focused and non-security-focused information systems. Furthermore, experts in the field of technological possibilities have been interviewed to incorporate their vision. Both the expert knowledge about the current state of the ISA and the expert knowledge about the technological possibilities serve as input for the development of scenarios for a future ISA.

To develop an ISA, a scenario approach is used which means that different possible future states are discussed. This is part of the constructive research [Wikipedia, 2007b] of work package 5.2. The scenarios differ in the degree to which government and market parties want to exchange security relevant information. If the needs from both the regulatory authorities and the market are high, another ISA is more appropriate than when both parties only have a low interest in gathering and exchanging security relevant information. For the development of the ISAs within the scenarios, brainstorm sessions have been conducted with experts in the field of SCS.

Finally, the ISAs proposed within the different scenarios have been validated in a workshop with domain experts and SC companies.

Since ISAs and SCS have been widely studied, a literature review is conducted before performing the research. About SCS, numerous articles have been published after terrorist attacks in America and Europe. On the subject of ISAs, various recommendations are available for developing an ISA in the form of enterprise architecture frameworks.

1.5 Reading guide

In this subsection an outline of the report is given. The contents of each chapter will be described and a graphical representation of the outline is given in Figure 4 (p. 14).

Chapter 2: Security in container transport
In this chapter, the concept of security in container transport is introduced. A description is given on what security in container transport actually is. In addition, the actors active in the SC are described, after which the physical processes in the SC are explained in more detail. Finally, in section 2.3, the results from research in work package 5.1 are outlined and the information needs from the different actors in the SC are identified.

Chapter 3: Information system architecture
The objective of this chapter is to give a description about what an ISA is. Different information exchange models are described and a framework is introduced which is used to develop different ISAs for exchanging security relevant information between the actors in the SC.

Chapter 4: Current state and development of the ISA for SCS
This chapter provides an overview of the current state and developments of ISAs in relation to SCS. The following types of ISAs are considered: (1) Neutral or open community systems, (2) Authority systems, (3) Container integrity systems and (4) Business (community) systems. This analysis serves as a foundation for the development of an ISA in the scope of the different scenarios described in chapter 6.

Chapter 5: Technological possibilities and developments
An analysis is conducted on the technological possibilities and developments to get the information from events in the SC to the different parties in order for them to be able to increase SCS. The results are presented in this chapter.

Chapter 6: Scenarios for an ISA for supply chain security
In chapter 6, three scenarios for future security information needs are introduced. Two factors that have influence on the security information needs are the degree of market and government driver. Within these scenarios different ISAs for SCS are appropriate. For each of the scenarios it is assessed which ISA is most suitable taking into account the conceptual framework introduced in section 3.6.

Chapter 7: Validation
To validate the findings of the research a workshop with experts as providers of information systems and domain experts have been conducted. Findings from this workshop are presented in this chapter.

Chapter 8: Conclusions and recommendations
In this final chapter, the conclusions of the research are presented and the possibilities for further research based on these findings are identified.

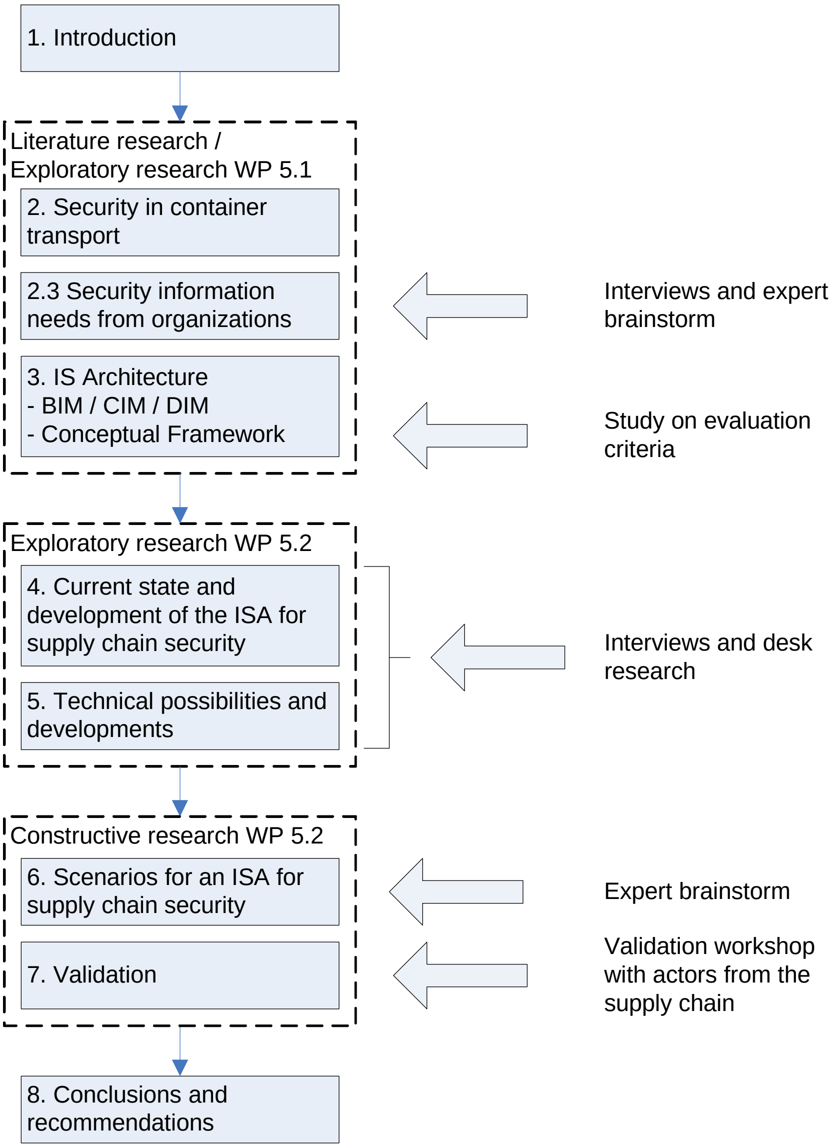

1. Introduction
Literature research /
Exploratory research WP 5.1
2. Security in container transport
2.3 Security information needs from organizations
3. IS Architecture
- BIM / CIM / DIM
- Conceptual Framework
Interviews and expert brainstorm
Study on evaluation criteria
Exploratory research WP 5.2
4. Current state and development of the ISA for supply chain security
5. Technical possibilities and developments
Interviews and desk research
Constructive research WP 5.2
6. Scenarios for an ISA for supply chain security
7. Validation
Expert brainstorm
Validation workshop with actors from the supply chain
8. Conclusions and recommendations

Figure 4: Research approach

2 Security in container transport

In this chapter, the concept of security in the SC of container transport is described in detail. In the SC, many organizations are involved in transporting containers as efficiently and as reliably as possible from the shipper to the consignee. Because of the increased awareness of threats to the SC, measures that improve the security receive much attention [Rice & Spayd, 2005].

The chapter is outlined as follows: In section 2.1, the physical processes conducted in the SC are explained. In addition, a definition is given of what a SC is and what is meant with security in relation to the SC. After the description of the processes in the SC, an overview of the actors involved in these processes is specified in section 2.2. These are the possible end-users of the ISA for SCS. Finally, in section 2.3 the user requirements for an ISA are described. These requirements are resulting from a study in work package 5.1 of the PROTECT project and are taken as input for the research presented in this thesis [Popal, 2007].

2.1 Supply chain for container transport

In this section, an overview is given about the processes in the SC. Before the processes are described, a definition is given of what a SC actually is. In subsection 2.1.1 and 2.1.2, the processes in the import and export chains are described in more detail.

A SC can be defined as follows:

> *A supply chain is a network of organizations that are involved, through upstream and downstream linkages, in different processes and activities that produce value in the form of products and services in the hands of ultimate consumers [Christopher, 1998; cited in Vrijenhoek, 2005].*

Definition 3: Supply chain

Some elements of this definition deserve extra attention. The ultimate customers of the SC for container transport are the sender and receiver (also called shipper and consignee) of the goods transferred in a container. Furthermore, the organizations that produce value in the form of products and services are all organizations involved in the physical process of transporting a container. The actors involved are described in more detail in section 2.2. In this definition, a chain is used to denote the linearity of the logistic process. Because of the complexity of the physical processes and information exchanges, the term supply network might be more accurate [Chapman et al., 2002; cited in Vrijenhoek, 2005].

From the point of view of the port of Rotterdam, two different processes can be distinguished. The first type of process is when a company wants to import goods from an offshore country. This process is depicted in the second part of Figure 5. The goods to be imported are gathered in an inland transport process in the offshore country and are transferred to a container ship in the offshore port. The goods are shipped to the port of Rotterdam and are then transferred via an inland transport process to the final destination.

The second type of process is exporting goods to an offshore country. The goods are gathered via an inland transport process and are transferred to the port of Rotterdam. The containers are loaded onto a container ship and are shipped to the offshore port. The offshore port unloads the goods and the goods are transferred to the final destination through an inland transport process. This export process is shown in the first part of Figure 5.

In this thesis, the focus is on the import process after – and the export process before the port of Rotterdam because to the Dutch economy these are of most interest. Therefore, the main concern is about risks involved on the Dutch side of the SC. The management of risks on the offshore part of the SC is left to the offshore port or country. In most cases however, risks that are relevant in the port of Rotterdam and the Netherlands are also relevant to offshore ports.

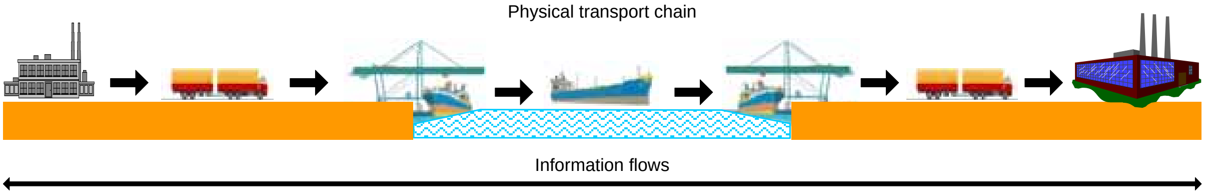


Figure 5: Carriage of goods [Oosterhout, 2003, p. 5]

2.1.1 Import

In this subsection, the physical transport process for importing containers is described. Figure 6 shows the different (sub) processes conducted when importing containerized goods. An enlarged version of the same figure is included as Figure 41 (Appendix B).

The standard physical flow for container transport is shown with the green rectangles (numbered) and alternative flows are shown in the red rectangles (unnumbered). Normal lines depict the standard transition between two processes, and the dotted lines depict alternative flows between the processes. The yellow rectangles depict processes that are not yet implemented; currently these are already planned to be implemented or they are discussed.

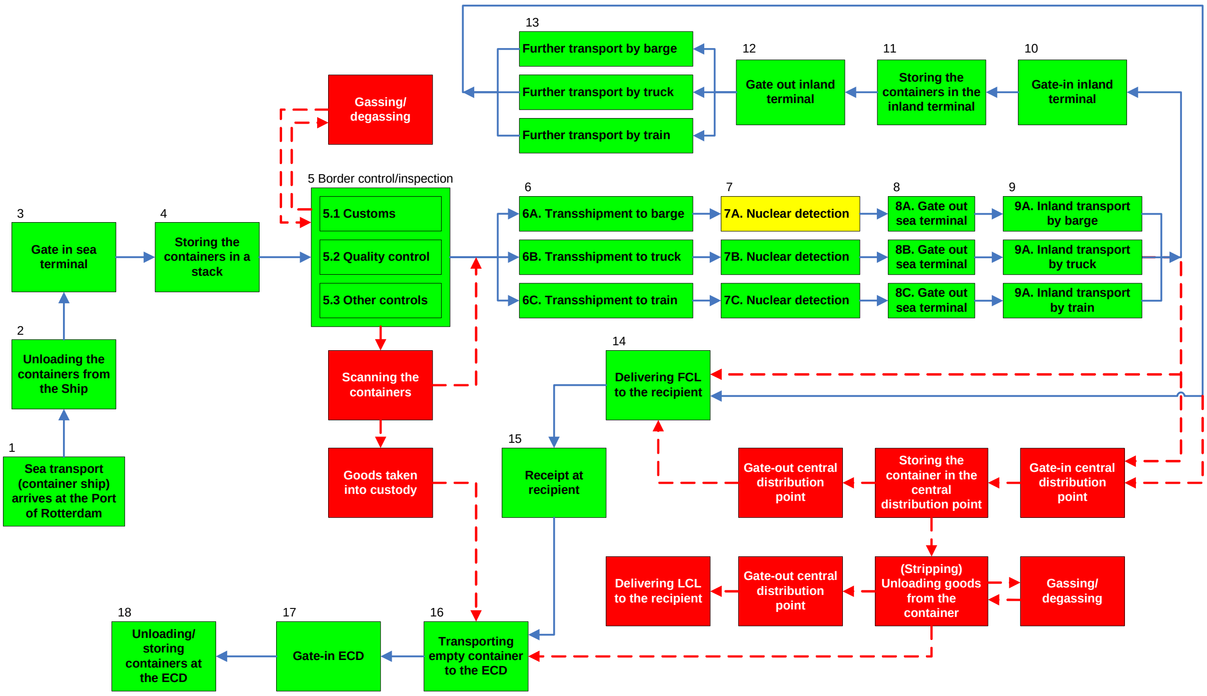

13
Further transport by barge
Further transport by truck
Further transport by train
12
Gate out inland terminal
11
Storing the containers in the inland terminal
10
Gate-in inland terminal
Gassing/ degassing
5 Border control/inspection
5.1 Customs
5.2 Quality control
5.3 Other controls
3
Gate in sea terminal
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
1
Sea transport (container ship) arrives at the Port of Rotterdam
Scanning the containers
Goods taken into custody
14
Delivering FCL to the recipient
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 6: Carriage of goods import [Popal, 2007]

The import process for containers starts with the arrival of the container ship at the Port of Rotterdam (1). In this port, the containership is unloaded and the containers are stored in a stack at the terminal. Before a container leaves the terminal to continue on the inland transport, it is checked by the regulatory authorities (e.g. Customs). When released, the container is transshipped to one of the three modalities for further inland transport. These three modalities are transport by barge via the inland waterways, transport by truck and transport by train.

When leaving the sea terminal by truck or train the containers are scanned for nuclear contents. For barge transshipments, this is not yet implemented. For inland transport, there are two possible destinations. The goods can be transferred directly to the recipient or they can be transferred to an inland terminal. At the inland terminal, the containers are stored before conducting further transshipment.

A second distinction is the delivery of less then full container loads (LCL) to different customers or transferring a full container load (FCL) directly to the customer. After sub process 9 or sub process 13 the container can be transferred to a central distribution point (for LCL) or to the customer (for FCL). The delivery of goods in a LCL is finalized by, for example, transport in trailer loads.

After the container is delivered to the final customer and the goods are unloaded or when the container is stripped at the central distribution point, the empty container is transferred to an empty container depot (ECD).

2.1.2 Export

In this subsection, the physical transport process for exporting containers is described. Also for the export process, a diagram is constructed. Figure 7 shows the different (sub) processes conducted when exporting containerized goods. An enlarged version of the same figure is included as Figure 42 (Appendix B).

The standard physical flow for container transport is shown with the green rectangles (numbered) and alternative flows are shown in the red rectangles (unnumbered). Normal lines depict the standard transition between two processes, and the dotted lines depict alternative flows between the processes. The yellow rectangles depict processes that are not yet implemented; currently these are already planned to be implemented or they are discussed.

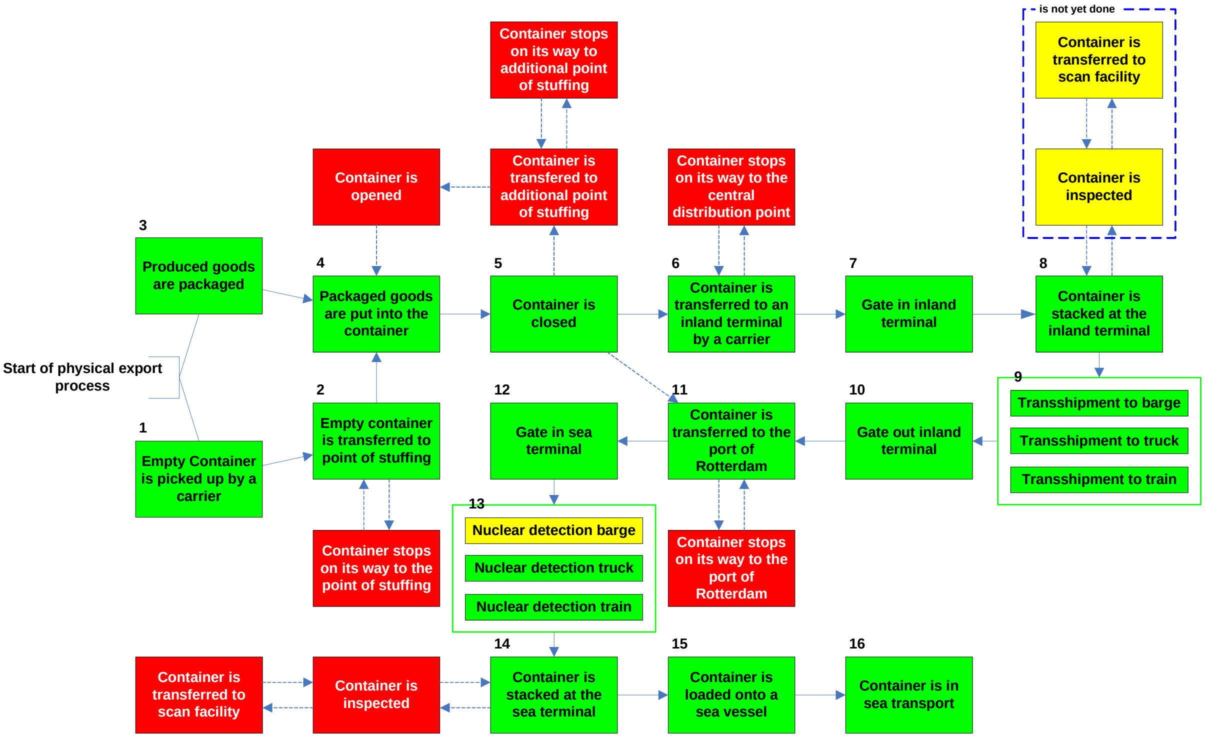

is not yet done
Container is transferred to scan facility
Container is inspected
Container stops on its way to additional point of stuffing
Container is opened
Container is transfered to additional point of stuffing
Container stops on its way to the central distribution point
3
Produced goods are packaged
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
13
Nuclear detection barge
Nuclear detection truck
Nuclear detection train
Container stops on its way to the point of stuffing
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 7: Carriage of goods export

The physical movement of the container starts at the ECD where the empty container is picked up (1) and transferred to the point of stuffing (POS) (2). The physical process of the goods that are transferred inside the container starts when they are packaged (3).

When the empty container arrives at the customer, the container is loaded and closed (4 and 5). After this, there are three possibilities. The container can be transferred directly to the port of Rotterdam, the container can be transferred to an inland terminal or the container can be transferred to an additional point of stuffing (for LCL).

When the container is transferred to an additional point of stuffing, the container is re-opened and extra goods are added to the container. After this process, there are again three possibilities for further transport as described above. It is important to note that containers are not always closed between the POS moments or even between the (final) POS and the port of Rotterdam. Ideally, the container is to be closed and sealed as soon as possible.

When the container is transferred to an inland terminal, the container is stored in a stack after which it is transshipped to one of the three modalities for further transport. When the container arrives at the sea terminal, the container is scanned for nuclear contents and is stored at the sea terminal.

At the sea terminal, the container can be inspected by the regulatory authorities. When released, the container is loaded onto a sea vessel and follows sea transport. After the ship reaches the offshore port, it enters the local import process.

2.1.3 Security in the supply chain

In this subsection, a definition is given of what security in relation to the SC actually is. In addition, a description is given about SCS found in the literature and a definition of SCS is discussed that was presented in previous parts of the PROTECT research.

The goal of this research is to make the SC more secure. What security is in this respect is very important. The meaning of security is described at Wikipedia as follows [Wikipedia, 2006]:

> *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.*

Definition 4: Security

In this thesis, the notion of safety is considered out of scope. Security in relation to container transport is the condition of being protected against terrorist attacks, smuggling and theft. In this respect, both internal and external threats are considered (this contrary to the definition above). With safety in container transport often, the safety of the container itself and the employees themselves is meant. In other words, the protection against damage of the container or machinery or the injury of employees is considered out of scope.

Now that a definition is given of security, it can be related to a SC. There are many different definitions of security in the context of a SC. At an earlier stage of the PROTECT project a secure SC was defined as follows [PROTECT, 2005]:

> *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.*

Definition 5: Secure supply chain

To assure a secure SC, security measures must be put in place. These measures have to ensure the security 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, 2005, p. 13].

2.2 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 five 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 report, 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 6: Terminology used in this report

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

Table 1: Supply chain actors adapted from Oosterhout et al. (2000)

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 (DCMR) Food and consumer product safety authority (VWA) Ministry of transport, public works and water management (Ministry of V&W) Plant health department (PD) Port authorities Seaport police

The shipper and the consignee are the final customers of the SC. The SC always starts with an exporter sending the goods packaged in a container or ends with an importer receiving the goods. 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 8, 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].

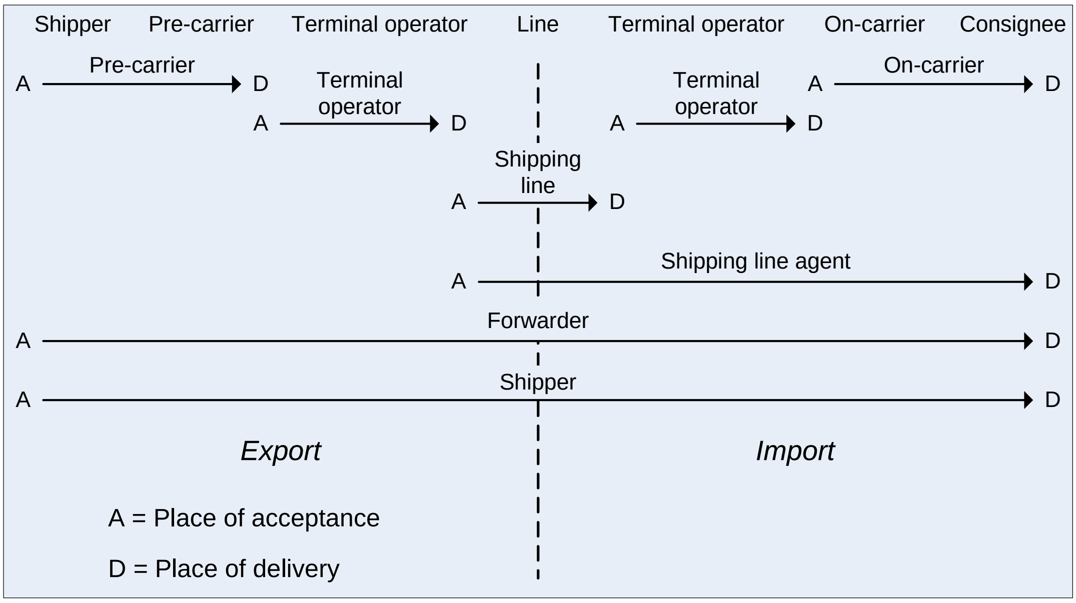


Figure 8: Scope of supply chain companies adapted from Oosterhout et al. (2000)

2.3 Information needs from organizations in the supply chain

In this section, a summary is given of the results from research performed in work package 5.1. In this analysis, interviews were conducted with SC actors to identify the information needs with regard to SCS. For every type of organization described in section 2.2, an interview was conducted where the information needs and the willingness to supply security relevant information were identified. A list of interviews can be found in appendix F.

The interviews were used to identify processes in the logistic process where the risks are the largest. Extra attention is given to reducing threats in these processes. This is done because improving the security at the weakest links of a chain increase the security of the overall SC. The following list contains processes that are identified by the interviewed SC actors as having a relatively high level of risk related to terrorist attacks, smuggling and theft [Popal, 2007].

- Point of container stuffing & stripping
- Point of sealing
- Points of feeding and consolidation
- Transshipment points
- Stops of inland transport
- Point of end-user arrival
- Handling of empty containers

The insights from the different interviews were aggregated and an expert brainstorm was used to identify common information needs. The information needs are grouped in the form of information blocks and the different data elements are scored to their relevance. The information blocks are depicted in the following list.

- Container (general) – this information block contains data elements about the container like the container number and the container status.

- 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 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. For more information, see section 4.3.3.
- 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.
- Cargo – in this information block, data elements relating to the cargo inside of the container are stored. This information includes, for example, the B/L[1] number, the cargo value, a cargo description and cargo weight.
- Ship details – this information block contains data elements about the ship that was used to transport certain containers.
- Process information on timing – the timing (time of arrival and time of departure) of the container in the different processes, as described in section 2.1, is contained within this information block.
- Personnel – in this information block, information about the personnel that handled the containers is stored. This information includes personal details and the organization for which the person is working.
- 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.
- 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.

2.3.1 Entity relationship diagram

In Figure 9, an entity relationship diagram [Elmarsi et al., 2000] of the information blocks is depicted showing the relationships between the information blocks. 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.

[1] Bill of Lading – Official legal document representing ownership of cargo, a negotiable document to receive cargo, and the contract for cargo between the shipper and the carrier. [RILA, 2007]

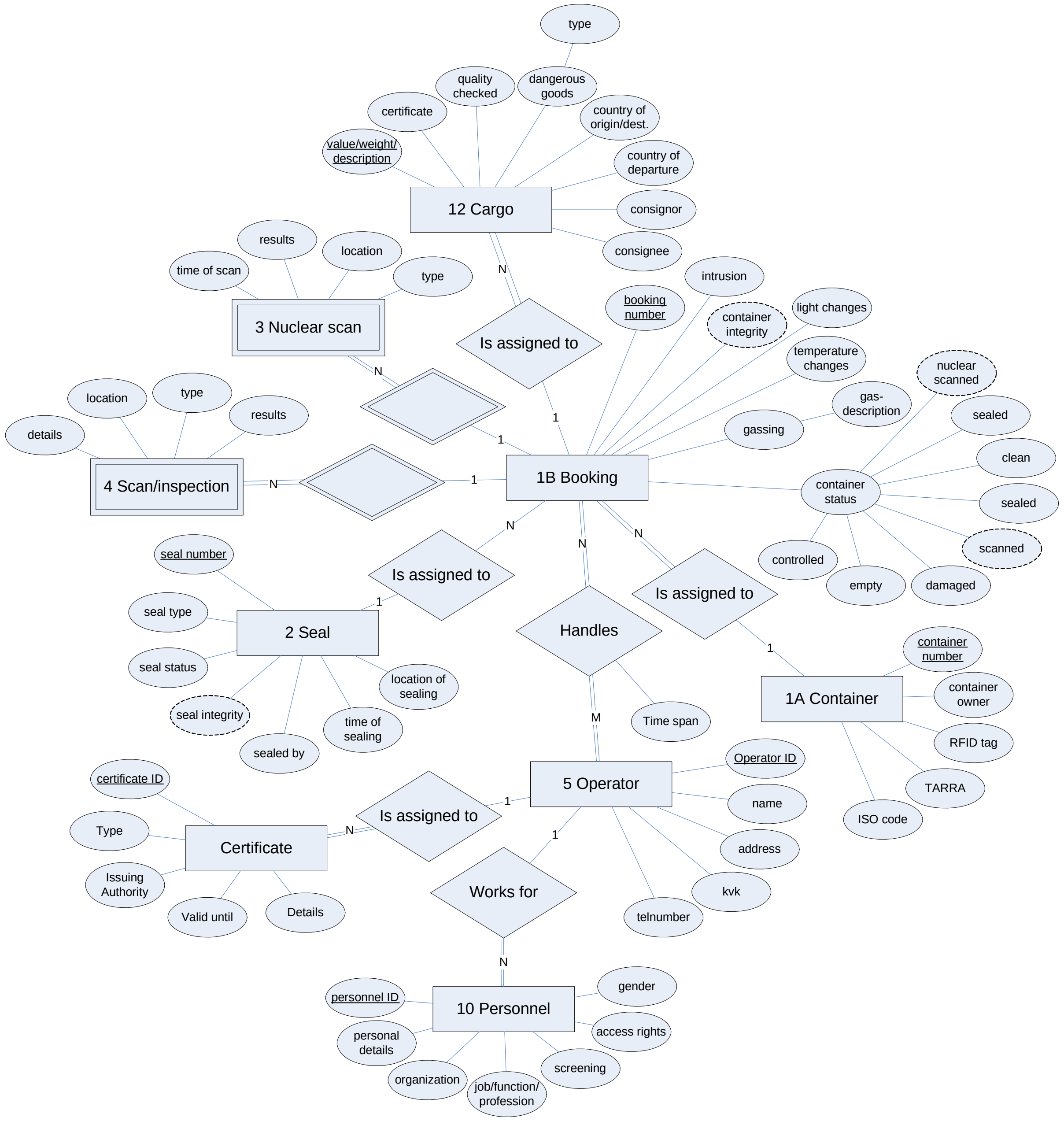


Figure 9: Entity relationship diagram for SCS relevant information

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.

For the operator information block, more detailed entity relationship diagrams are shown in Figure 10 and Figure 11. All the operators have the same data elements as the operator but have additional data elements specific to their function in the SC.

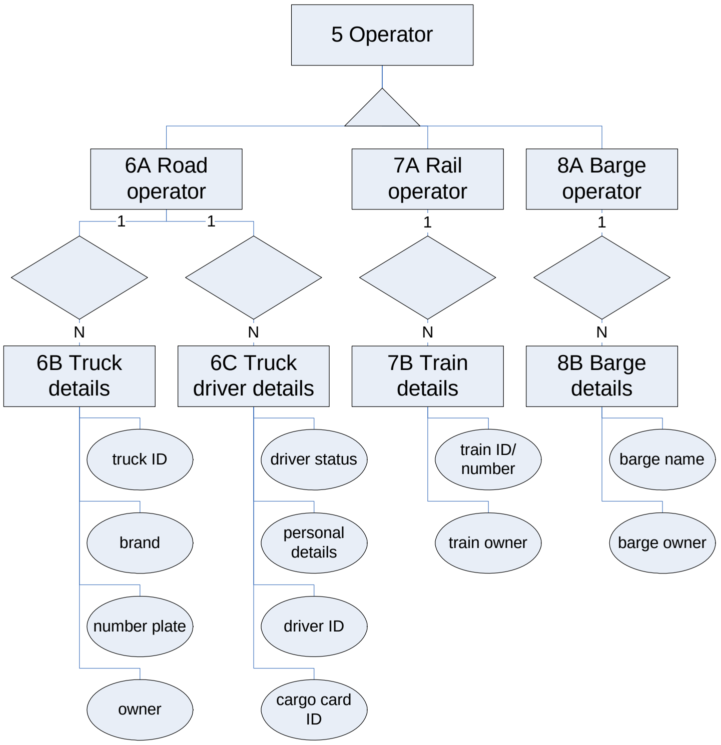


Figure 10: Entity relationship diagram for Pre- and on-carrier

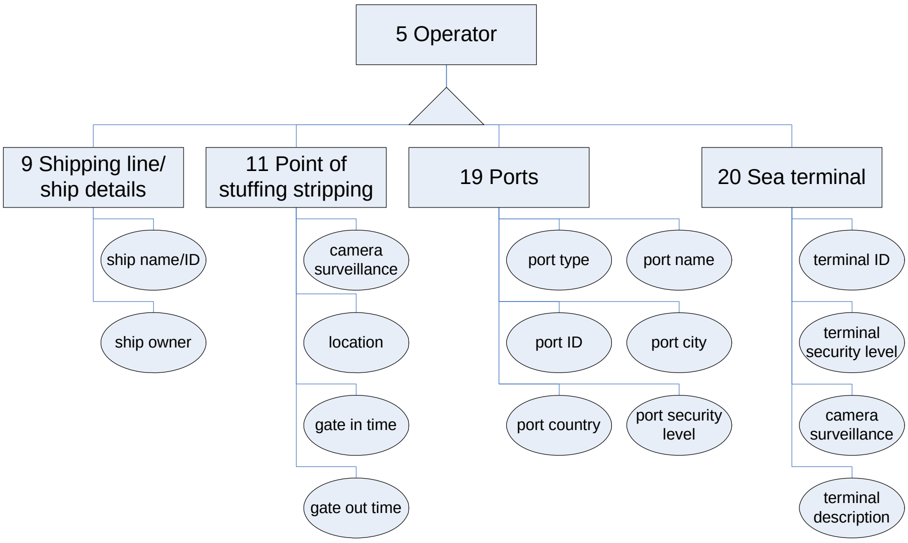


Figure 11: Entity relationship diagram for the remaining physical group

For a complete reference of all data elements and information blocks, see Popal (2007). The information blocks described above and the associated data elements represent the maximum of the information needs that the actors in the SC combined might have in the (near) future. For each data element, the importance is assessed with regard to the needs from the actors in the SC. Data elements that have a high importance represent the information needs that are present, even if the market and government driver are low.

2.3.2 Important data elements

In the interviews and brainstorm sessions, the importance of the complete set of data elements has been assessed. The data elements that are considered important are depicted in the following table.

Table 2: Data elements with high importance adapted from Popal (2007)

#	Category	Data element	Options / values
1	Container (general)	container number	
		container status	sealed (yes / no)
			nuclear scanned (yes / no)
		scanned	yes / no
		TARRA	
		container integrity	ok / not ok
2	Seal	seal number	
		location of sealing	
		time of sealing	
		sealed by	consignor / operator / authority
		seal status / integrity	ok / broken / damaged
3	Nuclear scan	location of scan	sea terminal, inland terminal etc.
		results of scan	ok / not ok
4	Scan / inspection (container contents)	container scan / inspection results	ok, not analyzed / ok, analyzed, not ok
5	Operators (general)	operator ID	
		operator certificate details	date / time of issue
			issuing authority
			valid until
12	Cargo	B/L number	
		cargo value	
		cargo weight	
		cargo description	
		cargo quality checked	yes / no
		dangerous goods	yes / no
		container track history	

In this table, different categories with the associated important data elements are depicted. Not all categories are represented and within the categories, not all data elements are considered important. The data elements depicted here are the result from interviews with different SC actors. The only data element that was not identified in the interviews is the information if an operator is certified or not and what the details of this certificate are. Certification in this sense means that an authority is confident the operator has taken sufficient security measures in order to do their part of the SCS. The knowledge that a container was only handled by certified operators increases the confidence that the transport of the container was secure and that the container cannot be used in a terrorist attack, that the container is not used for smuggling of goods and that the contents of the container is not stolen.

2.3.3 Means for exchanging the data elements

The data elements are coupled to the means for exchanging them. This means that messages that are currently exchanged between the actors in the SC contain most of the data elements that came from the information analysis. For some data elements no message exists which implies that the information is currently not (openly) exchanged between the actors in the SC. The different means are summarized in the following table.

Table 3: Means data exchange adapted from Popal (2007)

IMPORT

Means
Check selection & results
Crane reader
Fixed in database
Gate-in
Gate-out
Inhouse system
Interchange ECD
Internal business means
Notification captain
Nuclear scan
Physical check and/or RFID check
Physical check at discharge
Pre-arrival information
Pre-arrival vessel information
Pre-notification terminal visit
Reader
Selection and control notifications

EXPORT

Means
Check selection & results
Fixed in database
Gate reader
Gate-in
Gate-out
Inhouse system
Interchange ECD
Internal business means
Notification captain
Nuclear scan
Physical check and/or RFID check
Pre-departure information
Pre-departure vessel information
Pre-notification terminal visit
Reader
Selection and control notifications

The left side of Table 3 shows the messages that are exchanged for the import process. On the right side, the messages for the export process are shown. These messages are exchanged between the different organizations in the SC. The flow of messages is summarized in the following tables.

Table 4: Message exchange between actors in the SC (import) adapted from Popal (2007)

IMPORT

	To	1	2	5	6	7	8	9	10	12	13
From		shipper	forwarder	road operator	rail operator	barge operator	in-land terminal	sea terminal	shipping line agent	port authorities	customs
4	empty container depot			Interchange	Interchange	Interchange					
5	road operator						Pre-notification terminal visit	Pre-notification terminal visit			
6	rail operator						Pre-notification terminal visit	Pre-notification terminal visit			
7	barge operator						Pre-notification terminal visit	Pre-notification terminal visit			
8	in-land terminal			Gate-in	Gate-in	Gate-in					
9	sea terminal			Gate-out	Gate-out	Gate-out			Physical check at discharge Crane reader Gate-in Gate-out		
10	shipping line agent									Pre-arrival vessel information Notification captain (ATA)	Pre-arrival vessel information Pre-arrival information Notification captain (ATA)
13	customs							Selection & Control notifications	Selection & Control notifications		Nuclear scan
18	Food and consumer product safety Auth.	Check selection & results	Check selection & results						Check selection & results		

Table 5: Message exchange between actors in the SC (export) adapted from Popal (2007)

EXPORT											
	To	1	2	5	6	7	8	9	10	12	13
From		shipper	forwarder	road operator	rail operator	barge operator	in-land terminal	sea terminal	shipping line agent	port authorities	customs
4	empty container depot			Interchange	Interchange	Interchange					
5	road operator						Pre-notification terminal visit	Pre-notification terminal visit			
6	rail operator						Pre-notification terminal visit	Pre-notification terminal visit			
7	barge operator						Pre-notification terminal visit	Pre-notification terminal visit			
8	in-land terminal			Gate-out	Gate-out	Gate-out					
9	sea terminal			Gate-in	Gate-in	Gate-in			Physical check at loading Crane reader Gate-in Gate-out		
10	shipping line agent									Pre-departure vessel information Notification captain (ATD)	Pre-departure vessel information Pre-departure information Notification captain (ATD)
13	customs							Selection & Control notifications	Selection & Control notifications		Nuclear scan
18	Food and consumer product safety Auth.	Check selection & results	Check selection & results						Check selection & results		

Organizations that are not sending or receiving any messages are left out of these import and export message exchange tables. In the import table, for example, the shipping line agent (10) sends a “Pre-arrival vessel information” message to the port authorities (12) and Customs (13).

2.4 Conclusion

In this chapter, the SC for container transport and the most important results from the analysis of work package 5.1 were introduced.

First, the processes in the import and export of containerized goods were described. These individual processes are important because they are the basis for a threat analysis performed to identify key data elements that can be exchanged between the actors in the SC to improve SCS.

Second, the actors active in the SC were described in more detail. This was done to create a consistent definition of the actors in the SC throughout the analysis. The actors were 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.

Third, the results from the analysis of work package 5.1 were described. From interviews and expert brainstorms, different categories for security relevant information were defined. Within these categories numerous data elements were defined that could be exchanged to increase the SCS. Examples of the categories were general container information, nuclear scan information but also information about the operators that physically handled the container. For the categories, an entity relationship diagram was made to denote the interrelationship between the different categories. In the analysis, also the importance of the different data elements was assessed. Data elements that have a high importance received precedence over data elements with a low importance. After this, the means for exchanging these data elements were described, as they currently exist in the digital information exchange. The results from this analysis form the basis for the ISAs for SCS (within the scope of different future scenarios) described in chapter 6.

3 Information system architecture

In this chapter, a description is given on what an ISA is. First, a description of ISAs in general is given after which an ISA is related to the SC for container transport. This chapter forms the basis for analysis in chapter 4 in which the current state of the ISA for SCS in the container transport is described in detail.

In section 3.1, possible ISAs are described from a theoretical point of view. In this section, different models for information sharing are described as well as possible architectures for implementing these information exchange models. After the concept of an ISA is defined, in section 3.5, the factors that have an influence on an ISA for SCS (introduced in section 1.1) are described. These factors form the basis for the framework in section 3.6. In this section, a description is given of a framework that can be used to develop an ISA for particular information needs.

3.1 *Different types of information system architectures*

Because of the growing complexity of software intensive systems, ISAs become more and more important. Before the different types of ISAs are described, it is important to define what is meant by an architecture. The following definition is taken from IEEE Standard 1471-2000 [IEEE 1471-2000, 2000]:

> *An architecture is the fundamental organization of a system embodied in its components, their relationships to each other, and to the environment, and the principles guiding its design and evolution.*

Definition 7: Architecture

Recommendations for the ISAs for SCS that are proposed in this thesis focuses on the architecture of the information systems in relation to the information exchanges between the different actors of the SC. An enterprise architecture is defined as follows: “*Enterprise architecture is about understanding all of the different elements that go make up the enterprise and how those elements inter-relate*” [IFEAD, 2007]. An ISA for SCS is broader than an enterprise architecture in the sense that it looks at information exchanges across organizations instead of looking at one organization.

In the remainder of this section, different categories of ISAs are discussed. The different categories are the monolithic architecture, client/server architecture and peer-to-peer (P2P) architecture.

3.1.1 Monolithic architecture

The architecture used in many mainframe systems and still used on many home PCs is the monolithic architecture. In this architecture, processing, data and the user interface reside on the same system. In SC communication, this architecture is rarely used because of the automated collaboration of the different SC actors (often using some kind of network).

3.1.2 Client/server architecture

Instead, an architecture related to network technology is called a client/server architecture. In this architecture, a server waits for a request from a client to do some procedure and gives results back to the client. A common example of a client/server architecture is a web server delivering a website (in plain text) to a client. This client takes care of the user interface of the website by displaying it in a web browser. Within the client/server architecture, also different types of architectures can be distinguished relating to the number of tiers in the architecture.

A classic client/server architecture (also called two-tier architecture) has only two nodes. One node acts as a server waiting for a request to send some data. The other node acts as a client sending the requests to the server. The business logic is ideally contained within the server to increase uniformity although it can also be contained within the client. The user interface is commonly generated within the client.

An extension to this model is called a three-tier architecture. In this architecture, the presentation tier runs on a client that the user can use to propagate his request to the logic tier. This logic tier can be run on an application server that contains the business logic of the application. The logic tier, on its turn, uses the data tier for data storage and retrieval.

A further extension to the three-tier architecture is called an *n*-tier architecture. In this architecture, business logic from different sources can be used to represent multiplicity in the logic layer or data from different sources can be used to represent multiplicity in the data tier.

A well-known architecture that is comparable to an *n*-tier architecture is the service-oriented architecture. In this architecture, functionalities of applications are offered openly for other applications to be used. This means that different services from different systems (or organizations) can be used to reach a certain goal.

3.1.3 Peer-to-peer architecture

Furthermore, there is an architecture called a peer-to-peer (P2P) architecture. In this architecture, all nodes can act as both client and server and both possess equal functionality. A well-known use of a P2P architecture is Internet telephony and file sharing applications.

In the SC for container transport, a large number of organizations collaborate and share information. Because all parties deliver different services and supply different data to each other in most cases client/server architectures are used.

3.2 Models for information sharing

Besides ISAs, also models for information sharing can be used to describe the high-level architecture of the information exchange between the different actors in the SC. Three models for exchanging information (also called e-collaboration models) can be distinguished [Boertien et al., 2002]:

- Bilateral Information Model (BIM) – In this model, information is exchanged directly between two parties. The sender pushes data to the receiver. This receiver can do with the information whatever he wants to do with it. The receiver can store the information for further reverence or can delete the information after viewing it;
- Centralized Information Model (CIM) – In this model, information is pushed from the sender to a central information system where the data is made available to receivers that have access to the information. The data is only sent to the receiver if he asks for it. The receiver can do whatever he wants to do with the information. He does not have to store the information (but he can do so) because the information is stored centrally at the information broker. In principal, there are two copies of the data: one in the internal system of the sender and one in the central database;
- Decentralized Information Model (DIM) – This model is a further extension of the previous models. In this model, information is exchanged directly between two parties, but not on a push basis. The SC organizations make available the information to other (authorized) organizations. When the receiver wants to view certain information it retrieves this information from the sender and can do with the information whatever he wants to. In principal the information is only stored once at the source and is made available to the organizations that are authorized to access this information.

These information models can be used in parallel in an information system and organizations can communicate with each other using different models for exchanging information.

3.3 Relevance of information sharing models

Different kinds of information needs can be distinguished (section 2.3). First, there are the needs that originate from one organization and require only one (or a few) organizations to supply data. Second, there are the needs that originate from one organization and require numerous organizations to supply information. Third, there are information needs that originate from many companies and require only a few companies to supply data and finally there are information needs that originate from many companies and require information to be supplied by numerous organizations. The different combinations of information needs are shown in Figure 12. As depicted in the figure, the complexity increases with the number of senders and receivers.

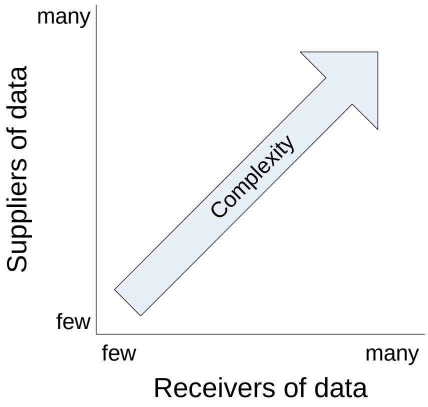


Figure 12: Different kinds of information needs

The models for information sharing discussed in section 3.2 are more suitable for some combinations of number of suppliers and number of receivers than they are with other combinations. In the following section first the BIM and the CIM are compared. After this subsection, the DIM is described and finally mixed models for information exchange are discussed.

BIM compared with the CIM

If there are only a few suppliers of data and only a few receivers of this data, then the BIM is the model of choice. Using a centralized solution requires a central organization (also called information broker) to be created which only would have to serve the few parties involved in the information exchange.

On the other hand, if there are many senders and receivers of data a centralized solution is preferred over the BIM. The following figure illustrates this.

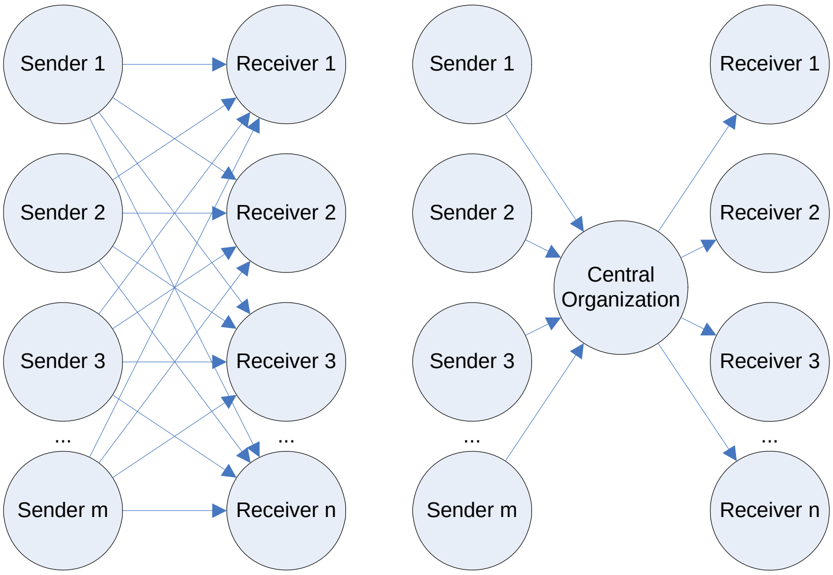


Figure 13: BIM and CIM for many senders and many receivers

On the left section of Figure 13, the BIM is illustrated. When using this type of collaboration the number of communication lines is *m* (the number of senders) times *n* (the number of receivers). The senders and receivers can have defined a common message format, but the format can also be different. This can become very complex if the number of senders and/or receivers is large. The complexity of this type of information exchange model is defined as $O(m \cdot n)$. The right section of Figure 13 illustrates the CIM. In this model, a central organization takes the responsibility of aggregating and converting the information. In this way, the senders only have to send the information once to the central organization and the receivers all have a uniform way of accessing or receiving the information. The number of communication lines is now *m* plus *n*, so the complexity is $O(m+n)$. Since $O(m+n) < O(m \cdot n)$ for $n, m > 2$, a reduction of complexity can be obtained.

In the case of only a few senders and many receivers or in the case of many senders and only a few receivers of information a similar reasoning can be done. The following figures illustrate the BIM and the CIM in these situations.

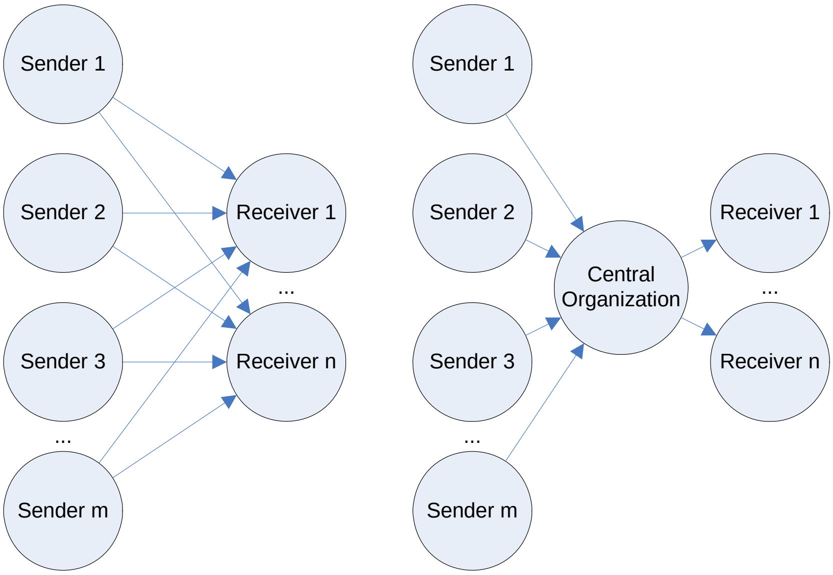


Figure 14: BIM and CIM for many senders and few receivers

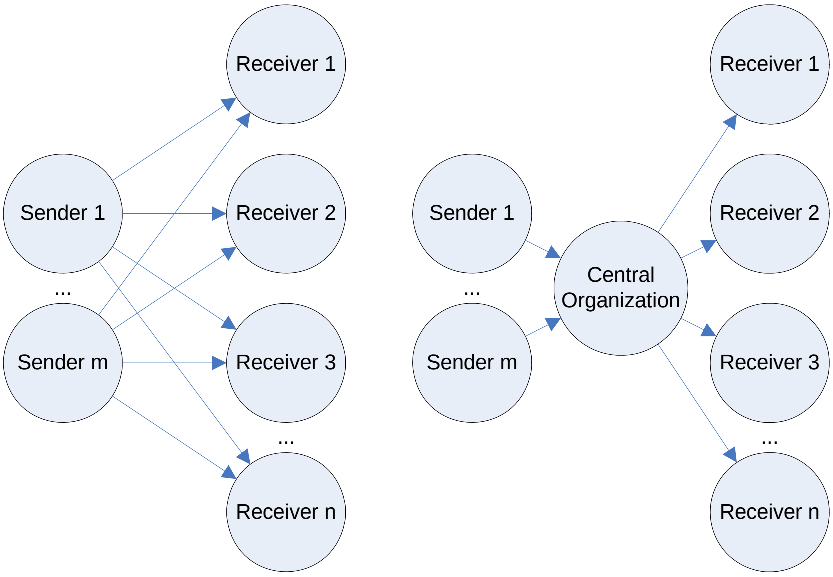


Figure 15: BIM and CIM for few senders and many receivers

For *m* and *n* larger than 2, the complexity is reduced from $O(m \cdot n)$ to $O(m+n)$, but the drive to create the central organization may also depend on other factors.

First, the drive to create a central organization is influenced by the market or government power of the sending or receiving party. If the sending or receiving part of the communication has market power, it can demand or be uncooperative in the creation of a central organization. In this reasoning, it is assumed that the creation of a central organization requires the cooperation of both senders and receivers.

Second, a central organization is primarily created to address the following functions: (1) information conversion, (2) information aggregation and (3) information relay. When no central organization is used (left sections of Figure 13, Figure 14 and Figure 15) the conversion can be performed by the sender or by the receiver, the aggregation is always done by the receiver and the relay (where to send the message to) is always performed by the sender. If the market power lies at the sending end of the communication lines, the sender can leave the conversion to the receivers, which means the sender does not have to invest much effort in the communication. This causes the drive for a central organization to be less than when the market or government power lies at the receiving end of the communication lines.

DIM

In all the three cases, as illustrated above in Figure 13, Figure 14 and Figure 15, a DIM may also be a solution. In a DIM, no central organization is created for the conversion and aggregation of information. Instead, clear arrangements are made between the different actors in the SC about the format and meta-information in order to prevent the need for conversion and to simplify the process of information aggregation. Often a central organization (called a registry) is created to take care of the message relay[2]. A DIM only reduces complexity if clear arrangements are made between all actors in the SC. Making such arrangements for exchanging security relevant information globally or even nationally can be difficult and time consuming.

Advantages of the DIM are that the information is only stored at one location and that information is transmitted when it is needed which ensures the actuality of the information. In a distributed setting also, the dependency on a central organization is removed. In a possible future where security measures are frequently extended and new information exchanges between different actors in the SC are added on a regular basis, the swiftness of decision-making is very important. Organizations can choose to make information available and this information can directly be accessed by authorized actors in the SC.

An example of a DIM that has received much attention the last few years is the service-oriented architecture. In this architecture, application services are offered for other applications to use. This means some kind of function is offered openly to other (authorized) users. An example of such a service is a data retrieval service that enables the user to retrieve some pre-defined set of data elements. Instead of one organization sending information to other organizations, the other organizations can retrieve the information by using the data retrieval service.

Currently, in the SC for container transport the DIM is rarely used [Boertien et al., 2002]. It is therefore not likely that this model is used if no extensive market driver exists. When this market driver does exist, transition towards the DIM will be gradual and time consuming.

3.4 Degree of coverage of an ISA

An important concept that is used in the analysis of the current state and developments of the current ISA and the recommendations for the improved ISA, is the degree of coverage (that can be obtained). Two different types of coverage can be distinguished: coverage in width and coverage in depth. With coverage in width, the amount of possible data elements that can be exchanged is meant. An ISA with a high degree of coverage in width can be used to exchange a relatively large subset of the total amount of data elements that need to be exchanged to ensure SCS. With coverage in depth, the number of participating organizations is meant. In an ISA where the degree of coverage in depth is high, relatively a large subset of the organizations participates in the ISA.

[2] The message is not actually relayed by the registry. Instead, the registry tells the sender where to find the receiver of the information.

3.5 Factors influencing the information system architecture for SCS

In this section, the factors that have an influence on an ISA for SCS are described in detail. These factors were introduced in section 1.1 and are (once more) depicted in Figure 16. For enterprise architectures (ISAs within one enterprise), numerous frameworks have been developed aiding in the development of such a system. Examples of enterprise frameworks are the Zachman-framework [Zachman, 1987] and the Capgemini Integrate Architecture Framework (IAF) [Mulholland et al., 2006]. In these frameworks, viewpoints are used to describe the enterprise architecture from different perspectives. In the IAF, the following viewpoints are described: (1) Business, (2) Information, (3) Information systems and (4) Technology infrastructure. This framework is adapted to suit the complexity of the SC without going into details about the exact implementation of the system.

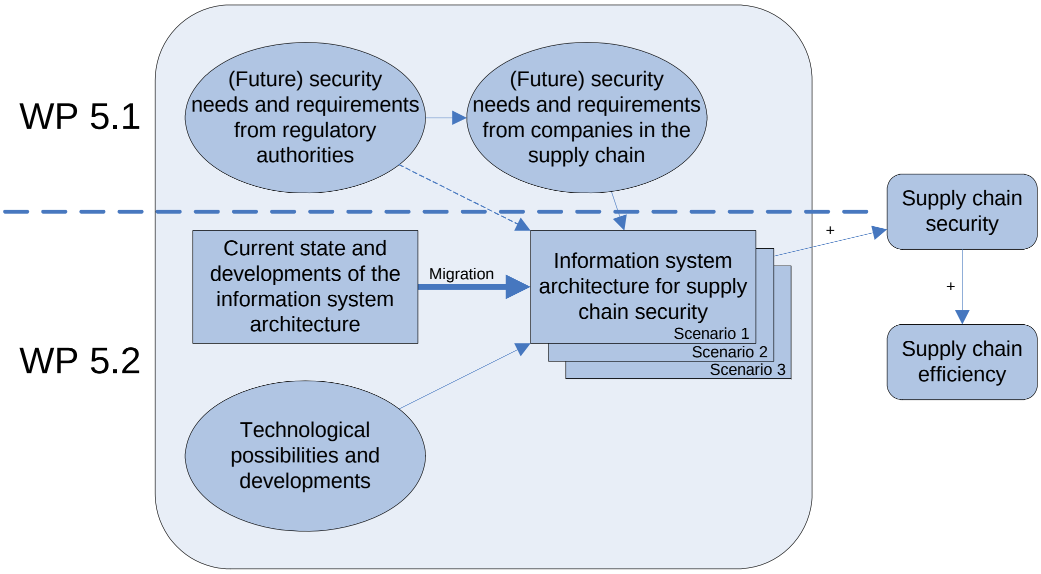

WP 5.1
WP 5.2
(Future) security needs and requirements from regulatory authorities
(Future) security needs and requirements from companies in the supply chain
Current state and developments of the information system architecture
Migration
Information system architecture for supply chain security
Scenario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

Figure 16: Factors influencing an ISA for SCS

3.5.1 Business and information

The business aspect area is described by Capgemini as follows [Mulholland et al., 2006]: *The Business Aspect Area adds knowledge about business objectives, activities, and organizational structure.* In this respect, the analysis about the physical SC (section 2.1) and the interviews conducted for work package 5.1 deliver valuable insight for this aspect area.

The information aspect area is described by Capgemini as follows [Mulholland et al., 2006]: *The Information Aspect Area adds knowledge about the information the business uses, the information structure and relationships.* For this aspect area, the analysis in work package 5.1 and described in section 2.3 about the information needs from the actors in the SC is an important input. The actual information that is exchanged in an ISA depends on the needs from the individual companies in the SC and from the regulatory authorities.

Each company has information needs regarding SCS (their part in the SCS) and may need different types of information from different parties in the SC.

Some security needs do not stem from companies within the SC but are social requirement. Threats of smuggling of materials that can be used in a terrorist attack do not have a high impact on the individual companies in the SC but can have a significant impact on the inhabitants of the country(s) the regulatory authorities are representing. These social requirements translate to requirements within the SC. Shipping line agents may demand that the container does not contain materials that can be used in a terrorist attack. This forces the terminal, for example, to take measures to prevent this, but they do not originate from companies within the SC. Needs from regulatory authorities also have a direct influence on the ISA because they require organizations within the SC to supply different kinds of information. This information includes, for example, container contents information for making a risk analysis.

3.5.2 (Current) information systems

The information systems aspect area is described by Capgemini as follows [Mulholland et al., 2006]: *The Information System Aspect Area adds knowledge about types of information systems (packaged or bespoke) that can automate and support the processing of the information used by the business.* Relating this to SCS identifies the need for an approach that besides the possible types of information systems also takes into account the current information systems used by the SC actors.

Besides the user requirements, there are thus the current state and developments of the ISA that have an influence on the information systems of the future ISA for SCS. In the current SC, different information systems are used for exchanging information regarding the physical flow of and the financial flow for container transport. The architecture of these current information systems has an influence on the ISA for SCS because organizations in the SC invested heavily in these information systems. Proposing an ISA for SCS in line with current systems is more viable in practice. To be able to implement the security architecture in practice it is required that the system is acceptable, as described in the technology acceptance model (TAM) [Davis et al., 1989]. An ISA is more acceptable if the architecture does not has to change completely (this means high costs for changing the ISA) or if the architecture does not cause the organizational workflow to change completely.

3.5.3 Technology infrastructure

Finally, there is the technology infrastructure aspect area of the ISA for SCS [Mulholland et al., 2006]: *The Technology Infrastructure Aspect Area adds knowledge about types and structure of infrastructure components ("boxes and wires") that support the information systems and actors.* In light of SCS, in this thesis the focus is less on the technologies interconnecting the different information systems but more on the sensor technologies that can be used. These technological possibilities have an influence on the ISA for SCS.

Developing an ISA is bounded by the technological possibilities because developing it outside the technological possibilities will render the system unusable in practice. A reason for designing a system outside the technological possibilities can be that current standards are not sufficient to guarantee the security of the SC. If this is the case, the security architecture can be used as a recommendation for future technological development.

It is also useful to keep in mind the technological developments in the market. This will make sure an ISA can be complemented with these developments or that the ISA is adaptable to these developments. Making sure the ISA is adaptable will increase the acceptance of the system and will ensure that the system is functional for a prolonged period.

3.6 Framework for developing an ISA for SCS

In the previous section, the requirements of an ISA for SCS are described from both the government and business point of view. In addition, the constraints of the current state of the ISA and the technological possibilities are considered. In order for an ISA for SCS to satisfy these requirements, a framework is introduced describing the main characteristics an ISA needs to succeed. In this section, a general description is given taking into account the needs of the organizations described in section 2.3. In chapter 6, this framework will be used to propose an ISA for SCS within the scope of different scenarios.

According to Bocij, et al. (2003, p. 424) a good quality information system:

- Is easy to use;
- Provides the correct functions for end-users;
- Is rapid in retrieving data and moving between different screen views of the data;
- Is reliable;
- Is secure;
- Is well integrated with other systems.

The list of characteristics depicted below is based on Hakkennes et al. (2006) where a theoretical framework is described for designing an identity management system in an e-commerce setting. The different characteristics are adapted and related to an ISA for SCS. The characteristics depicted in Figure 17 will be described in the remainder of this section.

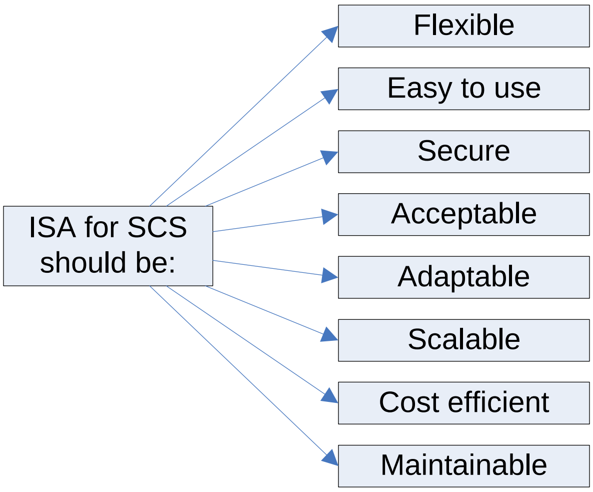


Figure 17: List of characteristics for an ISA for SCS

3.6.1 Flexible

The first characteristic an ISA for SCS has to succeed is to be flexible. The flexibility of an ISA is divided into different sub-characteristics. First, there is the flexibility in the different protocols used. Because of the great diversity of protocols already used in the information exchange between the different parties in the container transport, an ISA should support these different protocols. Examples of different protocols are the Simple Mail Transfer Protocol (SMTP) and the File Transfer Protocol (FTP). Supporting different protocols does not mean that different formats of messages are supported. The flexibility to support different formats is defined in the second sub-characteristic.

The second sub-characteristic is that an ISA should support different kinds of message formats. Also because of the large amount of existing information systems that exchange information in different formats, the conversion from one message format to the other should be done somewhere in the system. This can be done at the sender or receiver side of the information exchange or it can be done at the central organization in the CIM information exchange model. Enabling different information systems with different message formats to connect to the ISA for SCS will increase the acceptance because existing investments are preserved.

Besides the flexibility in protocols and message formats used, an ISA should offer flexibility in accessing the information available in the ISA for SCS. Offering the possibility to build in the information exchange for SCS into the local information system or offering web-based access to the security relevant information are two of the several possibilities available. Supporting several information access models will enable the different organizations active in the SC to choose the model most suitable for their organization.

3.6.2 Easy to use

The second characteristic an ISA for SCS has to succeed is that it has to be easy to use. With regard to SCS, this is not exclusively related to the ease of use for the end users of the system, but also for the organizations in general. This means that the ease of use for the in-house software architects (in the case of integration of the ISA for SCS in the internal business systems) also needs to be considered. The ease of use is especially important for those organizations that have a low interest in SCS, but are relevant parties for supplying information or want to monitor simple security relevant information. For those organizations that have a high interest in security relevant information (e.g. the Customs), often the consideration between ease of use and functionality is made in favor of functionality.

3.6.3 Secure

Additionally, an ISA for SCS should be secure because security relevant information can be competition sensitive or may cause security threats on its own. If, for example, information regarding the contents of the container comes into the wrong hands, this increases the risk in the logistic process. For consistency purposes, security of the security relevant information is called information security. The term security is used to denote the security of the SC. The information security of the data contained and exchanged in the ISA is divided into three parts. The three parts are the storing, retrieving and exchanging of security relevant information.

Storing and retrieving security relevant information

Essentially, there are three ways of storing security relevant information:

- The information can be stored at the sending end and at the receiving end of the communication line (in the case of push-based communication);
- The data can be made available at the sending end of the communication line;
- The data can be made available at a central organization (even in the case of a central organization local data repositories may exist because the CIM can also be used on a push basis).

This directly introduces the alternatives for retrieving the information. The information can be retrieved from different sources when it is needed by the end user or it can be retrieved from a local data repository. This data repository should contain all data the user might require to see. In a service-oriented architecture, the data can be made available at the sending end of the communication lines or at a central organization. This eliminates duplication of data and information is only exchanged if the user needs this information.

The different alternatives for storing and retrieving security relevant information are depicted in Figure 18.

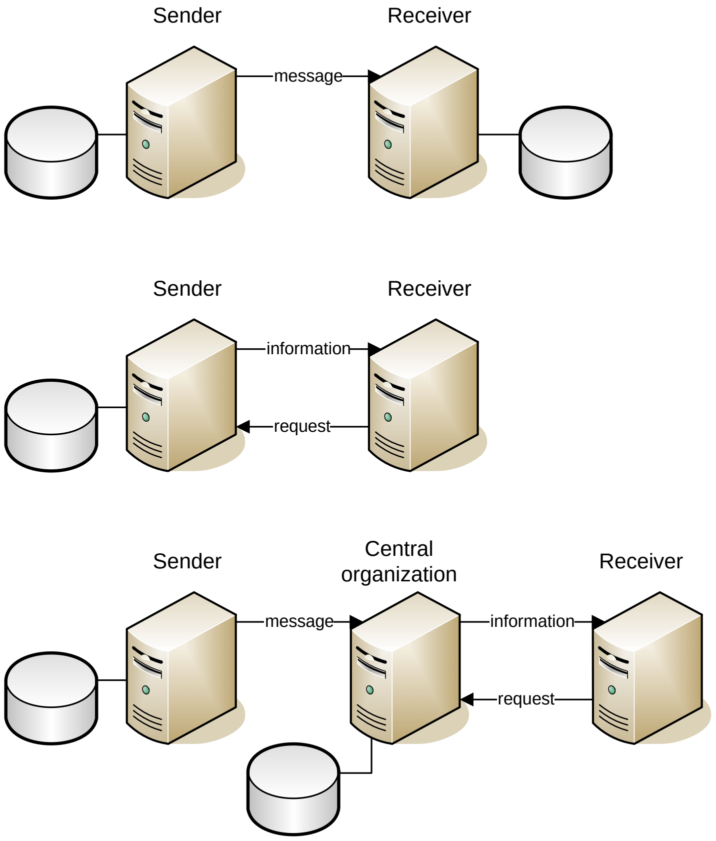


Figure 18: Storing and retrieving security relevant information

The first part of Figure 18 shows exchange and storage of data as used in the BIM. The sender sends a message to the receiver thus both keep a copy of the message.

In the second part of Figure 18, the storage and retrieval in the DIM model is shown. In this model, the receiver retrieves the information from the sender by sending a request to the sender. The sender then sends the information to the receiver. Because this process can be repeated, the receiver does not have to store the information, but can retrieve the information on demand.

In the final part of Figure 18, the storage and retrieval in the CIM model is illustrated. In this model, data is retrieved by the receiver from a central organization that has received the information from the sender in a message. The receiver does not have to store the information because it can be retrieved from the central organization. An alternative is that the central organization does not store any information but only acts as a conversion step in the information exchange process. The receiver requests the information from the central organization. This organization retrieves the information from the sender and converts this information. This converted information is send to the receiver. If the central organization does not convert any information, the third model is no different than the second model of Figure 18.

Exchanging security relevant information

In the exchange of the information, the communication should be secure (information) because otherwise non-authorized persons can access the information. For communication between SC organizations, this means that secure information connections should be used for competitive sensitive data and for security relevant information that could cause security threats on its own. Another important aspect of the exchange of information in an inter-organizational setting is the access control to the information. As soon as information is made available to other organizations this information is out of control of the sending organization. Clear agreements have to be made regarding the ownership of the data.

Confidentiality, integrity and availability

Information security of the different exchange models is related to the CIA (confidentiality, integrity and availability) criteria described in the British standard 7799 [BS 7799-1:1999]. The information security aspects can be divided in terms of confidentiality, integrity and availability and are defined as follows:

> *confidentiality: ensuring that information is accessible only to those authorized to have access;*
>
> *integrity: safeguarding the accuracy and completeness of information and processing methods;*
>
> *availability: ensuring that authorized users have access to information and associated assets when required.*

Definition 8: Information security

In all three information exchange models, confidentiality is very important since the messages exchanged can contain competition sensitive information or the information itself can cause security threats. Only those authorized to access the information should be able to access it. In the BIM, the confidentiality has to be managed at every individual actor that makes available information to other parties. In a bilateral communication, each pair of organizations has to reach agreement about the way to maintain confidentiality and there has to be a consensus of what is considered confidential. In a CIM, the confidentiality only has to be managed at one side. This improves manageability of the information security. In a DIM, the confidentiality again has to be managed at every individual actor. On top of this, the actors in the SC have to agree upon the definition on how confidentiality is managed and maintained. An organization does not want to supply information to a party that does not comply with the confidentiality demands of the first company.

The second aspect of information security is the integrity of the information contained within an ISA. From the point of view of information security, the information should be as accurate as possible. In a push-based information exchange model, the information at the receiving end of the communication line is as accurate as it was at the moment of sending. If afterwards the information has changed and the receiver is not informed, the information is not accurate anymore. If security relevant information is made available to the receiver on pull-base, the information is always up-to-date.

3.6.4 Acceptable

An ISA for SCS should be acceptable. Increasing the acceptability increases the number of users, which in turn increases the value of the total network. In interviews with Port infolink and Cargonaut it became clear that the value of a community system is extensive when a large degree of coverage is realized [Interview 4 Cargonaut (WP 5.2)]. Many companies just use a community system because many other companies are using it. Most security measures are only relevant and valuable if 100% coverage is obtained. Otherwise, the person that, for example, wants to commit a terrorist attack will find the 1% that the security measure does not cover [Interview 8 Kuehne+Nagel (WP 5.1)].

3.6.5 Adaptable

The adaptability of an ISA is also very important. An adaptable ISA for SCS ensures that new information exchanges can be added without compromising the future usefulness of the system. It is possible that also in a setting where the information needs are already very extensive, they are even further extended by new information exchanges. This means that new information exchanges should be easy to implement without inducing high costs to the SC actors. Also in a setting where not yet all possible information exchanges are implemented it is sensible to make sure the ISA is adaptable to anticipate on a possible growth of information needs.

3.6.6 Scalable

That an ISA for SCS is scalable means that the number of transactions (information exchanges) between SC actors and the number of actors can grow substantially without the ISA becoming slow or even unresponsive.

A point to take into account is the fast growth of the container transport in general. The growth of the container transport will also increase the number of messages exchanged between the SC actors and it will thus increase the exchange of security relevant information. An ISA for SCS that supports this will ensure the system to be usable for a prolonged period.

3.6.7 Cost efficient

A cost efficient ISA for SCS simply means that the ISA offers a low cost per transaction. The price should be relative to the functionalities of the system taking into account that a more complicated architecture with larger information coverage is more expensive than an ISA that is less complicated.

Especially for cost-conscious companies this is an important property because it will increase acceptance of the system by these companies. In a setting where the information needs are extensive because of a high perceived value of security relevant information, the cost of information exchange is less important. In this case, it is still relevant to look for low cost solutions if the solution performs within the set of other characteristics.

Besides a low cost per transaction, also the collateral benefits of the information exchanges have to be considered. If certain information exchanges are also relevant for increasing the efficiency of the operations in the SC, the cost of using the ISA for SCS can be recovered.

3.6.8 Maintainable

Finally, an ISA for SCS should be maintainable. This means that when the system crashes or produces errors the system should be easily repaired. According to Looijen (2004), maintaining an information system results in repairing errors, prevention of errors and adaptation of the information system.

Looijen (2004) defines three forms of maintenance. The first is functional maintenance, which makes sure the functionalities of the system are maintained. The second is application maintenance, which makes sure the applications (on a higher level than the functionalities) and the data stores are maintained. The last type is called technical maintenance and is responsible for making and keeping the system operational because the system must be continually available.

3.7 Conclusion

In this chapter, the concept of an ISA was described in more detail. This was needed because it forms the basis for the analysis in chapter 4 where the current state of the ISA for SCS is outlined.

First, a description of an ISA from a theoretical point of view was given. It was shown that the client/server architecture is the most common used architecture in the exchange of information in the SC for container transport. The architectures differ in the way information is distributed between the SC actors. In this respect, different models for information sharing were described. These information exchange models are BIM, CIM and DIM; all having their own advantages and disadvantages. It was shown that when a large number of communication lines exist for the same message the CIM has preference over the BIM. Whether a DIM is used depends on the degree of market driver and on the degree of adaptability needed. Currently in the SC for container transport, the DIM is rarely used and it is therefore questionable if the DIM will be used in the near future.

Second, the factors that have an influence on the future state of an ISA for SCS were described. The needs and requirements from the actors in the SC, derived in work package 5.1, are of importance for a future state of the ISA for SCS. Besides these requirements also the current state of the ISA and the technological possibilities for security measures are of influence to the new ISA. In the new state the SCS is increased which may also cause the SC reliability and efficiency to be increased.

Finally, a framework was introduced to aid in the development of an ISA for SCS. In this framework, a number of characteristics were defined that the new ISA has to satisfy in order to be successful. These characteristics are: flexible, easy to use, secure, acceptable, adaptable, scalable, cost efficient and maintainable. These characteristics will be used in chapter 6 for the development of the ISAs for SCS (within the scope of different future scenarios).

4 Current state and development of the ISA for SCS

In this chapter, the current state and development of different types of information systems are described in more detail. In section 4.1, an introduction is given about the current information exchange between the SC actors. In section 4.2, the more Neutral or open community systems that are used in the SC are described. These systems include the Port community systems of Port infolink and Cargonaut. In section 4.3, Authority systems are described. These systems include Customs systems and Seaport police systems. Additionally, in section 4.4 Container integrity systems (CISs) are discussed; these include the CommerceGuard and the Savi Networks system that are used in combination with electronic seals in order to monitor the integrity of the container (these electronic seals can also be used to monitor other aspects of the container like temperature or humidity). Finally, in section 4.5, Business (community) systems are discussed. The different ISAs are illustrated in the following three-layer model described in Willis et al. (2004).

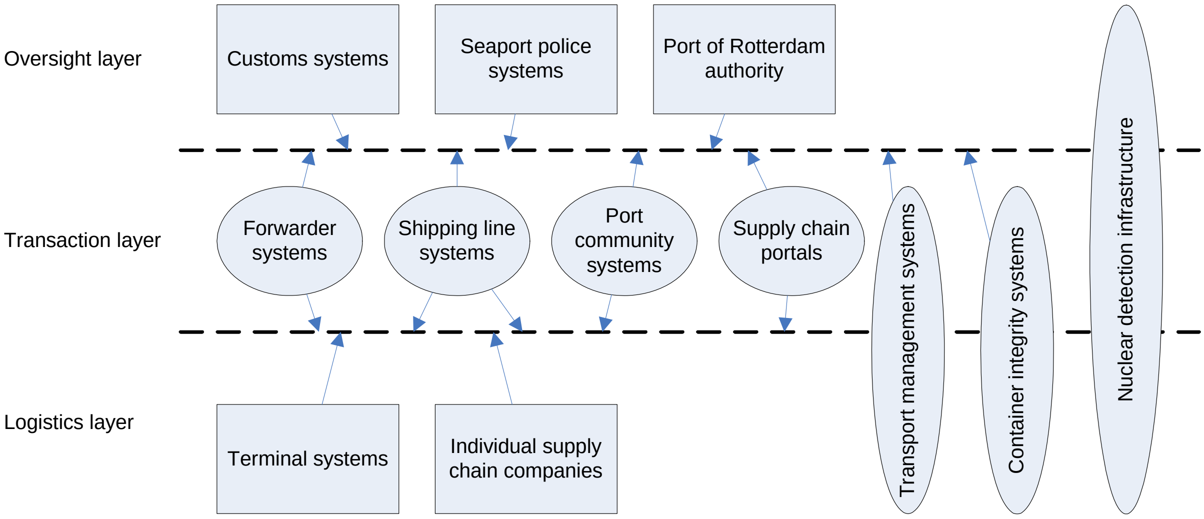


Figure 19: Three layer model of the different ISAs

The SC is divided into three different layers. Below is the logistics layer. In this layer, the companies and there information systems reside that physically handle the containers. Essentially every individual SC company is a potential point of analysis, but in the analysis in this chapter, only the terminal systems are considered. Second, there is the transaction layer. In this layer, the companies that are active in mediation and SC management are depicted. On top, there is the oversight layer. In this layer, there are the regulatory authorities that have a controlling role over the operations in the transaction and logistics layer. Some information systems and communities transcend the boundaries of the layers in the SC. The nuclear detection infrastructure, for example, is used to connect the physical operation in the logistic process to the oversight layer in order for the Customs to determine if it is secure to transfer a container. In addition, CISs are used to enable the companies active in the transaction layer, to monitor what happens in the logistics layer. The information if a container is transferred incorruptibly is also interesting for the regulatory authorities to determine whether it is secure to transport this container.

In this chapter, the following notation is used for the description of the different aspects of the ISA for SCS.

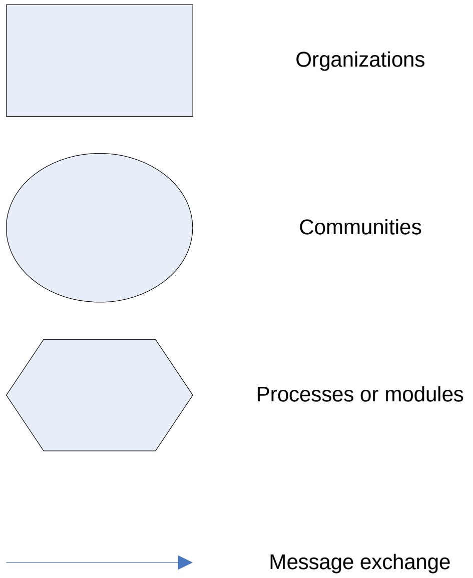


Figure 20: Notation used in chapter 4

A rectangle is used to denote an organization and the information systems contained within the organizations. If two organizations are interconnected by a message exchange this implies that the BIM is used. When the CIM is used this is denoted by the usage of a community (oval). Communities are central organizations that can aggregate, translate and relay information that is exchanged between the actors in the SC. Furthermore, the hexagon is used for processes or modules of specific functions within a company or community. Finally, a line indicates information exchange between two entities (organizations or communities). Line arrows show to which entity the information is made available. In the following section, the current information exchange is introduced.

4.1 Current information exchange in the supply chain

As described previously, on top of the current information exchange, additional information can be shared between the different organizations in the SC to enhance the security of that SC (section 1.2). In the SC, information between the actors is already shared in different ways. The simplest form of information sharing is the exchange of physical documents. The process of physically exchanging documents, however, is time consuming, information is not real time (delay between sending and receiving of the information), communication is prone to errors and the process is very labor-intensive.

Due to the advances in information technology (IT), document or information exchanges can be automated between organizations using al kinds of technologies. Since the 1960s companies have used technologies such as electronic data interchange (EDI) to communicate essential documents with each other [Weitzel et al., 2000]. In administration, commerce and transport EDIFACT (Electronic Data Interchange for Administration, Commerce, and Transport) is a widely accepted EDI standard. In the port of Rotterdam, Port infolink uses the UN/EDIFACT standard as a basis for the exchange of numerous documents between the different parties in the SC [Port infolink, 2006].

To enable inter-organizational information sharing, different types of ISAs can be used. In the current setting, the different organizations in the SC have their own information systems and they exchange data between the information systems using EDI, as described above. Because the process of sharing information using EDI is expensive and complex [Iacovou et al., 1995; Steel, 1996; cited in Jui-Lin et al.], Weitzel et al. (2000) proposes the use of XML as a universal data format for business-to-business (B2B) communication. Small and mid-sized enterprises (SMEs) can integrate EDI-processes into their ISA at lower costs using this method.

Because the SC for container transport consists of many SMEs, the use of this technique will increase the number of organizations that use inter-organizational information sharing compared to using only EDI [Weitzel et al., 2000].

The disadvantage of using XML for communication is that many of the current ISAs only use EDI messages and thus do not support XML. The port community system of Port infolink (described in more detail in section 4.2.1) already promotes the use of XML messaging, but also facilitates the use of EDI messaging. Therefore, the use of XML for exchanging security related information/documents would cause current systems to be changed, which would incur adaptation costs. It is questionable if the advantages of lower implementation costs weigh up against these adaptation costs. If many organizations in the SC are using EDI, it is better to use the EDI infrastructure for exchanging security related information. Because the use of EDI is relatively standardized and Port infolink (see section 4.2.1) facilitates continuously growing numbers of document exchanges using EDI it is rational also to use the EDI infrastructure to facilitate the communication of security related information.

4.2 Neutral or open community systems

In this section, the more neutral or open community systems are described. These community systems are used by the actors in the SC to exchange information and can deliver different operational functionalities. Important neutral or open community systems are the port community system (PCS) of Port infolink in the port of Rotterdam and the PCS of Cargonaut in the air transport in Schiphol. This type of neutral system is described in detail in the following section. Other neutral or open community systems identified, but not discussed, are SC portals and transport management systems.

4.2.1 Port community systems

First, a general outline of a PCS is given after which the ISA of Port infolink and Cargonaut are described in detail. Cargonaut is not active in the container transport as defined in the scope of research in this thesis, but is active in the information exchange for the transportation of goods with aircrafts. The current structure and initiatives of Cargonaut are used to compare the two PCSs. Approaches in the PCS of Cargonaut can be used as possible improvements for the PCS of Port infolink or vice versa.

A PCS is a system delivering and transferring information to and from the different supply chains operating in the port the PCS is supporting. A PCS is defined as follows by Capgemini [Smit, 2004]:

> *A port community system can be defined as 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.*

Definition 9: Port community system

A PCS can be seen as a central hub for communication between the different parties in the SC. Instead of different bilateral communication lines between the organizations, a PCS acts as a centralized party delivering the messages to and from the different organizations in the SC. A PCS is an example of the central information exchange model described in section 3.2. Furthermore, a PCS can store information for future use, or it can store information to make it available to other parties in the SC.

A model representing the communication lines in the container transport in the port of Rotterdam is given in Figure 21.

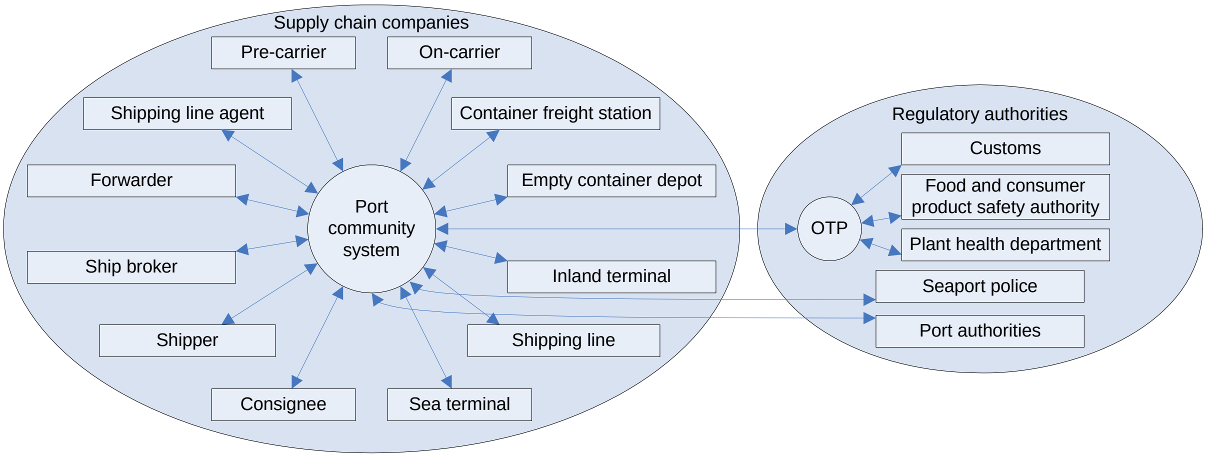


Figure 21: Users of the PCS

In this figure, the different organizations involved in container transport are shown. Ideally, these organizations communicate with each other via the PCS, although communication might also go between parties directly. On the left, the companies active in the SC (as described in section 2.2) are depicted and on the right, the regulatory authorities are depicted. The PCS sends and retrieves information on behalf of the SC companies to and from the regulatory authorities using the government transaction port (OTP). Figure 21 illustrates the situation for the port of Rotterdam and is comparable to the situation for Port infolink. In the following subsections, the PCS of Port infolink and Cargonaut are described in detail.

Port infolink

Port infolink started in 2002 with the development of a PCS to support the organizations involved in the supply chains going through the port of Rotterdam.

The ISA of the PCS of Port infolink is shown in Figure 22 [Interview 1 Port infolink (WP 5.2)].

Some organization involved in the container transport in the port of Rotterdam can communicate with the PCS using the Internet infrastructure. This means that the physical location of the organization is not important and that the organizations can connect anywhere-anytime to the PCS.

There are two ways of communicating with the PCS: (1) the organization can send data to the PCS in XML or EDI format by means of (S)FTP, AS2/3 or WebSphere MQ or (2) the organization can use one of the many applications the PCS is offering using a web browser.

If the organization chooses to send some data to the PCS, Port infolink converts this message to an internal, uniform XML format for use in its core system and application logic. The core, that is the heart of the PCS, is mainly used for messaging and stores these messages in a database. This data can then be used later in the logistic process by the same or other party that originally submitted the data.

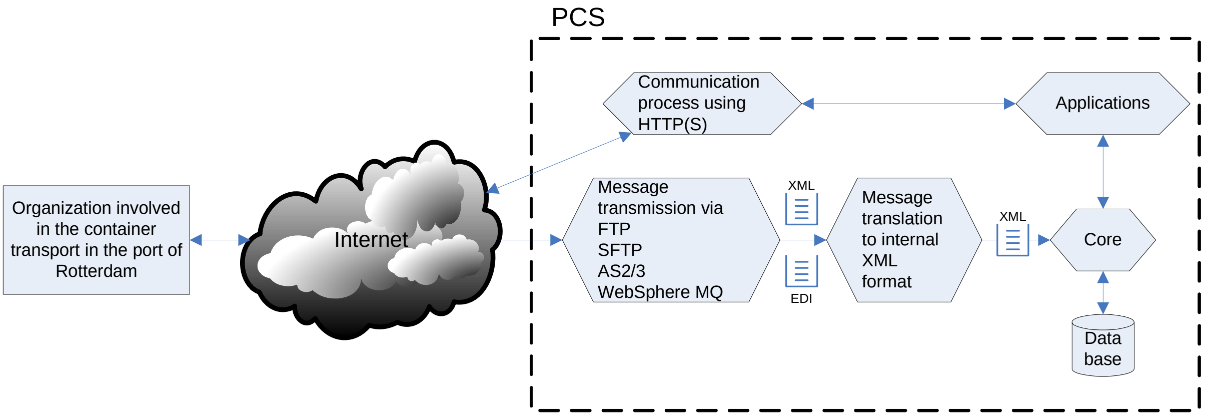

PCS
Communication process using HTTP(S)
Applications
Organization involved in the container transport in the port of Rotterdam
Internet
Message transmission via FTP SFTP AS2/3 WebSphere MQ
XML
EDI
Message translation to internal XML format
XML
Core
Data base

Figure 22: ISA of Port infolink

The second way is by accessing one of the many applications the PCS is offering with a web browser, since they are all web based. Applications use the core of the PCS, which uses stored data of previous messages or can store additional information in the database. The web applications can also be used as data entry applications, instead of using EDI or XML messages described earlier. The organization that enters the information into the PCS will always be the owner of the data, which means that no other party can access this information unless the requesting organization is explicitly granted access to the information.

Currently the focus of Port infolink is on the exchange of planning information such as cargo, carrier and arrival and departure information. Because the system is already in use for numerous information exchange processes, there is a lot of information available in the PCS. Adding extra data elements to existing messages or adding new messages can be fairly simple because of the great adaptability of the PCS. If, for example, a certain data element is added to an existing message, it is very simple to include this extra data element in the PCS. Adding this data element to the information systems of all individual organizations is more cumbersome. From the point of view of the PCS, the addition of security relevant information can thus be achieved very easy, but there are more far-reaching implications for the overall ISA in the SC.

For Port infolink, there are two different types of communication: the communication between companies and the government (B2G communication) and the communication between companies (B2B communication).

Information exchange between PCS and the regulatory authorities

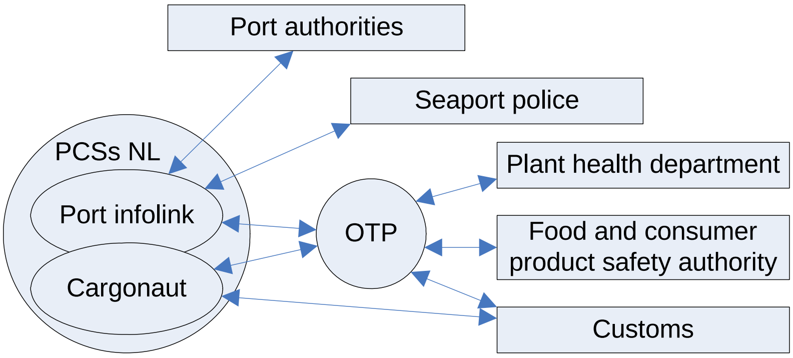


Figure 23: B2G communication using a PCS

In this figure the PCSs of Port infolink and Cargonaut are depicted on the left. The SC companies provide information to the PCS that communicates on their behalf with the government. Most of the communication with the government is transferred via the government transaction port (OTP). The information flows via the OTP to the relevant government authority.

Electronic communication from the government to the SC companies also is transferred via the OTP. This means that the OTP is a digital post office for most electronic communication between the business and the government. The OTP is not a community on its own because no information is stored and no conversion of the messages takes place at the OTP. In addition, there is no information reuse between the government organizations via the OTP.

The PCS of Port infolink also has direct connections to the regulatory authorities like the Port of Rotterdam Authority. Moreover, the Customs has direct insight in the information system used by Cargonaut.

In the following subsection, the PCS of the airport Schiphol (Cargonaut) is described. Subsequently, a comparison is made between Port infolink and Cargonaut.

Cargonaut

Cargonaut is the company that developed and implemented the PCS for the airport Schiphol in the Netherlands. The system of Cargonaut supports the information exchange between the different actors involved in the logistic process in the Schiphol area. The degree of coverage of the Cargonaut system is very large which means that most of the information exchanges between the businesses or business and government take place using the Cargonaut system.

The SC as defined by Cargonaut is less extensive than the definition used in this thesis. For the Cargonaut system, the SC for export begins at the gate-in at the Schiphol area and ends with the loading of the aircraft. Their part of the SC coverage then ends and it continues with the airline company, which transfers information to the PCS of the airport of destination. For import, the SC begins when the aircraft arrives and it ends when the goods leave the Schiphol area. In light of SCS Cargonaut is thus primarily focused on exchanging security relevant information for this part of the SC.

An important advantage of the PCS of Cargonaut is the focus on both B2B and B2G communication. Community systems in other airports are focused more on one of the two types of communication, which will undo many of the advantages of a community [Interview 4 Cargonaut (WP 5.2)]. The primary driver for exchanging security relevant information in air transport is the government. This means that a lot of information flows from the businesses to the government via the Cargonaut system. In most cases this is done with obligatory declarations (like in the container transport), but in the case of Cargonaut the Customs has access to all information available in the PCS. The demand for security relevant information from the SC companies in the air transport is low [Interview 4 Cargonaut (WP 5.2)].

In the following diagram, the high-level architecture of Cargonaut for the import process is illustrated.

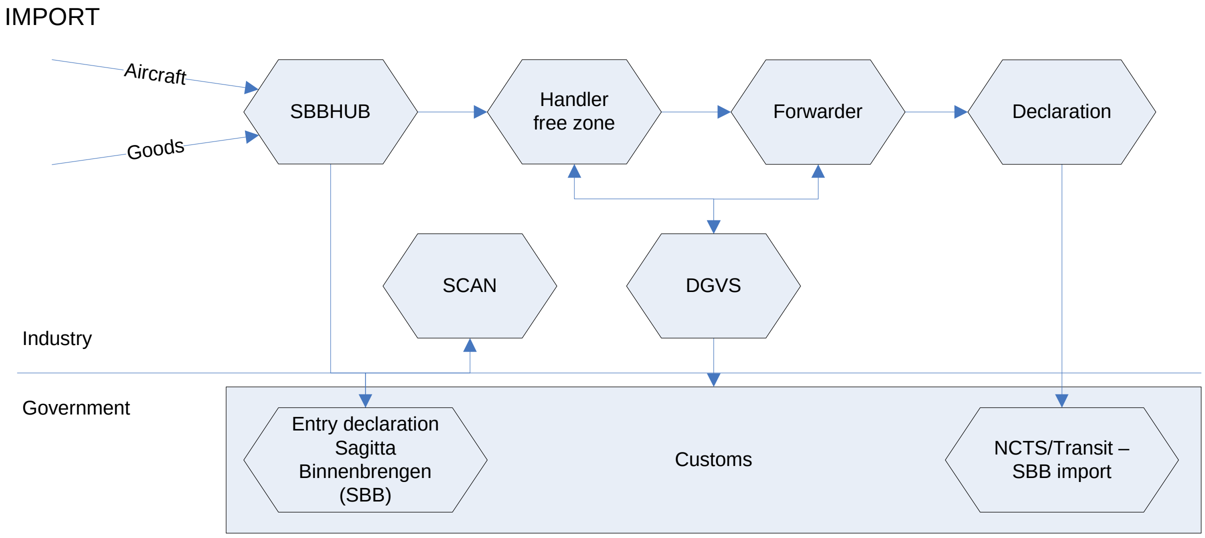


Figure 24: ISA of Cargonaut for import

Information about the goods and the aircraft enter the Cargonaut system via the SBBHUB. This module is used to do the entry declaration to the Customs for Sagitta Binnenbrengen (SBB). The Customs uses this information to make a risk analysis and selects goods that will be scanned. This information flows back to the Cargonaut system in the SCAN module.

The logistic process continues in a free zone, which means the goods can move freely between the different companies in this free zone. The module Documentloos Goederen Volgsysteem (DGVS) (Tracking of goods without physical documents) is used to track the goods in the free zone and the Customs has complete insight into this system.

The logistic process continues with the forwarder and all information gathered in the logistic process is used to do the final declaration to the Customs for Sagitta Binnenbrengen import. The scope of Cargonaut ends with this final declaration and the goods are in the inland transport.

For the export of goods, a similar process is used which is depicted in Figure 25.

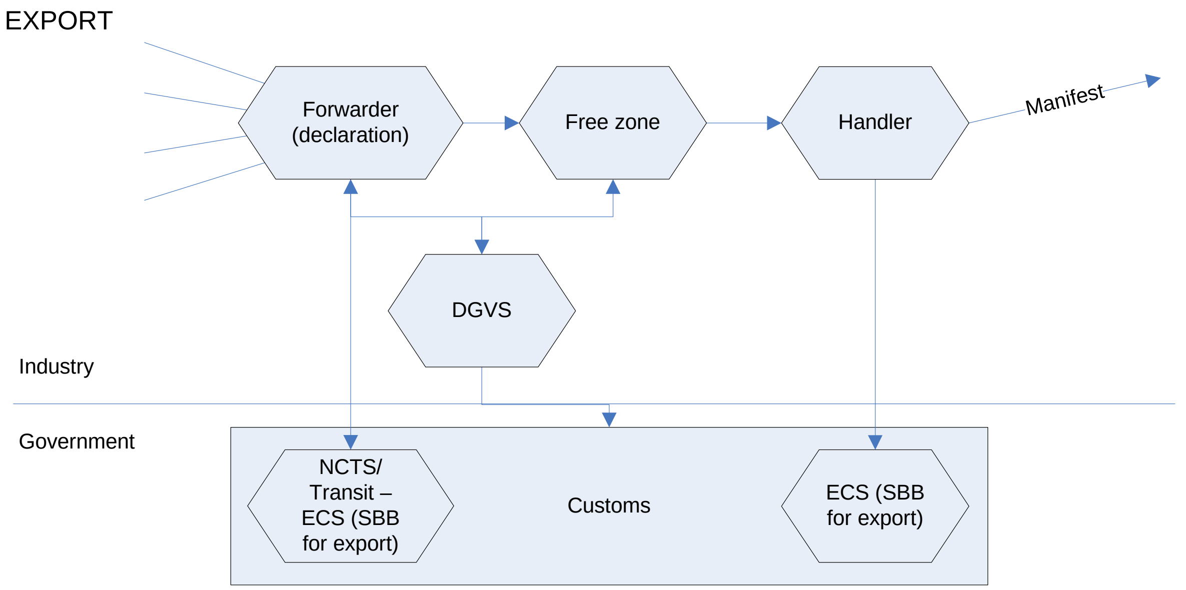


Figure 25: ISA of Cargonaut for export

The SC in the Cargonaut system now starts when the goods enter the Schiphol area. Before the goods may enter the free zone in the Schiphol area, the goods have to be declared. The information for the declaration to the government comes from the forwarder and goes to the NCTS/Transit system.

When the goods have entered the free zone, the movements of the goods are registered in the DGVS module. The Customs again has direct access to the DGVS system and can monitor all goods movements in the free zone. After the handler has loaded the goods into the aircraft, the manifest is sent to the airline company and a declaration is sent to the government Export Control System (ECS). This system is comparable to the SBB system for import. The airline is the link between the port of departure and the port of destination. If the processes and information exchanges between the different Customs are more standardized the information can be sent directly to the Customs at the port of destination.

Important is that the Cargonaut system offers different methods for sending and changing information in the Cargonaut system. Information can be send using EDI messages and some information can be submitted or changed using web-services.

Similar to the PCS of the port of Rotterdam is that the sender of the data always stays the owner of the information. This means that no one has access to the information unless this party is the owner of the data or is explicitly granted access to the information.

In the following subsection, the PCS of Port infolink and the PCS of Cargonaut are compared. This comparison is not made to make a value judgment of the PCSs, but serves to discover and to emphasize the reasons for certain choices.

Comparison between Port infolink and Cargonaut

The most important difference between the two PCSs is the degree of coverage. For the Cargonaut system, the degree of coverage is 100% for both B2B and B2G communication, but for many companies in the container transport this number is lower [Smit, 2004]. The main drivers behind this high coverage are the concentrated situation and the high time pressure. Because the goods have a low lead-time and delays are very costly a close cooperation and thus an extensive and swift information exchange is required. This close cooperation ensures low lead-times are obtained and high information availability towards the government ensures less intervention of the government.

Another difference between the two PCSs is that the Customs has full insight in the Cargonaut system while the Customs in relation to container transport only has information that is sent to the Customs in the form of declarations. If the Customs has complete insight into the community system, there is the drive to exchange information outside of the community system. Because the timing of the information in the logistic process and the high integration of the SC actors in the Schiphol area is that important, the drive to use the community system surpasses the drive not to use the community system.

Furthermore, there is a difference between the scopes of both PCSs. Cargonaut has chosen to focus on the Schiphol area from gate-in to gate-out. With this, Cargonaut thus focuses more on the depth than on the width of the scope. Cargonaut pays close attention to the demands of the SC companies and the need has not arisen to widen the scope of the Cargonaut system.

A similarity between the both PCSs is the wide array of different channels in which the exchange of information is supported between the SC companies and the PCS. The drive exists to offer web-services (web sites) to submit and change information, but traditional EDI message exchanges are also supported.

4.3 Authority systems

In this section, authority systems are considered. These information systems or set of information systems are used by authorities for numerous reasons. The Customs, for example, uses information systems to analyze information that is received from the SC companies for a risk analysis. In the remainder of this chapter, the different authorities and their systems are discussed. First, the systems of the Customs are discussed. Second, the information systems used by the seaport police are described and finally the nuclear detection infrastructure used in the port of Rotterdam for detecting nuclear contents in containers that are transshipped to or from train and trucks is described.

4.3.1 Customs systems

Historically, the approach of the Customs was on the levying and recovery of Customs rights. This includes the recovery of import duty and excise. The focus thus not was on security relevant information, but more on information relating to the fiscal objective of the Customs. Partly due to the terrorist attacks in America and Europe and the sharpened security demands from politics, the focus on security related information was added to the Customs' objectives. Currently the activities for the fiscal and security objectives cannot be seen separately.

Information for inspection is exchanged in different ways with the Customs. Between the SC companies and the Customs still paper information exchange exists, but more and more information is exchanged digitally. All information exchange between the Customs and the SC companies uses the government transaction port (OTP). This port is used for message relay between the companies and the government in general. Currently only some information is exchanged with the OTP, but there is the intention that in the future all digital information is exchanged with the OTP. The OTP does not convert or aggregate information (see section 3.3), but is only used for message relay. Information is exchanged on a bilateral base between the business and the Customs, although message standards are enforced by the Customs to ensure information uniformity. The Customs has government power thus leaving the information conversion to the business parties. Information contained within the business systems, is often converted into a target format before sending this information to the Customs.

Information that is meant for and used by the Customs is stored locally at the Customs. If other regulatory authorities (government) want to use it, bilateral arrangements are often made for exchanging information. In this respect, the Customs can function as a portal for the supply of information for other regulatory authorities. In some areas, this is already the case where information gathering and processing is outsourced to the Customs.

International exchange between Customs organizations

Within the European Union (EU), regulatory authorities are collaborating to exchange information between member states. Currently, already information concerning transit (import) is exchanged between the member states. In the near future Customs authorities will exchange more information among themselves about declarations. This is done to improve the inspection of the flow of goods and to make sure that different goods do not have to be declared multiple times. For export, for example, collaboration between the member states in light of transit will start in July 2007.

4.3.2 Seaport police systems

In contrast with the Customs that is responsible for the monitoring of goods movements, the seaport police is responsible for the immigration of people. Each year almost half a million people enter the port of Rotterdam on approximately 33.000 sea vessels [Ordina, n.d.]. Registration of all these people is necessary to do a well-founded risk analysis.

An important information system used by the seaport police is the ZUIS system. This system is used to monitor the flow of information proactively as opposed to reactively where data is entered into the system after the check has completed. This system contains valuable security relevant information that can be used to improve the security in the SC.

From an interview with seaport police [Interview 7 Zeehavenpolitie (WP 5.1)], it emerged that (further) cooperating with other regulatory authorities can help in increasing SCS. Furthermore, it was identified that gathering and exchanging information about incidents helps in improving measures, which in turn improve SCS.

4.3.3 Nuclear detection infrastructure

The nuclear detection infrastructure is used by the Customs to scan every container that enters or leaves the port of Rotterdam by truck or train for nuclear contents. Containers transported by the barge operators are not yet scanned for nuclear contents mainly because of logistical and technological difficulties.

Containers that are identified as emitting radiation are directly taken out of the SC and are scanned with more advanced equipment to measure the radiation level more accurately. If the radiation level is above certain margins, a specialized team is deployed to do a physical check on the contents of the container.

Ideally, for every container it is known if the container was scanned and what the container number is. This is facilitated by the installation of RFID readers in combination with the nuclear detection sensors. For each container that passes the nuclear detection infrastructure and is equipped with a RFID chip, the container number and the radiation level (if existent) are registered.

Currently the information from the nuclear detection infrastructure remains within Customs. It is not communicated to SC companies or to other regulatory authorities (only in case of high radiation levels the Dutch Ministry of V&W is informed). The information flow of the nuclear detection infrastructure is depicted in the following figure.

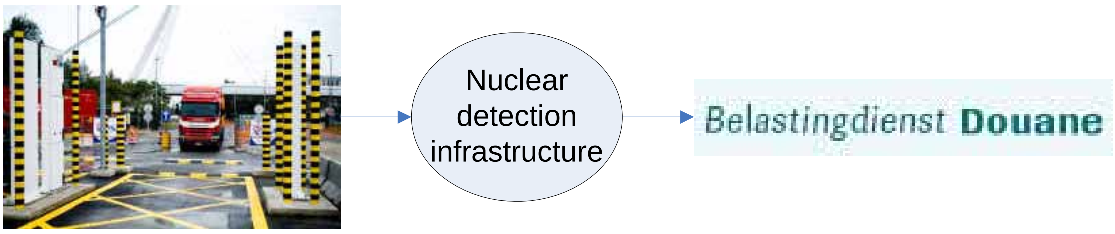


Figure 26: ISA of the nuclear detection infrastructure

4.4 Container integrity systems

In this section, container integrity systems (CISs) are discussed. CISs 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. Commonly some kind of technology is put onto the door to monitor it and some kind of reading infrastructure is used to communicate with monitoring device.

Two different kinds of reading infrastructures are used in practice. The first is a constant monitoring using the Global Positioning System (GPS) and the second is a point-to-point monitoring using a local scanning infrastructure. In the case of CommerceGuard (a General Electric-Siemens cooperation), a RFID reader infrastructure is developed where readers are installed at major ports and at key transport junctions for the current customers of the CommerceGuard system.

The CISs differs in the degree of information that can be supplied using the system. This is constrained by the technology that is put on the door and potential sensor technology that is coupled to the system.

The different CIS initiatives are discussed in the following subsections.

4.4.1 CommerceGuard

CommerceGuard is a CIS and is jointly owned by General Electric, Mitsubishi Corporation, Samsung and Siemens. This system uses a point-to-point based RFID reader infrastructure to track containers that are equipped with the CommerceGuard container security device (CSD). This CSD contains a RFID chip that can be read by RFID readers put into service by CommerceGuard at all major ports and at key transport junctions in the logistic process of the customers of CommerceGuard. Furthermore, the CSD contains sensor technology to monitor if the door was opened or not. The chip registers the moments the container is opened and closed in a log that can be reported to the CommerceGuard system.

A picture of a CSD is shown in the following figure.

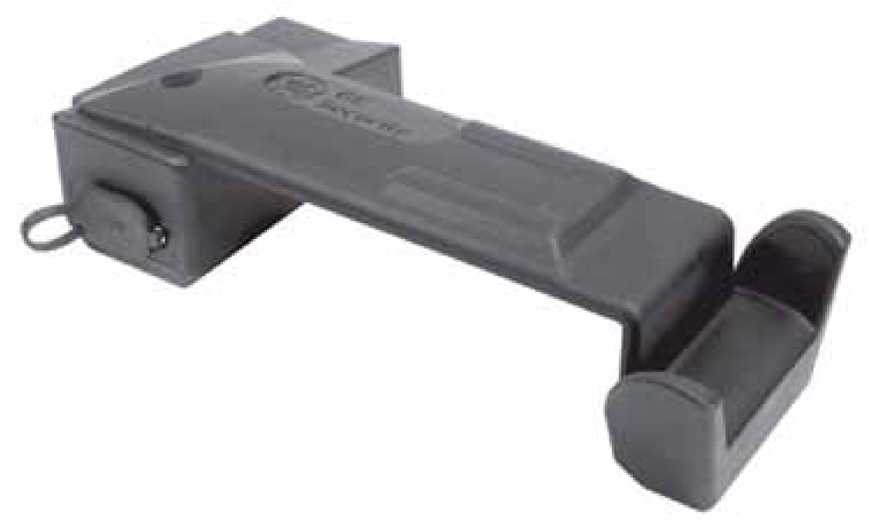


Figure 27: CommerceGuard CSD [GE Security, 2006]

The right hand side of the CSD is put on the outside of the door. The left hand side of the CSD is on the inside of the container and offers an interface for additional sensor technologies. The antenna of the RFID chip is on the outside of the container because of the better readability of the information contained within the CSD.

The idea behind guarantying the integrity of the container is that the SC is considered secure if the organizations who load the goods into the container are believed to be trustworthy and that it can be proven that the container was transferred incorruptibly between the SC actors. The CSD and the RFID reader infrastructure enable the SC actors to monitor that.

Besides the information about the open and close status of the door, additional sensors can be connected to the CSD to monitor, for example, light intensity, humidity and temperature inside the container. This sensor information is reported to the CommerceGuard system every time the CSD comes in contact with the RFID reader infrastructure.

The business model of CommerceGuard is that they sell information that comes from the CSD and RFID reader infrastructure to organizations that use the CSD. Besides security relevant information, the CSD is also used for inventory control, origin risk mitigation and access control [Interview 2 Siemens (WP 5.2)]. Furthermore, the CSD information is made available to the Customs. The Customs can use this information to give a green lane status [Interview 2 Siemens (WP 5.2)] to the organization that uses the CSDs.

The high-level architecture of the CommerceGuard system is depicted in Figure 28.

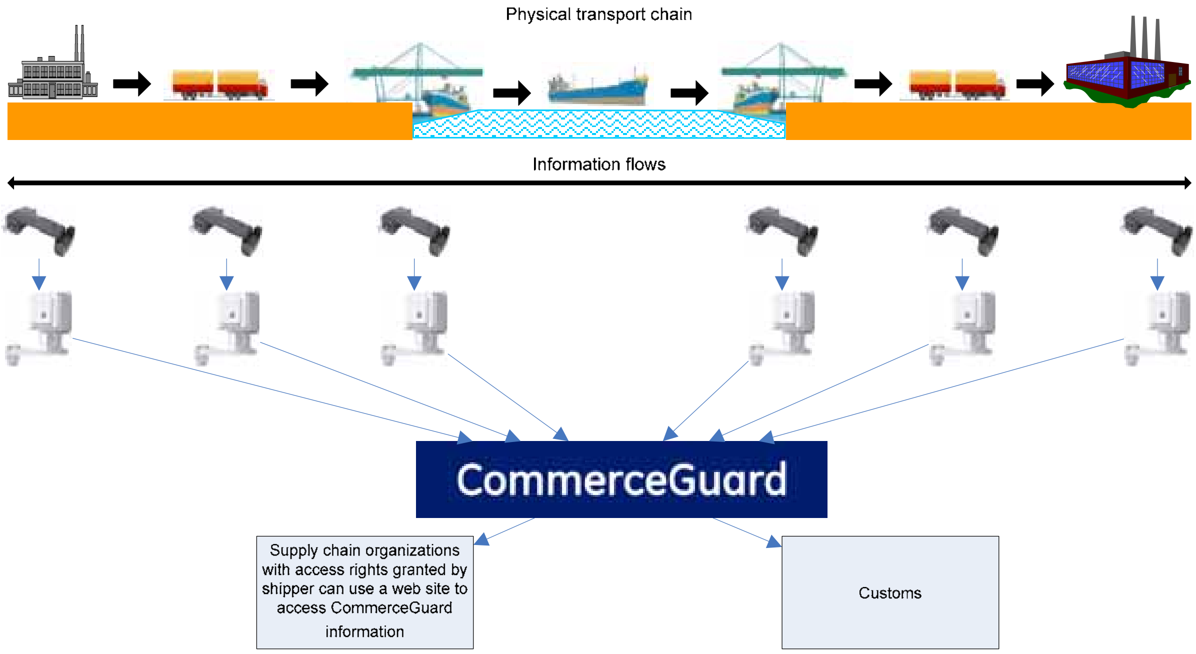

Physical transport chain
Information flows
CommerceGuard
Supply chain organizations with access rights granted by shipper can use a web site to access CommerceGuard information
Customs

Figure 28: CommerceGuard ISA

In the middle the CSDs are depicted. These CSDs are connected to the containers that, each time they come in contact with a CommerceGuard fixed or mobile reader, transmit their status to the CommerceGuard system. These readers are present at key SC locations like the POS, local distribution centers, inland terminals, local and foreign ports and the point of acceptance of the customer. CommerceGuard essentially is one large database with logs of the individual CSDs and their associated shipper. The shipper and every SC actor that is granted access by the shipper can access the status information via a web site and can receive information (push-based) when the reported status changes outside predefined bounds. In addition, the information about which container is equipped with a CSD is made available to the Customs. The Customs can access this information or it can receive this information on a timely basis.

4.4.2 Savi Networks

Savi Networks is a joint venture between Savi and Hutchison Port Holdings. Savi Networks also uses a point-to-point based RFID reader infrastructure to track and monitor containers equipped with SaviTags. Besides offering RFID tags mainly meant for tracking, Savi Networks also offers tags that contain sensors to monitor the door of ISO containers. Savi Networks uses a fixed reader infrastructure that is installed at major ports in the same way as the CommerceGuard system. Mobile readers are offered to customers to trace containers at end-points of the SC. Containers can be monitored whenever they come in contact with a Savi reader. In the following picture, a SaviTag for monitoring the container door is shown.

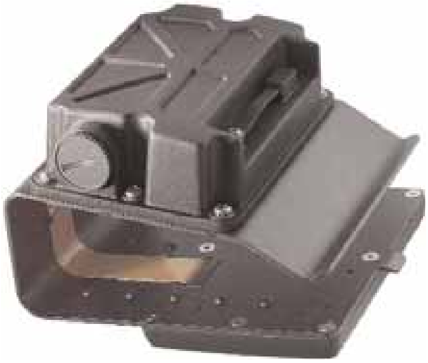


Figure 29: Savi Networks RFID tag [Savi Networks Tag, 2007]

The top part of the device is put on the inside of the container. The antenna is on the outside of the container and enables the communication with a Savi Reader.

The following figure shows the high-level architecture of the Savi Network. On the left, a handheld reader is shown at the POS. The handheld reader communicates with the Savi Networks Hosted Software. In the middle two fixed readers are shown that are installed at the cranes used to embark and debark the containers. Finally, on the right, a mobile reader installed at the point of acceptance is used to monitor the container.

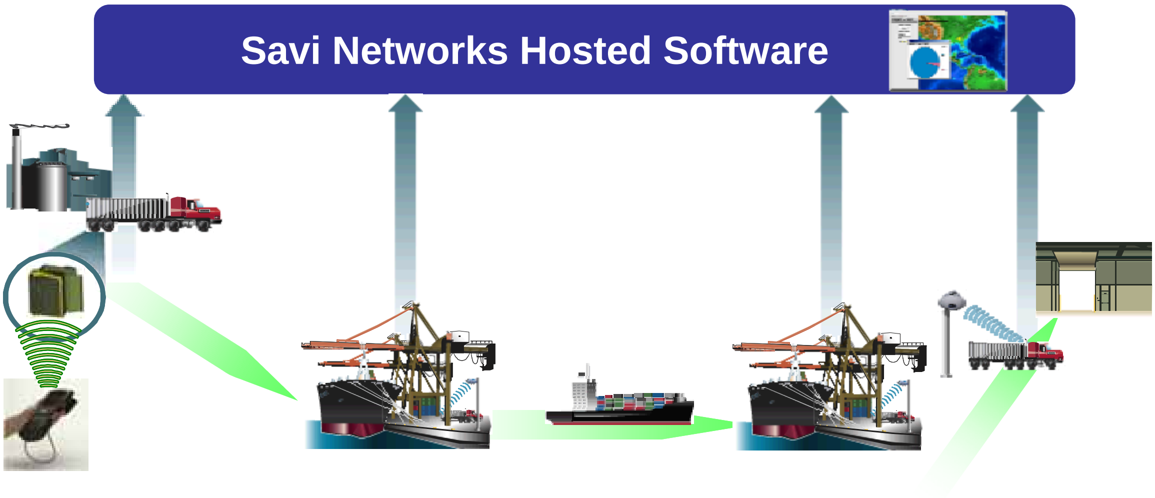


Figure 30: Savi Networks ISA [Verma, 2005]

Information from within the Savi Networks software is made available to the final customers using web-based services, alert services and data services. Data services can be used to integrate the Savi Networks information into the enterprise architecture of individual SC companies.

4.5 Business (community) systems

The remaining category of systems identified is the information systems of the individual SC companies and the community systems set up by groups of SC companies. The difference with neutral or open community systems is that market parties can be excluded from participation in the community. In open community systems like the PCS of Port infolink, no organization is excluded from participation.

Within the different information systems of individual SC companies or within business communities, important information resides that can be used to take measures to improve SCS. It is not feasible to discuss every information system of the individual SC companies, but a short list of the different business community systems is presented.

The different business community systems identified are:

- Forwarder systems – these systems are used for the booking of container transport in merchant haulage;
- Shipping line systems – these systems are used shipping lines in carrier haulage for the booking of container transport;
- Terminal systems – these systems are used for planning and control of terminal operations.

Important information about the operations in the SC resides within these systems. If this information is needed for SCS, it has to be made available to the actor that takes the security measures.

4.6 Conclusion

In this chapter the current state and developments of the ISA for SCS in the container transport was described. The different major information systems were described and the relevance for SCS was discussed. The information systems were divided into four categories.

The first category is those of the neutral or open community systems. These systems are used by the SC companies and the regulatory authorities to exchange information. They act as an information broker between the different actors and fulfill the following functions: information aggregation, conversion and relay. An example of a neutral or open community system is the PCS of the port of Rotterdam put into operation by Port infolink. This system adds value to the business parties enabling them to exchange information more efficiently. The PCS uses a CIM where data is stored centrally and made available to all parties who have access to the information.

In addition, the PCS of the port of Rotterdam (Port infolink) and the port community system of the airport Schiphol (Cargonaut) are described and compared with each other.

In the second category discussed in this chapter, the authority systems were addressed. In these authority systems much information resides that can be considered security relevant. Parts of this information are shared between the different regulatory authorities but are not made available to the SC companies. When the regulatory authorities do communicate with the SC companies, this is often on a bilateral basis. Important information that resides within the authorities is (nuclear) scanning information and information about physical inspection of the (contents of a) container.

Third, the CISs including CommerceGuard and Savi Networks were discussed. These systems supply information about the integrity of the container during transport. They do this by using a RFID reader infrastructure that communicates with devices attached to the container to check the integrity of the container. In the most basic form, these devices measure if the container was opened, but more advanced measuring instruments can be added. Measuring light intensity, humidity and temperature are several of the many possibilities when using these extra modules. The RFID reader infrastructure uses point-to-point monitoring of the container integrity devices. This means that no real-time tracking of the container (contents) can be done. For the CISs, fully centralized systems are used and customers of the CISs can access the information using a website. This means a fully standardized BIM is used.

The final category concerns the business (community) systems. Information systems of individual SC companies are not discussed in this chapter, but an introduction of these systems is given. Often SCS relevant information comes together in business community systems or in neutral community systems. To increase SCS this information has to be made available to the actor that takes the security measures.

The analysis in this chapter forms the basis for the scenarios discussed in chapter 6. In this chapter, different future states are described and the directions for an ISA for SCS are discussed. In the next chapter, the second factor that has influence on a future state of an ISA for SCS is discussed.

5 Technological possibilities and developments

In this chapter, technological possibilities and developments that ultimately have influence on the new ISA for SCS are discussed. From work package 5.1, different information needs have been derived that can be mapped to the current information availability. After this, deficiencies have been identified using gap analysis. These deficiencies require that new information is gathered and exchanged. In this chapter it is discussed how information from the transaction and physical layer can contribute to the security architecture and thus to the security of the SC using technological possibilities and developments.

Within the current state and developments of the ISA discussed in the previous chapter, already some technologies have been discussed that are used in the SC to monitor the physical processes in the SC. These technologies are used to monitor the (contents of the) container, to monitor the personnel employed by the SC companies and the monitoring of the vehicles or vessels used to transport the containers. More information on technological possibilities can be found in Becker et al. (2005), also part of the research project PROTECT.

5.1 Monitoring of the (contents of the) container

In the previous chapter, already an important container monitoring technology was discussed. CISs are used by the SC companies to monitor the container throughout the logistic process. Different aspects of the container can be monitored like the integrity of the container (whether the container was transported incorruptibly), but also the interior of the container can be monitored. Examples of possible quantities that can be measured are humidity, light intensity and temperature. The sensor data is linked to an RFID chip that can communicate this data with an RFID reader infrastructure as discussed in section 4.4. The status of a container can only be read when the container is in proximity of an RFID reader (part of the RFID reader infrastructure). Required proximity varies with the RFID standard used but for 433 MHz active RFID chips, this is approximately 30 m [Interview 5 ScreenCheck (WP 5.2)]. The use of RFID in container transport is not common in practice mainly because of associated costs. However, the price of RFID is decreasing rapidly (especially for the low proximity and passive variants). Another important influence on the use of RFID technology is the commitment of regulatory authorities. If the use of RFID is somehow obligated by law, or advantages are offered, the use of RFID technology will increase significantly.

5.1.1 Real-time tracking

An important technological development that is not discussed previously is the real-time tracking of (the contents of) containers. This can be done using GPS and a communication infrastructure with extensive coverage. The mobile infrastructure used for telecommunication is an important network that can be used to transfer data about the container location to the actors in the SC that are interested in this information. This network mainly covers land and thus can be used to monitor the container when it is not in sea transport. Other technologies like satellite communication can be used to overcome this limited coverage. Recently a project has been announced [IBM, 2006a] that explores possibilities for real-time tracking of the container. In this project IBM, Safmarine, Heineken, the Vrije Universiteit Amsterdam and different Customs authorities cooperate to research possibilities in real-time tracking and distributed availability of data stores to meet the (security) information needs of the different actors. The solution, that is called Secure Trade Lane, is depicted in Figure 31. In this figure, a container is shown equipped with various sensors. During the entire transport, the controller (TREC unit in the figure) can communicate with the container information system to report the status of the different sensors connected to the controller.

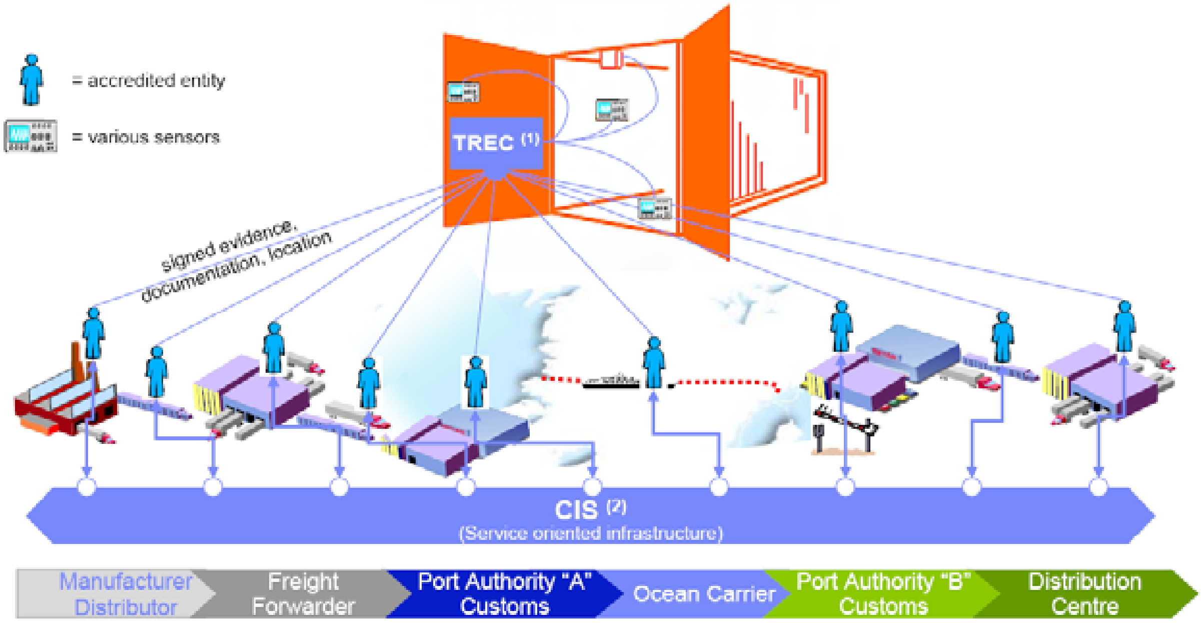
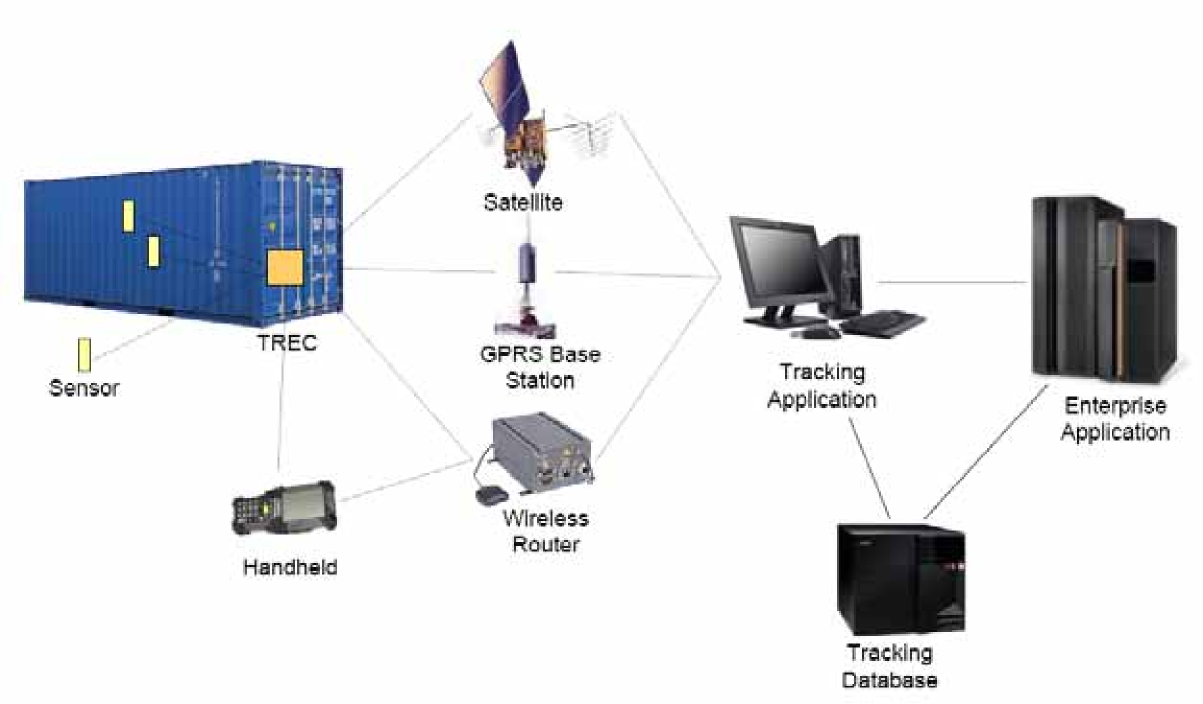

= accredited entity
= various sensors
TREC (1)
signed evidence, documentation, location
CIS (2)
(Service oriented infrastructure)
Manufacturer Distributor
Freight Forwarder
Port Authority "A" Customs
Ocean Carrier
Port Authority "B" Customs
Distribution Centre

Figure 31: IBM Secure Trade Lane [IBM, 2006b]

To achieve real-time tracking a global satellite communication network is used. The following figure illustrates the use of the different communication possibilities.



The TREC controller can communicate directly with a satellite network or can communicate with a wireless router if no direct communication with a satellite or GPRS base station is possible.

5.1.2 Scanning and inspection

For inspection and scanning purposes, many technological possibilities make the security measurers and the associated information exchange possible. Technological developments in the sensor equipment of nuclear radiation have made it feasible to scan containers for nuclear content without disrupting the logistic process. The same technological possibilities for low intensity X-ray scanning are under development. If it is possible to achieve 100% scanning of container contents, this will become an important part of the security relevant information about containers.

Taking into account the developments described above in the future ISA, is important because this ensures the future usefulness of the system.

5.2 Monitoring of personnel employed by the SC companies

Another important category that was identified in the information analysis presented in section 2.3 is information regarding the personnel employed by the operators in the SC (those employees that physically handle containers). Monitoring these employees and managing access rights is an important security measure that can help SCS. Currently in the terminal areas in the port of Rotterdam, biometric information is used to identify personnel. After identification, it is checked whether the employee is authorized to take the container. Achieving SC coverage with more advanced identification and authorization methods is a solution to attain increased SCS.

Managing access rights and advanced identification techniques are the main business of a company that was interviewed for this subject [Interview 5 ScreenCheck (WP 5.2)]. In the interview, it was identified that technologically already, a lot is possible but in practice, many companies are reluctant towards using these technologies. Real-time tracking of employees (using a RFID reader infrastructure) and managing access and authorization of employees centrally are two of the many possibilities already offered, but privacy issues and associated costs cause the low degree of acceptance of these technologies.

5.3 Monitoring of vehicles or vessels

Especially for reactive security measures, it is important to keep track of the containers and the vehicles or vessels transporting these containers. If, for example, it is found out that something is wrong with the container, the location of the container is important. If no real-time tracking of individual containers is possible, it may be possible to track the vehicles or vessels and link containers to these modalities in an information system in order to achieve container tracking. Monitoring of vehicles or vessels also helps when complete trucks are stolen. The monitoring of vehicles or vessels thus helps in reducing the threat (or effect) of theft and can help taking preventive measures for terrorist attacks and smuggling. This monitoring can again be done by GPS tracking (monitoring device) and satellite communication (communication infrastructure with extensive coverage).

5.4 Conclusion

In this chapter, an overview was given about different technological possibilities that have influence on the future state of an ISA. This introduces an extra uncertainty because the outcomes of technological developments are not defined up-front. Keeping the technological developments in mind in the development of an ISA is important to ensure the future usefulness of the ISA.

The technological developments are related to what type of information from the logistic layer is transferred to the transaction or oversight layer as defined in chapter 4 (p. 39). The different types of information are information about:

- The (contents of the) container;
- The personnel employed by the SC companies;
- The vehicles or vessels used to transport the container.

Most of the technological developments are present within the different ISAs discussed in chapter 4 and thus are taken into account in the information exchange between the SC actors. The remaining elements are kept in mind in the development of the ISAs for SCS within the scope of different scenarios discussed in chapter 6.

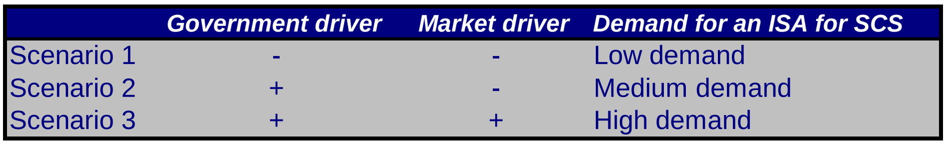
6 Scenarios for an ISA for supply chain security

In this chapter, three scenarios for exchanging security relevant information between the actors in the SC are introduced. These scenarios define the possible future market and government driver. This scenario approach is used because the future directions in SCS are uncertain. For these scenarios, far ends are used but a complete scale of future states exist between the defined scenarios. In the first section (6.1), the scenarios are introduced. The main discriminator between the scenarios is the degree of government and market driver. Thereafter (6.2), the scenarios are linked to the characteristics described in section 3.6. The characteristics that an ISA for SCS should satisfy are: flexible, easy to use, secure, acceptable, adaptable, scalable, cost efficient and maintainable. Third (6.3), three possible future scenarios are described in detail. This includes a short explanation of each scenario, the reasons behind the high or low market and government driver and the amount of information exchanged. After this, different ISAs are proposed that comply with the information needs and with the characteristics described in section 3.6.

6.1 Introduction

In order to develop an ISA for SCS scenarios are used. In these scenarios, possible futures are used as a starting point for analysis. The main differentiator for the scenarios is the extent of market driver and government driver for exchanging security relevant information. In section 2.2 the different actors active in the SC where described. In a scenario analysis, the SCS interests of the different SC companies are summarized in the market driver and the SCS interests of the different regulatory authorities are summarized in the government driver. This is to reduce the complexity of the problem, thus reducing the number of scenarios. If the demand for security relevant information from the government is high, it is assumed that the need for an ISA that supports this information exchange is also high. The same holds for the market driver with the difference that these market parties have a more direct influence on the ISA. This assumption is made while considering the high volume of information exchanges relating to SCS and the cost-consciousness of the SC actors.

Combining these two drivers leaves us with four possibilities (assumed that the market and government driver are high or low). Furthermore, it is assumed that when the government driver is low the market driver for exchanging and gathering of security relevant information is also low. This is resulting from research in work package 5.1 where interviews where conducted with SC companies. These organizations clearly considered rules and regulations as the primary driver for exchanging security relevant information. This leaves us with the following three scenarios.



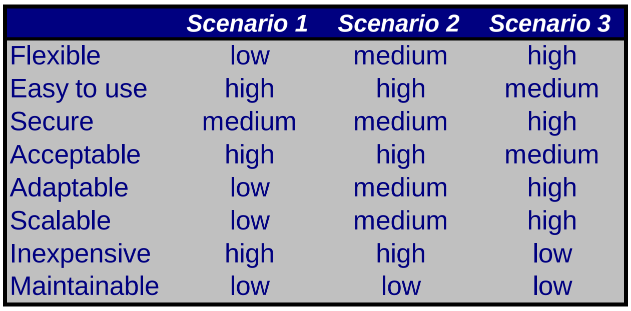
	Government driver	Market driver	Demand for an ISA for SCS
Scenario 1	-	-	Low demand
Scenario 2	+	-	Medium demand
Scenario 3	+	+	High demand

Figure 32: Scenarios

In these scenarios, the extreme ends are used in the analysis. Between the proposed scenarios, a scale of different scenarios of possible futures exists, but to decrease the complexity only these scenarios are considered.

6.2 Characteristics

In the scenarios, some characteristics (as described in section 3.6) are of more importance than others are. In the analysis of section 6.3, the focus is on the characteristics that have a high importance to the related scenario. A summary of the scorings is listed in Figure 33 and results from a brainstorm with experts in the field of SCS. A low or medium score does not mean the characteristic is irrelevant for the scenario, but it is left out to reduce the complexity of the problem.



	Scenario 1	Scenario 2	Scenario 3
Flexible	low	medium	high
Easy to use	high	high	medium
Secure	medium	medium	high
Acceptable	high	high	medium
Adaptable	low	medium	high
Scalable	low	medium	high
Inexpensive	high	high	low
Maintainable	low	low	low

Figure 33: Relevance of framework characteristics

Flexible: In scenario 1, flexibility of the ISA is of low importance. In this scenario, the demand for exchanging security relevant information is the smallest of all the scenarios, which means that not many actors have to communicate with each other. In scenario 3, the information needs are the most extensive which means a multitude of actors will have to communicate with each other. Consequently, all kinds of information systems have to be linked and many conversions have to be made. Furthermore, these information systems communicate using different protocols, which requires the ISA for SCS to be flexible in supporting those different protocols.

Easy to use: In both scenario 1 and scenario 2, the business driver is low. This means that the SC companies do not want to invest much money and effort in the exchange of security relevant information. The ease of use of the system is of more importance than the functionalities it offers. In the third scenario, the market driver behind exchanging security relevant information is high thus putting more focus on functionality. The ease of use still is considered medium, because many individual employees of the organizations will have to interact with the system. These employees want the system to be relatively easy to use in order for them to accept the technology.

Secure: The information security is considered of importance because of the competitive sensitive information and the fact that the information relevant for SCS can also cause security threats on its own. Although, the SC companies are in practice not keen on exchanging information securely. From the interview with Port infolink [Interview 1 Port infolink (WP 5.2)], it became clear that not all SC companies want to make a great effort in exchanging information with the proper security measures, even if these measures were supported by the PCS. In scenarios where the market driver is low, the information security is thus considered medium. If the ease at which information can be exchanged securely is improved, the demand for information security will increase.

Acceptable: To increase the effectiveness of the network it is important to have a high degree of coverage (see section 3.6.4). In the scenarios where the market driver is low, this is of extra importance because the market parties must be convinced to use the system in order for it to be effective. This is under the assumption of voluntary usage; if the use of a system is enforced by law, the system has to be accepted by the SC companies anyway. In the Netherlands a very supportive Customs is active [Interview 3 Dutch Customs (WP 5.2)] which means with a proposed information exchange the Customs takes into account the SC companies’ acceptance of the system. In the scenario where the market driver is high, the focus is less on the acceptance of the system because the market parties already have a high interest in the ISA for SCS. In the three scenarios, it is also assumed that the driver of the government does not have a high influence on the degree of acceptance of the system. The government has to use the existing or proposed system because of the national or international law and it can enforce government power to suite their needs.

Adaptable: The adaptability of the ISA is more important if information needs are high and if the information needs are subject to change in the future. Since currently not all information needs regarding SCS can be identified, the ISA should be adaptable, especially in the scenario where both market and government driver are high. In the scenario where both the market and government driver are low, the demand for an adaptable system is also low. In this case new information that has to be exchanged to support basic security needs can be added to the current information exchange, but new information exchanges are not probable because of the low driver of both groups of end users.

Scalable: In a setting where growth of usage is apparent, scalability of the system is very important. Because of the high interest in keeping the SC secure, the amount of information exchange can rapidly grow and the system should be able to keep track of the growing amount of container transports in real-time. This means the ISA being scalable with respect to: growing information needs, processing capability and with the growing number of transactions because of the increase of transport movements. The scalability in a scenario where the driver of both the market and the government are low can be considered low. This does not mean that the system should not be scalable, but the scalability only pertains to the expected increase of transactions due to growth of the container transport movements.

Cost efficient: In both scenarios where the market driver is low, there is the necessity for the ISA to be cost efficient because of the public support for security measures. The costs of gathering, exchanging and processing security relevant information should always be relative to the costs of the security threats (i.e. both social- and business relevant costs). In a scenario where both the market driver and the government driver are low, the social and business costs have to be low which enforces the constraint on the ISA to be cost efficient. When both drivers are high, the costs of gathering, exchanging and processing security relevant information can be higher because of the higher benefits related to the security measures. The second scenario lies in the middle.

Maintainable: The degree to which the maintainability of the system is important mainly depends of the complexity of the system. When the number of transactions and the versatility of information exchanges grow substantially, the complexity increases. This means that for scenario 3 – where the information needs are the largest – the maintainability of the system should be of higher importance. However, within all scenarios this aspect is considered of minor interest.

6.3 Description

In this section, the scenarios are further explained. With each scenario, the following aspects are discussed:

- First a description of the scenario is given;
- After this a description of the market and government driver is given with the reasons behind the degree of market or government driver;
- Finally, the amount and type of information exchanged between the SC actors is described.

6.3.1 Scenario 1

Description

In scenario 1 both the government and market driver are low which leaves a low demand for an ISA for SCS. In this scenario, organizations in the SC do not want to invest large amounts of money in gathering, exchanging and processing of security relevant information.

Market and government driver

Possible factors that have an influence on this low market and government driver are: (1) a low perceived value of information, (2) a decreasing threat of terrorist attacks, smuggling and theft and (3) unwillingness to share information because of the competitive sensitivity of information.

Amount of information exchanged

This does not mean that no new information is gathered and exchanged, but the so-called quick wins have precedence over information exchanges and gathering that require large investments and adaptation of the current ISA. Only a selective set of new information exchanges is added to the current information exchange between the SC actors, which represents only a small set of the security relevant information that can be exchanged. If this is related to the information needs represented in section 2.3, this means that the information that is considered important is exchanged in this scenario.

Table 2 in section 2.3 depicts the information elements that are considered important and is repeated here.

Table 6: Data elements scenario 1 adapted from Popal (2007)

Category	Data element	Means import	Means export	From	To
Container (general)	container number	Pre-arrival information	Pre-notification terminal visit (1) or pre-departure information (2)	Shipping line agent (1) or operator (2)	Customs (1) or inland terminal and sea terminal (2)
	container status	Pre-arrival information	Pre-notification terminal visit (1) or pre-departure information (2)		
		Nuclear scan	Nuclear scan	Customs	Customs
	scanned	Selection and control notifications	Selection and control notifications	Customs	Sea terminal and shipping line agent
	TARRA	Pre-arrival information	Pre-notification terminal visit (1) or pre-departure information (2)	Shipping line agent (1) or operator (2)	Customs (1) or inland terminal and sea terminal (2)
	container integrity	Physical check and/or RFID check	Physical check and/or RFID check	Container integrity system (in case of electronic seal) and multiple actors in case of physical check	Customs and shipper
Seal	seal number	Pre-arrival information	Pre-notification terminal visit (1) or pre-departure information (2)	Shipping line agent (1) or operator (2)	Customs (1) or inland terminal and sea terminal (2)
	location of sealing	Physical check and/or RFID check	Physical check and/or RFID check	Container integrity system (in case of electronic seal) and multiple actors in case of physical check	Customs and shipper
	time of sealing				
	sealed by				
	seal status / integrity				
Nuclear scan	location of scan	Nuclear scan	Nuclear scan	Customs	Customs
	results of scan	Nuclear scan	Nuclear scan	Customs	Customs
Scan / inspection (container contents)	container scan / inspection results	Selection and control notifications	Selection and control notifications	Customs	Sea terminal and shipping line agent
Operators (general)	operator ID	Pre-arrival information	Pre-notification terminal visit (1) or pre-departure information (2)	Shipping line agent (1) or operator (2)	Customs (1) or inland terminal and sea terminal (2)
	operator certificate details	Fixed in database	Fixed in database	Central organization for certificate information	Customs and shipper
Cargo	B/L number	Pre-arrival information	Pre-notification terminal visit (1) or pre-departure information (2)	Shipping line agent (1) or operator (2)	Customs (1) or inland terminal and sea terminal (2)
	cargo value				
	cargo weight				
	cargo description				
	cargo quality checked	Check selection & results	Check selection & results	VWA	Shipper and forwarder
	dangerous goods	Pre-arrival information	Pre-notification terminal visit (1) or pre-departure information (2)	Shipping line agent (1) or operator (2)	Customs (1) or inland terminal and sea terminal (2)
	container track history	B/L	B/L	several	several

These data elements come from different sources. The container number, for example, is contained within the pre-arrival information for import and in the pre-departure information for export (carrier haulage). In both cases, this information is transferred from the shipping line agent to the Customs. For each data element, the last two columns are depicted to show which SC organization supplies the information and which SC organization receives the information. The end-point of the data elements where the importance is considered high is often the Customs. This is because the market driver and government driver is low and the Customs gathers only basic information to guarantee public safety. Information to reduce theft in the container transport is considered less important.

Many data elements are already contained within the current message exchange, but some are not. Data elements that have to be added to the current information exchange are the container integrity, the location of sealing, the time of sealing and the operator certificate details. An ISA for SCS that fits these information needs and takes into account the scenario characteristics discussed in section 6.2 is discussed in section 6.4.

6.3.2 Scenario 2

Description

Scenario 2 represents the possible future where the government demand for security relevant information is high but where the SC companies do not have a high drive for exchanging this information. The information exchange between business and government is obligated by law and the SC companies thus exchange and gather this information as efficiently as possible. The need for information besides this obligated set of information is low and thus the exchange of security relevant information between the SC companies is low.

Market and government driver

In this scenario, the high government driver is caused by an increased threat and awareness of terrorist activities. Exchanging information that is relevant for reducing the risk of a terrorist attack has a high value. If a terrorist attack occurs, this has a large impact on the economy (both in infrastructure and in human life). The low market driver in this scenario is caused by the high costs associated with gathering and exchanging security relevant information. Additionally the perceived market value of the security relevant information is low because the SC companies are more interested in increasing the efficiency of the SC. This causes information exchanges that are relevant for both the security and efficiency of the SC to have high market acceptance, but information purely useful for SCS to have a low market acceptance.

Amount of information exchanged

The information needs in this scenario are more extensive than in the previous scenario. The needs are a more substantive subset of the security information that can be exchanged between the SC actors. This includes information that the regulatory authorities consider relevant for reducing the threat of a terrorist attack and that they consider the SC companies to be able to gather and exchange without disrupting SC operations. In an expert brainstorm, as part of the analysis in work package 5.1, the importance for the Customs and the importance for the SC organizations in general have been assessed. Each data element that is considered mandatory by the Customs or is considered important for the SC companies is a potential candidate for exchange in this scenario. This is a subset of the complete information analysis in work package 5.1 [Popal, 2007] and is summarized in the following table.

Table 7: Data elements scenario 2 adapted from Popal (2007)

Category	Data element
Container (general)	container number
	container status
	ISO code
	scanned
	gassing
	gas-description
	TARRA
	container integrity
Seal	seal number
	location of sealing
	time of sealing
	sealed by
	seal status/integrity
Nuclear scan	location of scan
	results of scan
X Ray scanning (container contents)	container scan type
	container scan location
	container scan results
	scanning details
Operators (general)	operator ID
	operator certified
	operator certificate details
Road operator	operator ID
	cargo card ID
	driver ID
Truck details	truck ID
	truck number plate
Truck driver details	driver ID
	driver status
Rail operator	operator
	train number
Train details	train ID/number
Barge operator	operator
	barge name / ID
Barge details	barge name / ID
Shipping line/ship details	operator
	ship name / ID
Personnel	personnel ID
	personal details
	organisation
	job/function/profession
	screening
	access rights
Point of stuffing (STUF) or point of stripping (STRIP)	cargo B/L
	STUF/STRIP sealing
	container number
	operator ID
Cargo	B/L number
	cargo value
	cargo weight
	cargo description
	cargo item
	cargo code
	cargo export certificate
	cargo health certificate
	cargo quality checked
	dangerous goods
	dangerous goods type
	country of origin
	country of departure
	consignor / shipper ID
	consignee ID
	container track history
Process information on timing STUF/STRIP	expected time STUF/STRIP
	actual time of departure from STUF/STRIP
Process information on timing inland terminal	ETA at inland terminal
	ATD from inland terminal
Process information on timing sea terminal	ETA at sea terminal
	ATD from sea terminal
Process information on timing container vessel	ETA of container vessel
Consignor (shipper)	consignor ID
	consignor details
	consignor certified
	type of certificate
Consignee (final recipient)	consignee ID
	consignee details
	certified
	type of certificate
Ports	port type
	port name
	port ID
	port city
	port country
	port security level
Sea terminal	terminal ID
	terminal description
	terminal security level
Incidents	incident ID
	incident type
	incident location
	operator ID
	management ID(s)
	CMP

6.3.3 Scenario 3

Description

In this scenario, information demands are extensive. The information for business to government is obligated by law and the market driver for B2B communication is high. This scenario is plausible if (especially) the risk of terrorist attacks and smuggling of materials that can be used in terrorist attacks increases and the international governments want to minimize this risk by taking extensive security measures.

Market and government driver

The government driver in this scenario is thus high because there is public support for investing in security measures. This high government driver is not only caused by the local drive for exchanging security relevant information but also by the international tendencies to secure supply chains. It has been identified in interviews in work package 5.1 that taking security measures that are not in line with international (or European) driver for SCS will make the local supply chains unnecessary expensive.

The market driver for exchanging and gathering security information is also high in this scenario because of the awareness and perceived usefulness of measures against terrorist attacks. Furthermore, the increased risk of smuggling and theft or the economic viability of measures to be taken causes the exchange of information to have a high market acceptance.

Amount of information exchanged

This means that a lot new information has to be gathered and many sources of information are used. The number of communication lines increases because not only information needed for SC operation is exchanged but information coming from new technologies (like RFID) is also used. In the most extreme case, it is possible that all information that is relevant for SCS is also exchanged between the SC actors. This leaves the set of possible data elements discussed in section 2.3.1. Even in the most extreme case, the ISA for SCS should be flexible in adding new data elements or information exchanges to support the growing need for SCS.

6.3.4 Scenario summary

The scenarios discussed in the previous sections are summarized in the following figure.

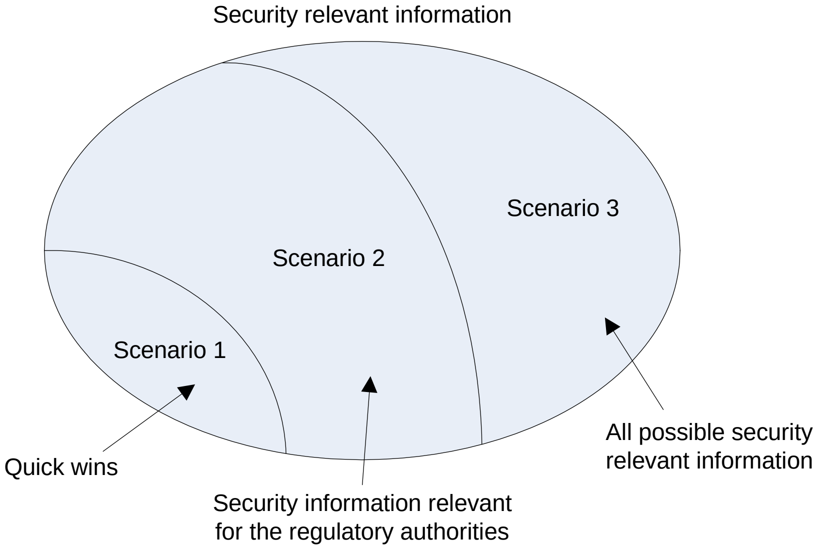

Security relevant information
Scenario 3
Scenario 2
Scenario 1
Quick wins
All possible security relevant information
Security information relevant for the regulatory authorities

Figure 34: Scenario summary

In this figure, the possible set of security relevant information is depicted by the ellipse. In scenario 1, only a small subset of the possible security relevant information is gathered and exchanged between the SC actors. This can be information already present at the individual SC actors but that is not exchanged yet, or it can be new information that has to be gathered but it needs to be collected with low costs.

Scenario 2 describes the possible future where the main driver for the exchange of security relevant information is the government. A larger subset of the possible information is gathered and exchanged (including the information exchanged in scenario 1). The information that is exchanged on top of scenario 1 is mainly the information that is considered useful for reducing the risk of terrorist attacks and smuggling by the regulatory authorities.

Finally, in scenario 3 all possible security relevant information is exchanged between the SC actors. This includes the information in scenario 1 and 2 but also adds information that the SC companies consider relevant for reducing the threats in the SC. Because the set of possible security relevant information exchanges is constrained by current thoughts about SCS and the technological possibilities, the ISA should be flexible in adding new information easily in case of changed information demands in the future.

6.4 Different architectures proposed

In section 3.1, different types of architectures were described that can be used to build an information system. A distinction was made between different client/server architectures where the main differentiator is the number of tiers used in the architecture. In section 3.2, the different types of information sharing models were described. Combining these two leads to the following high-level architectures for the ISA for SCS:

- ISA close to the current architecture; in this scenario government demands some new information to be added in the current messages already send to the regulatory authorities. This means that current messages and communication lines are used. For specific security information of interest to some high-end business parties, bilateral information exchanges are used;
- Central organization used for gathering and exchanging security relevant information (e.g. Port infolink). In this architecture, one central organization is used for exchanging security relevant information. Information needed is supplied by organizations to the central ISA. Authorized users (this can be the regulatory authorities or other SC companies) can access this information using some data retrieval service of the central organization or the information can be pushed to the receiving party in some format;
- Service oriented architecture where different organizations make available all kinds of information for other authorized users to access. Central organizations can be used to consolidate this information into one view (they do not store data) or the local IT systems of the organizations in the SC can be changed to incorporate this information in the local software.

In the remainder of this section, directions in the ISA for SCS within each scenario are outlined. Per scenario, it is shown what degree of coverage can be obtained by combining the different ISAs in the SC. In the information analysis described in section 2.3 it is assessed by domain experts where the required information currently resides (in which ISA as described in chapter 4). Besides the degree of coverage that can be obtained, an impression is given of a possible architecture to achieve this.

6.4.1 Scenario 1

In this scenario, already many of the data elements that need to be exchanged are now or in the future available within a PCS. The remaining data elements reside within CISs and can thus be linked to the PCS to obtain a higher degree of coverage. Table 8 summarizes the degree of coverage in width by combining different types of information systems. In this table, the following notation is used for the linking of different information systems. In the tables '||' means 'or', '&&' means 'and' and '!' means 'not'. 'PCS || CIS' can thus be read as: 'information that is available in the PCS or the CISs'.

Table 8: Degree of coverage scenario 1 (import and export)

PCS	Container Integrity System	Authority Systems (Customs, Port Authorities)	Business (Community) Systems	Electronic Availability	PCS || CIS	PCS || Authority Systems	PCS || CIS || Authority Systems
79%	39%	89%	21%	93%	89%	82%	93%

It can be seen that already 79% of the data elements is available in the PCS (in the future). CISs have 39% of the data available and by combining these two ISAs a degree of coverage of 89% can be obtained. In the last three columns, the percentages are shown for the combination of different information systems. It can be seen that by linking the PCS, the CISs and the authority systems a 93% degree of coverage can be obtained. The remaining 7% is not electronically available in the current ISA.

In section 6.2, characteristics where described that are especially important to the different scenarios. For scenario 1 the characteristics that where qualified as high are: “Easy to use”, “Acceptable” and “Cost efficient”.

As the ISA should satisfy the criteria easy to use, it should be as easy as possible for the SC actors to exchange security relevant information. This means that CISs must be linked using the PCS for the market parties with a low driver for SCS, but that the container integrity information also has to be made available to the more high-end companies using the BIM.

In order for the ISA to be acceptable, a high degree of coverage has to be reached. Both in the number of data elements covered as in the number of SC companies that support this information exchange. Having a link between a PCS and CISs is less useful when the degree of coverage of the CISs is low (e.g. if only 5% of containers use electronic seals also only 5% of the containers has the complete set of data elements required). To further increase the acceptance of the system, information that is currently only available in the authority systems has to be made available to the SC companies to give something back for the increased provision of data to the government.

The last characteristic of the ISA is that the system has to be cost efficient. The ISA does not have to change substantially which means low adaptation costs. Considerable costs are incurred by the usage of electronic seals and the associated information systems.

In the following figure, the link between the PCS, the CISs, the individual SC companies and the authorities is shown.

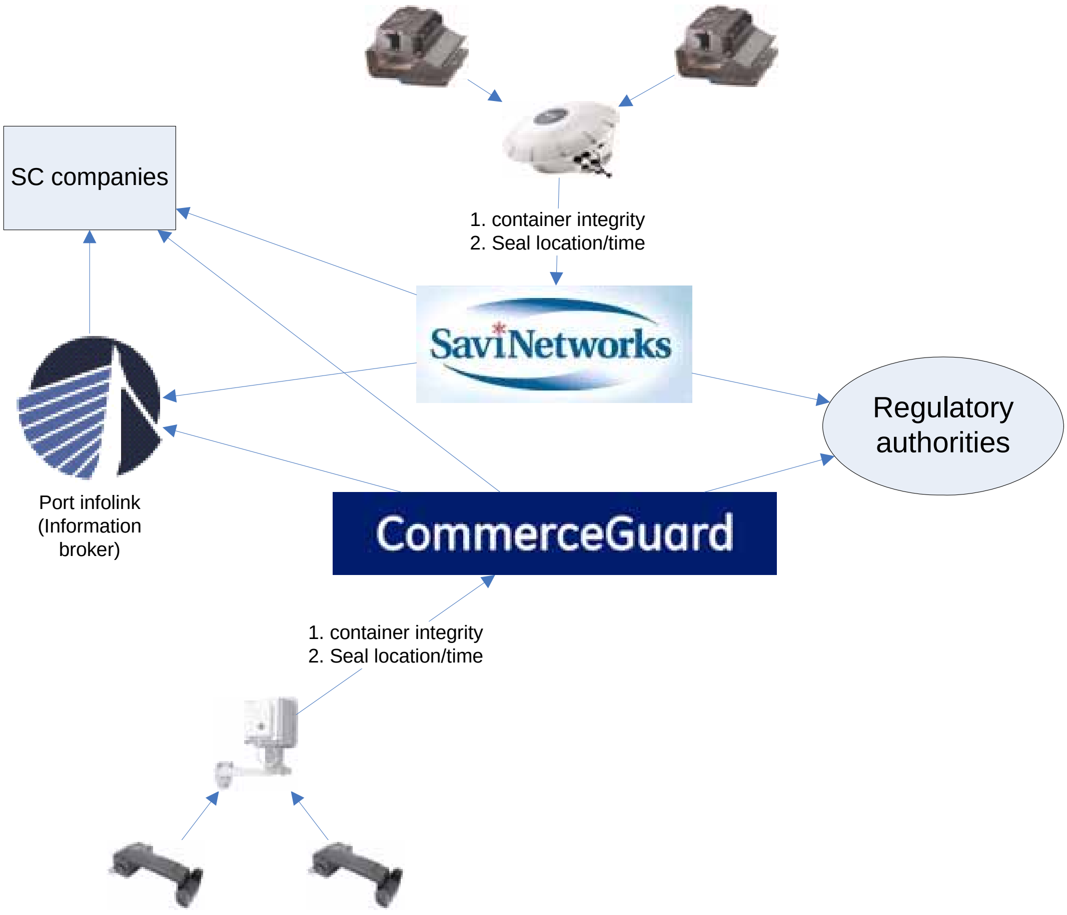


Figure 35: Linkage of CISs scenario 1

The CISs supply information on a bilateral basis to the local Customs. The local Customs on its turn makes relevant information available to the other Customs authorities in the EU. This means that the CISs have to make bilateral arrangements with each local authority. To the business community the CISs can be linked on a bilateral basis to each individual SC company (format is imposed by CISs) or they can be made available to the SC companies using the PCS. In the following diagram, the authority systems are linked to the PCS or SC companies.

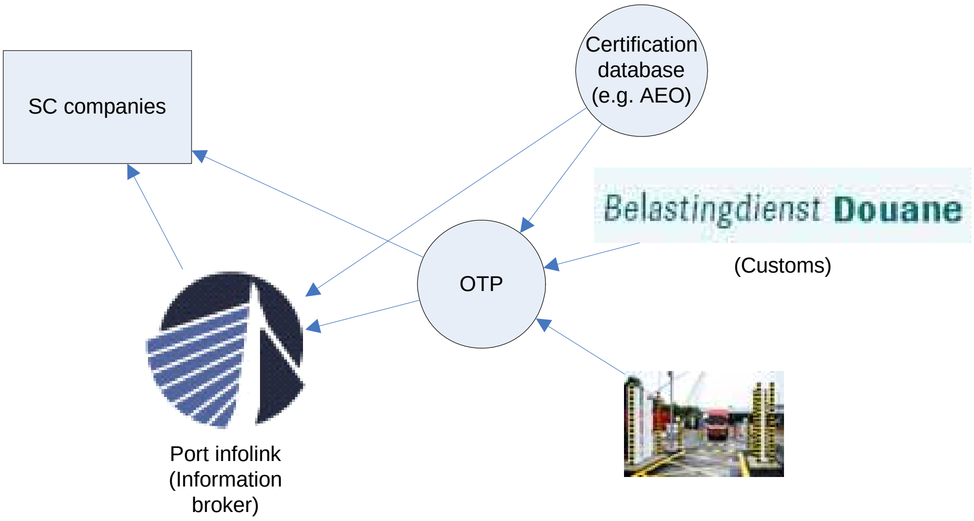

SC companies
Certification database (e.g. AEO)
Belastingdienst Douane
(Customs)
OTP
Port infolink (Information broker)

Figure 36: Linkage of authority systems to SC companies scenario 1

To give something back to the business community information from the authorities can be linked to the PCS or directly to the SC companies. This information includes information from the (future) certification authorities and information from the nuclear detecting infrastructure. As described in section 4.3 information going to the SC companies goes through the OTP. Adding the links between the information systems as described in this section ensures that a high degree of coverage is obtained for scenario 1. In the following section, the same analysis is conducted for scenario 2.

6.4.2 Scenario 2

In scenario 2, additional information on top of scenario 1 has to be gathered and exchanged between the SC actors because of the increased government driver. Also in this scenario, most of the data elements are already available in the different systems. The following table summarizes the degree of coverage in width of the individual systems and the degree of coverage in width that can be obtained by linking them[3]. On the left import is shown and on the right export is shown. The two only differ marginally because of the data element "ETA of container vessel" that is not available for export, but is available for import.

Table 9: Degree of coverage scenario 2 (import and export)

Import									Export								
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)
73%	11%	61%	43%	80%	76%	76%	79%	15%	72%	11%	61%	28%	79%	75%	75%	78%	15%

It can be seen that already 73% of the relevant data elements is available in the PCS (in the future). CISs have 11% of the data available and the authority systems have 61% of the data available. In the sixth, seventh and eighth column again the degree of coverage is shown that can be obtained by linking the different information systems. An extra column is added to show which information is available in the business (community) systems but is not available in the PCS, the CISs, or the authority systems. This information has to be opened up from the business (community) systems to some of the other systems to increase the degree of coverage of security relevant information. It can be difficult to make available this information and it is unclear how much of this information is electronically available. If the information is not electronically available, this information has to be automated or gathered by the SC companies.

In section 6.2, different characteristics where described that are especially important to the different scenarios. For scenario 2 the characteristics that where qualified high are: "Easy to use", "Acceptable" and "Cost efficient".

Just as in scenario 1, the linking of the CISs has to be done as easily as possible. The information again has to be linked to the SC companies on a bilateral basis or can be made available through the PCS for the less high-end SC companies. Because of the high government driver, the focus on centralization and standardization exists for the regulatory authorities in the EU. Especially for standardized information like the information from CISs, this means that logically information can be linked to the regulatory authorities on an EU level. In the EU, regulations can enforce the consistent handling of container integrity information to enable improved cooperation between the member states. The EU member states can exchange pointers to the correct information and the individual countries can use these pointers to access the right information from the CISs. To increase the degree of coverage

[3] Notation is described in section 6.4.1

information has to be opened up from the business (community) systems. An information broker like a PCS can play an important role in simplifying the information exchange between the SC companies and the regulatory authorities. B2B communication only marginally increases because of the low market driver. The extra information provision is thus primarily meant for the regulatory authorities.

The acceptance of the system is again of importance. The degree if coverage of the container integrity devices is again important for the overall coverage of the system. To improve the availability of information that is currently only contained within the business (community) systems, the provision of information must be obligated by law or the regulatory authorities have to return something to the SC companies. This can be reduced lead-times or extra information availability to the SC companies.

Finally, the ISA for SCS has to be cost efficient. This again is realized by low adaptation costs and the return of something by the regulatory authorities to compensate for the incurred cost for making the extra information available.

In the following figure, the link between the PCS, the CISs, the individual SC companies and the authorities is shown.

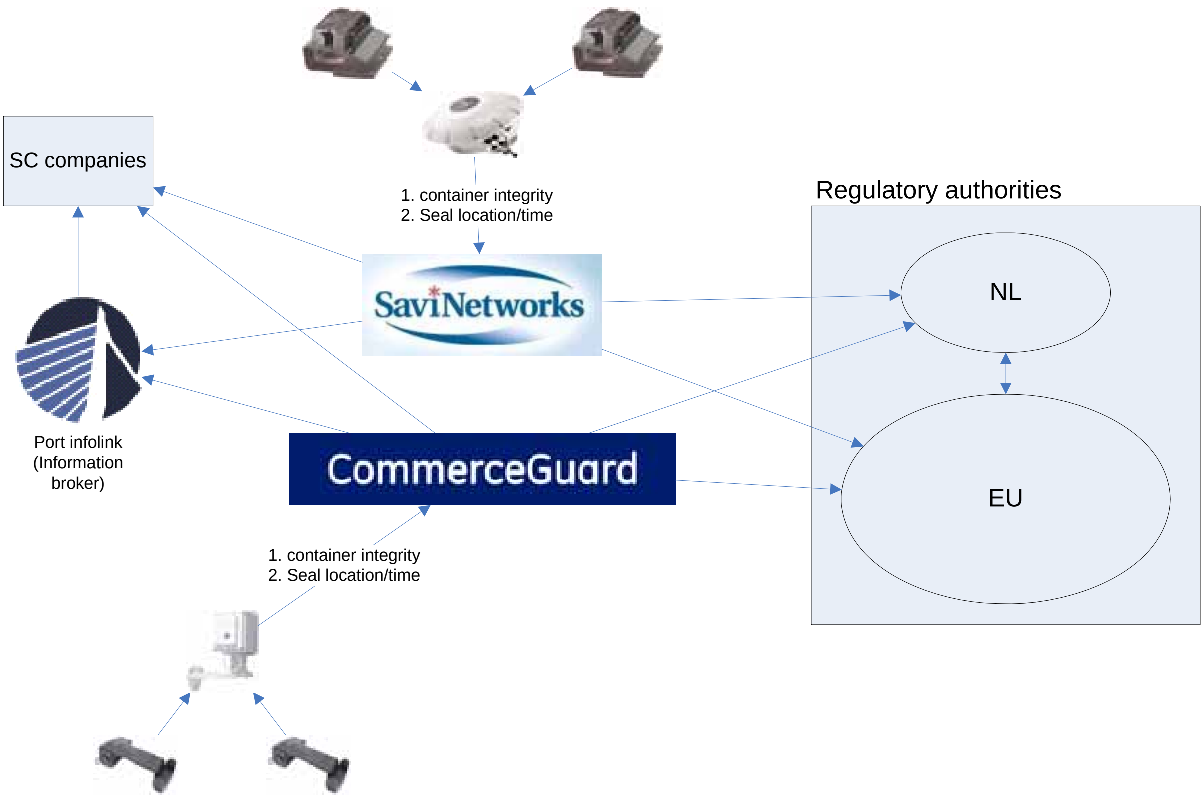


Figure 37: Linkage of CISs scenario 2

The CISs supply information on a bilateral basis to the local Customs. The local Customs on its turn makes available pointer information to the other Customs authorities in the EU in order for the foreign Customs to find the relevant information within the appropriate CIS. This still means that the CISs have to make bilateral arrangements with each local authority, although message exchange can be standardized. To the business community the CISs can be linked on a bilateral basis to each individual SC company (format is imposed by CISs) or can be made available to the SC companies using the PCS. For the linkage of the authority systems to the SC companies, the same approach can be taken as in scenario 1. Some initiatives can be transferred to the EU and thus be linked at EU level.

The approach to increase the information provision from the SC companies to the regulatory authorities is more complex. Because many parties are involved, numerous communication links exist. It was shown in section 3.3 that when many senders (the SC companies) have to supply information to several receivers (the regulatory authorities) the CIM is more appropriate than the BIM. The central party in the form of an information broker can take care of the message aggregation, conversion and relay. In the port of Rotterdam this is often done by the PCS of Port infolink and it is thus plausible that extra information is supplied using this system. For the Customs, for example, no distinction is made between SC companies that supply the information directly or via the PCS. Both the BIM and the CIM will exist next to each other in the future. In the following figure, an example of a completely centralized solution is shown.

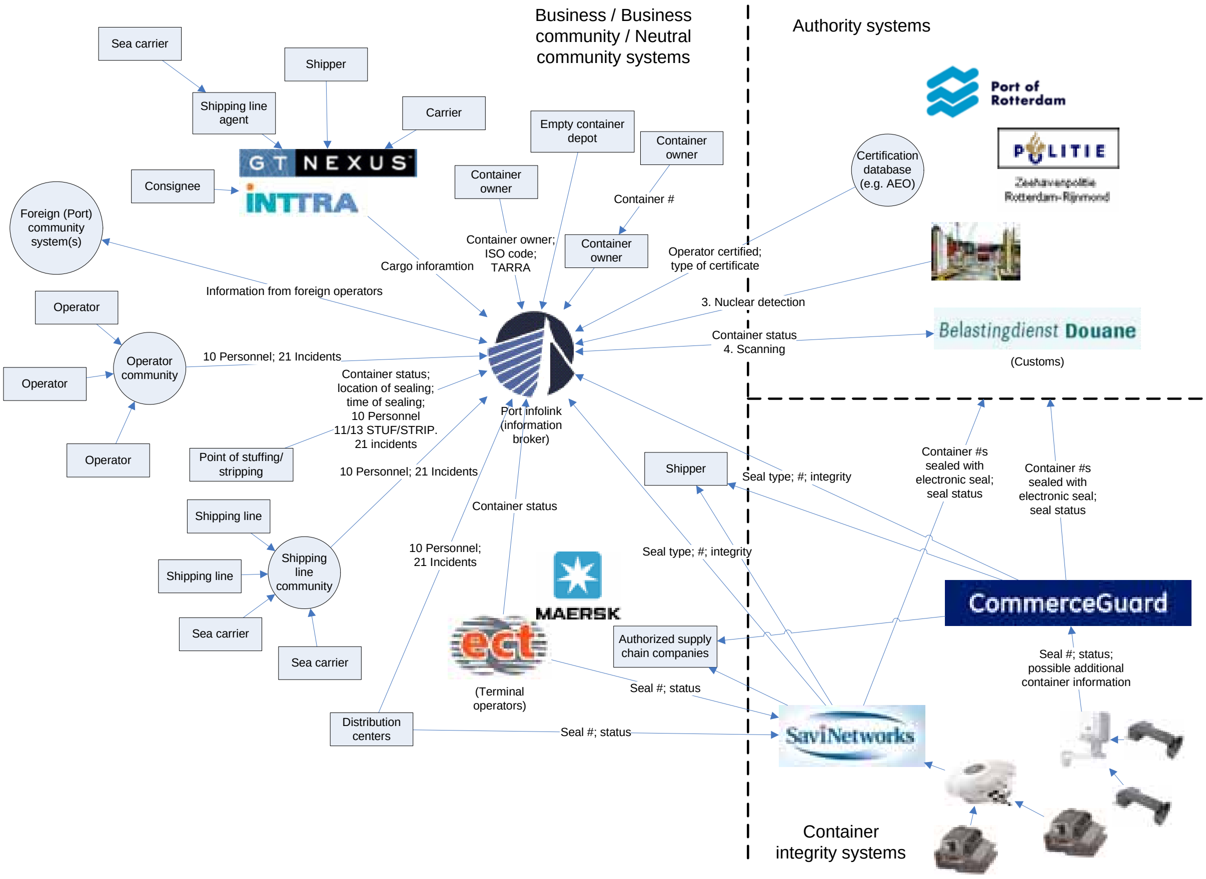

Business / Business community / Neutral community systems
Authority systems
Sea carrier
Shipper
Shipping line agent
Carrier
Empty container depot
Container owner
Consignee
GT NEXUS
INTTRA
Container owner
Foreign (Port) community system(s)
Container #
Certification database (e.g. AEO)
Port of Rotterdam
POLITIE
Zeehavenpolitie Rotterdam-Rijnmond
Container owner; ISO code; TARRA
Container owner
Operator certified; type of certificate
Cargo inforamtion
Information from foreign operators
Operator
3. Nuclear detection
Container status
4. Scanning
Belastingdienst Douane
(Customs)
Operator community
Operator
10 Personnel; 21 Incidents
Container status; location of sealing; time of sealing; 10 Personnel 11/13 STUF/STRIP. 21 incidents
Port infolink (information broker)
Operator
Point of stuffing/ stripping
10 Personnel; 21 Incidents
Shipper
Seal type; #; integrity
Container #s sealed with electronic seal; seal status
Container #s sealed with electronic seal; seal status
Shipping line
Container status
Shipping line
Shipping line community
10 Personnel; 21 Incidents
Seal type; #; integrity
MAERSK
CommerceGuard
Sea carrier
Sea carrier
ect
Authorized supply chain companies
Seal #; status; possible additional container information
(Terminal operators)
Seal #; status
Distribution centers
Seal #; status
SaviNetworks
Container integrity systems

Figure 38: Linkage of business (community) systems scenario 2

In Figure 38, an ISA for scenario 2 is shown. In the top right corner, the different authority systems are depicted. Customs is an important receiver and supplier of data. It sends information about the container status and the scan results to the SC companies. This information is made available and can be incorporated in the centralized information broker system. The SC companies make available security relevant information through the information broker. This information includes personnel information and information about incidents. In the figure, all data elements are considered that were defined as relevant in section 6.3.2 except the data elements that are already available in the PCS. In the next section the final scenario is discussed where the information needs are the most extensive.

6.4.3 Scenario 3

This is the scenario where both the market and government driver are high. In this scenario, 175 data elements should be accessible by the different actors in the SC. Of these elements only about 60% is (in the near future) available in the PCS. These 175 elements correspond to the complete set of data elements identified as security relevant in section 2.3.1. Table 10, summarizes the data availability in the different systems.

Table 10: Degree of coverage scenario 3

Import								
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%	10%	55%	44%	76%	69%	69%	71%	20%

Export								
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%	10%	55%	32%	76%	69%	69%	71%	20%

In the sixth, seventh and eighth column again the degree of coverage is shown that can be attained by linking the different information systems. The notation used is described in section 6.4.1. By linking the three major information systems, only a degree of coverage can be attained of 71%. Of the remaining 29% most of the information resides in business (community) systems or is not electronically available.

In section 6.2 four characteristics were defined that are of high importance to this scenario. The characteristics are “Flexible”, “Secure”, “Adaptable” and “Scalable”. Defining an ISA that satisfies these characteristics and is viable in practice is difficult. There are opposing forces that pull the ISA in different directions.

For the flexibility of the system, it is important that different protocols, message formats and data retrieval services exist. On the other hand, standardization is important to reduce the complexity of the system in a setting where both the number of data elements and the number of messages increases. Information brokers have an important role in this respect and it is to be expected that cooperation between information brokers will increase.

For the information security of the ISA, it is important that the CIA criteria as described in section 3.6.3 are met. Designing a completely distributed ISA requires, for example, that the different SC companies have to guarantee a certain degree of information availability in order for the Customs to be able to do their job. The feasibility of this is questionable considering the high amount of actors involved.

Making sure the ISA is adaptable is another characteristic that is considered important in this scenario. Even in the scenario where the information requirements are the most extensive, the number of data elements exchanged can increase because of future needs. Also because of the path towards the new ISA, the system should be adaptable. Not al future information requirements can be implemented at once. Adapting the ISA several times may be necessary.

Finally, the ISA needs to be scalable. Making sure the ISA is scalable does not only require the technical infrastructure to be scalable, but also the functions that are performed with the ISA. The Customs, for example, has to cope with a continuously increasing amount of data (more data elements and more transactions). The ISA has to support the increased data availability, but taking into account limited recourses available at the Customs to scan containers and to make a risk analysis.

To realize an ISA that satisfies all four characteristics, a mixture of e-collaboration models is needed. Because of the large amount of information available and the increased amount of communication lines, the complexity is large. According to the Dutch Customs [Interview 3 Dutch Customs (WP 5.2)] in light of certification the drive exists to reduce the number of data elements on declarations. This means that certified organizations only have to supply a reduced set of data elements at fixed times and have to make available the remaining data elements. This is a combination between the DIM and the BIM or CIM. Part of the information requirement is shared between the actors in the SC on a bilateral basis or via a central organization like the PCS, but the remaining data elements are made available distributed throughout the network. An example of a distributed structure is shown in the following diagram.

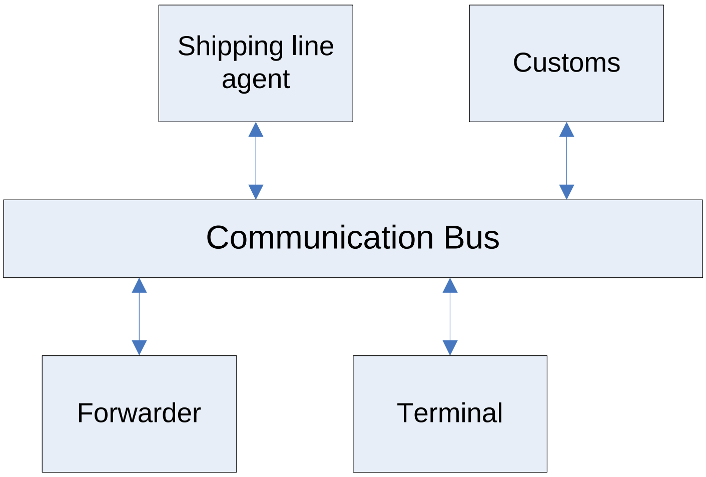


Figure 39: Distributed architecture scenario 3

Besides the central and bilateral communication between the SC companies and the regulatory authorities as shown in Figure 36 and Figure 38, information can be exchanged using the DIM. This has the advantage that information is only stored at the owner of the data and that when information is collected, this information is most up-to-date. For the Customs, this has the advantage that not a very large set of data has to be analyzed, but that extra information can be gathered if the reduced declaration gives reason for a more detailed analysis. The downside of this architecture is that every party that makes available information in this distributed architecture has to guarantee a certain degree of information availability in order for the Customs to be able to do their job.

From the business point of view, a distributed architecture has several advantages. Because the business value of security relevant information is high in this scenario, the protection of this information from competitors is more important. In a distributed setting, access rights to the information can be managed locally. If a company derives competitive advantage from dealing with security relevant information more stringently, this company wants to have the information into their own hands. From different interviews, it was derived that several SC companies already are dealing with this problem. They have questions about the information security inside the systems of information brokers although most of these information brokers appoint independent parties to assess the information security in the system. Another advantage of a DIM is that communication lines can be created between organizations that now do not communicate directly. Finally, the advantage of the DIM is that the dependence on the third party is taken out of the equation.

6.5 Conclusion

In this chapter, three scenarios were introduced defining the possible future market and government driver. This scenario approach is used because the future directions in SCS are uncertain. For these scenarios, far ends are used but a complete scale of future states exist between the defined scenarios.

In the first scenario, both the market and government driver are low which caused the demand for an ISA for SCS to be low. This does not mean that no extra information is exchanged between the SC organizations, but there is only an exchange of the important data elements. In expert sessions and individual session with specialists, the importance of the different data elements was assessed. This meant for scenario 1 that only some information that is considered relevant, is not currently available in the PCS. A high degree of coverage can be reached by coupling the different information systems. Important new information elements that have to be added are the operator certificate details (from the authority systems) and container integrity information (from the CISs). Both systems can be linked to the SC companies using the BIM or CIM. In practice, both architectures will exist in parallel. For the linkage of the CISs to the regulatory authorities, local arrangements have to be made. This means the BIM is used between the CISs and the authority systems.

In scenario 2, the government driver is assumed high. This causes the information requirement from especially the Customs to increase significantly. This extra information requirement increases the demand for an ISA for SCS. It was shown that by linking the PCS, the CISs and the authority systems a complete coverage could not be reached. In this scenario, SC companies have to gather or make available extra information to meet the increased information needs. The regulatory authorities can enforce the SC companies to supply this information or can give something in return for this information. This can be reduced lead-times in the logistic process or extra information provision from the government to the SC companies. In this scenario, the communication between the SC companies and the government can again be done using the BIM and the CIM. Because several new data elements have to be made available by the SC companies, information brokers can help in this by offering information aggregation, conversion and relay in order to supply the necessary information to the regulatory authorities.

Finally, in scenario 3, both the government and market driver are considered high. The number of data elements required is even more extensive and a larger part of the information is currently only available within the business (community) systems. Some of the information is currently not electronically available and has to be gathered by the SC companies. Because of the increased value of SCS relevant information, this information can be more business sensitive. In a distributed setting access rights to data can be managed locally which improves the confidence in information security. Also because of the growth of container transport and the increased amount of data elements exchanged between the SC companies and the regulatory authorities, a drive exists for decentralized availability of data. This enables the Customs, for example, to check only a reduced set of data elements and retrieve only the extra data elements if they are necessary for further analysis. This is most relevant for the certified and more high-end SC companies. In this scenario, the three information models described are all used in parallel.

7 Validation

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 G. These people represent expert opinions from three of the four major information systems that were examined in this research. Experts from CISs, the PCS of the port of Rotterdam and the authority systems of the Dutch Customs participated in this workshop.

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.

7.1 Work package 5.1

During the validation of work package 5.1, the information analysis as presented in section 2.3 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 and whether data elements were mandatory or preferable. Because this is of great importance to the scenario analysis described in the previous chapter of this thesis it was discussed to plan extra individual expert sessions to further improve or validate (in the case the assessments were correct in the first place) the valuation of the different data elements. The extra expert sessions are still in progress when writing this thesis. Because of time constraints, it was not possible to await further outcomes of these extra sessions. However, methodology described ensures that when these extra sessions are finished the implications for work package 5.2 can be assessed.

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 Popal (2007), it is best to look at all modalities with equal concern.

7.2 Work package 5.2

The second part of the session was used for the validation of the research presented in this thesis. Because of the fact that various experts from different domains were present at the validation workshop the second part was introduced with the presentation of results. The scenario approach was introduced and the directions of the ISA for SCS for each of the scenarios were discussed.

It was difficult to discuss all of the results for each of the scenarios because of the limited amount of time available. Participants of the workshop were asked to assess the feasibility of recommendations for development of the ISA for SCS in each of the scenarios.

7.2.1 Scenario 1

For scenario 1, the main points of discussion were the amount of data exchanged and the degree of coverage that can be reached by combining the different information systems. The amount of information exchanged was called into question because of two reasons. First, the scenario represents a possible future where some extra security relevant information is exchanged, but where the market and government driver are low. What are the forces that solicit this exchange of information?

The scenario represents a possible future where the drive for future security relevant information is low. Current information needs that result from the high valuation (the important data elements) of different SC actors are considered to be in the current development of the ISA and are thus exchanged in the (near) future. Adapting the ISA to take into account these requirements is necessary for the ISA to be useful in the future.

An additional point of discussion was the degree of coverage that could be reached by linking the different information systems. As described in section 6.4.1, a degree of coverage could be reached of 93%. In this calculation, the different data elements are valuated equally and planned information availability is already taken into account in the information exchange. The certainty that this scenario is reached is not 100% and maybe it is already a large step for the near future. The feasibility in a practical setting was not assessed because of time constraints. Ideally, the ISA for SCS for scenario 1 should be demonstrated to enable a full validation of the outcomes of the research presented here. Developing this proof-of-concept is considered an important next step in the research in the PROTECT project.

7.2.2 Scenario 2

In this scenario, the government driver was considered high. For this scenario, the main point of discussion was the choice of data elements exchanged and required by the regulatory authorities. The reaction of the experts present from the authority systems was that it first has to be assessed exactly which data elements are important and how difficult it actually is to gather these data elements. This again is grounds for the extra individual expert sessions for work package 5.1, where the user requirements are identified.

Another point of conversation, which was also discussed in section 6.4.1, was the degree of coverage of the individual information systems that are to be linked. By linking the different information systems, not automatically a higher degree of coverage can be reached. If, for example, the degree of coverage of CISs is only a few percent, an increased coverage of security relevant information is only obtained for these few percent of containers by linking the CISs to the PCS. The same holds for operator certificate information made available by the regulatory authorities. If only a few high-end operators are certified information contained within the different information systems is complete, but the security in the supply chain is only marginally improved.

7.2.3 Scenario 3

Scenario 3 represents the possible future where both the market and government driver are high. This scenario was the most difficult to validate because the proposed ISA for SCS differs the most from the current state of the ISA. Both the expert from CommerceGuard and the experts from the authority systems identified that distributed availability of information is a clear development present in the exchange of (security) information between the SC actors. Whether this is a development for all actors active in the SC for container transport is questionable, but no explicit remarks were made concerning the validity of the choices made in this scenario.

7.3 Conclusion

Doing a complete validation is difficult without testing the different scenarios in practice. For further research, it would be relevant to develop an ISA within a specific case to demonstrate the possibilities of improved information exchange. The main problem identified was the importance of the different data elements. For this problem, extra expert sessions are planned, but these have not finished before the completion of this thesis. As an extra validation step, it is important to reassess the outcomes of this thesis when these sessions have completed.

8 Conclusions and recommendations

Given the increased interest in the security of the SC and the growing number of container transport movements, information exchanges about the (security of the) container are becoming more and more important. An ISA that supports the growing need for security relevant information is therefore warranted. In section 8.1, the main outcomes of the research are presented. From these outcomes, recommendations for the development of an ISA for SCS are formulated in section 8.2. Finally, directions for further research are identified in section 8.3.

8.1 Conclusions

The objective of this thesis was formulated as follows: *"To provide recommendations to extend the current information system architecture in order to improve supply chain security"*. These recommendations were further specified within three scenarios for the path towards possible future states of market and government driver. This approach was used because the future information needs of the actors in the SC are uncertain. To come to these recommendations five research questions were defined that should be answered before the recommendations can be formulated. The research questions are discussed one by one in the remainder of this section.

What are the (future) information needs from the actors in the supply chain?

This research question was addressed in work package 5.1 of the same research project and outcomes are presented in section 2.3. The (future) information needs of the actors in the SC were assessed using interviews and an expert brainstorm approach. These information needs form the basis for the ISAs for SCS discussed in chapter 6. Because the future information needs are uncertain, the information analysis not only identified what information was possibly security relevant, but also tried to assess the importance of the different data elements. This analysis is still in progress at the moment of writing this thesis. Preliminary (but already extensive) results from Popal (2007) were used in research conducted in this thesis.

What is the current state of the information system architecture for supply chain security?

To answer this question, different groups of ISAs were identified and analyzed. The main types of systems are:

- Neutral or open community systems;
- Authority systems;
- Container integrity systems;
- Business (community) systems.

In the first type of information system, SC companies come together to exchange (security relevant) information. Communication between different SC companies is often on a bilateral basis and neutral community systems are often designed using the CIM. Community systems act as an information broker and fulfill the following functions: information aggregation, conversion and relay. In the port of Rotterdam, the PCS of Port infolink is used to exchange information between the SC companies themselves or between the SC companies and the regulatory authorities. This system adds value to the business parties enabling them to exchange information more efficiently. On top of the information broker functions, Port infolink offers extra services like management information, security profiles and alerts.

The second category consists of systems used by the regulatory authorities. In the authority systems much information resides that can be considered security relevant. Parts of this information are shared between the different regulatory authorities but are not made available to the SC companies. When the regulatory authorities do communicate with the SC companies, this is often on a bilateral basis.

The third type of information systems discussed are the CISs including CommerceGuard and Savi Networks. These systems supply information about the integrity of the container during transport. They do this by using a RFID reader infrastructure that communicates with devices attached to the container to check the integrity of the container. For the CISs, fully centralized systems are used and customers of the CISs can access the information using a website. This means a fully standardized BIM is used.

The final type of information systems discussed are the business community systems. These systems are used by the SC companies to exchange information primarily meant for SC operation. The difference with neutral or open community systems is that SC companies can be excluded from participation in the community.

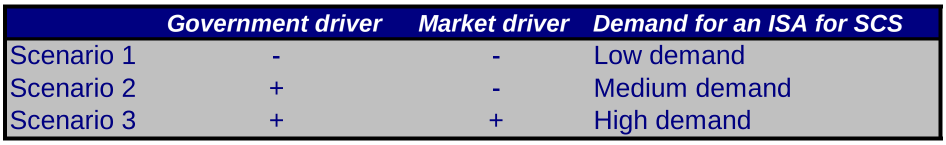
What relevant technological or architectural developments can be recognized with regard to supply chain security?

Parts of this research question were already addressed in the discussion about the current state and development of the ISA. CISs, for example, use technological developments like RFID technology and scanning equipment inside the container to offer information to the customer of the CIS. Technological developments also lie at the basis of many of the systems used by regulatory authorities. Nuclear scanning, for example, is made possible by technology. This technology is combined with an ISA in a nuclear detection infrastructure to improve SCS.

Technological developments that are not discussed as part of an ISA are the real-time tracking of container (contents) and the real-time tracking of personnel. These technological developments have possible security value and it is therefore useful to take into account the information that may be integrated in the ISA in a later stage.

What are possible recommendations to extend the current information system architecture with supply chain security relevant information in the scope of different future scenarios?

The user requirements, the current state and developments of the ISA for SCS and the technological developments all have influence on a future state of the ISA for SCS. In chapter 6, recommendations for an ISA were derived under the assumption of different future scenarios for the user requirements. The user requirements were linked to the degree of market and government driver that could be high or low. A scenario where the market driver was high, but the government driver was low, was not considered relevant because from interviews it was derived that currently an important driver for gathering and exchanging security relevant information is the government. This left the following three scenarios.



	Government driver	Market driver	Demand for an ISA for SCS
Scenario 1	-	-	Low demand
Scenario 2	+	-	Medium demand
Scenario 3	+	+	High demand

Figure 40: Scenarios

Recommendations for these scenarios are discussed in the following section.

8.2 Recommendations for the development of an ISA for SCS

In the first scenario, only the important data elements are exchanged. For the ISA, this means that only some information that is considered relevant, is not currently available in the PCS. A high degree of coverage can be reached by coupling the different types of information systems. Important new information elements that have to be added are the operator certificate details (from the authority systems) and container integrity information (from the CISs). Both systems have to be linked to the SC companies using the BIM or CIM. For the linkage of the CISs to the regulatory authorities, local arrangements have to be made. This means the BIM is used between the CISs and the authority systems. For the development of the ISA for SCS, this means that by extending the PCS (where already a lot of security relevant information is available) with links to other types of systems, a high degree of coverage can be reached.

In scenario 2, the information requirement from especially the Customs causes the overall information requirement to increase significantly. It is shown that by linking the PCS, the CISs and the authority systems not a complete coverage can be reached. In this scenario, SC companies have to gather or make available extra information to meet the increased information needs. The regulatory authorities can enforce the SC companies to supply this information or can give something in return for this information. This can be reduced lead-times in the logistic process or extra information provision from the government to the SC companies. The focus thus should be on SC efficiency and SCS should be derived from SC efficiency. This ensures a larger drive from the SC companies to comply with extended information needs from the regulatory authorities. In this scenario, the communication between the SC companies and the government can again be done using the BIM and the CIM. Because several new data elements have to be made available by the SC companies, information brokers can help in this by offering information aggregation, conversion and relay in order to supply the necessary information to the regulatory authorities. For the development of the ISA, this means that information brokers have a key role. Anticipating the information needs and the associated functions offered by the information brokers (message aggregation, conversion and relay) will determine the success of the ISA and the companies offering the ISA.

Finally, in scenario 3, both the number of data elements required is even more extensive and a larger part of the information is currently only available within the business (community) systems. Some of the information is currently not electronically available and has to be gathered by the SC companies. Because of the increased value of SCS relevant information, this information can be more business sensitive. In a distributed setting access rights to data can be managed locally which improves the confidence in information security. Also because of the growth developments of container transport and the increased amount of data elements exchanged between the SC companies and the regulatory authorities, a drive exists for decentralized availability of data. This enables the Customs, for example, to check only a reduced set of data elements and retrieve only the extra data elements if they are necessary for further analysis. This is most relevant for the certified and more high-end SC companies. In this scenario, the three information models described are all used in parallel. For the development of the ISA, this means that the role of information brokers becomes less important and that these companies thus have to focus on niche markets. The smaller SC companies are more likely to use information brokers because of the costs of implementing a new information system and setting-up the required communication lines with the different SC actors.

8.3 Recommendations for further research

The most obvious opportunity for further research is the development of an ISA (demonstration) that can validate the research findings in practice. For this, a specific threat in the logistic process can be chosen where information must come together from different sources to take adequate security measures. In this respect, the linking of the PCS, the authority systems and a CIS seams logical. A situation similar to scenario 1 can be developed in this demonstration ISA.

An example of a possible case can be that a container arrives from another EU country to the port of Rotterdam. This container is selected for a second line scan after the container is found positive for emitting high radiation levels (authority systems). In the foreign port, the container was not nuclear scanned. In the second line scan, the container is physically inspected and it is observed that the seal was tampered with. From the inspection, it also follows that the container does not contain any nuclear materials. When comparing the manifest information to the checks of sealing (CISs and terminal systems) it is found out that, one container was not properly sealed when entering the port of Rotterdam. No physical check was conducted. The container is said to contain materials that can camouflage certain small amounts of radiation (PCS/authority systems). The container can be blocked for further import and is inspected. This example shows that by linking different information systems the SC can be made more secure.

Especially for scenario 2 where the market driver is low, further analysis is needed to identify the conditions under which SC companies are (more) willing to share information. Supply of information by the SC companies can be attained by giving something back. It is useful to identify the business value of certain advantages the regulatory authorities can offer.

It would also be interesting to make a cost/benefit analysis for the security measures and information gathering and exchange proposed in research presented in this thesis and in Popal (2007). Doing a cost/benefit analysis enables the improved judgment of the relevance of security measures besides the expert opinions used in this stage of the research. The cost/benefit analysis can be conducted on two areas: (1) opening up of data elements within the different scenarios and (2) security benefits versus collateral benefits. The second area is closely related to the business value that can be offered by the regulatory authorities described in the previous paragraph.

To extend the information analysis and the proposed ISAs further, a specific analysis on SC actor level is required. This includes the data availability of the different actors and under which conditions they want to share this information. With this, rules and regulations play an important role (e.g. privacy regulations). This mainly concerns information that is available in business (community) systems because this was not extensively studied in the information analysis and in this thesis. Also for future information needs and exchanges, it is useful to identify which actor can gather and make available this information most efficiently. This has influence on the degree of coverage in both width and depth that can be attained by coupling different information systems. A more specific analysis on the degree of coverage in depth of the different data elements is required to assess the degree of coverage (both width and depth) of the overall ISA more exactly.

Risk analysis conducted by the Customs is an important security measure that requires numerous data elements. An improvement of data-mining techniques can cause the overall information need to increase (more information is better), but within Customs also the drive exists to reduce the declarations because of the growth of container transport movements and the reduced availability of resources to conduct the risk analysis. Taking into account the drive within the different regulatory authorities for data mining techniques is important for the future usefulness of the ISA.

Additionally, research can be performed to assess another approach in container transport then the current B2G communication in the form of declarations. In the case of Cargonaut, the Customs can monitor all B2B communication within the ISA. This can increase the security of the SC for container transport further. Timing is of less importance, but if lead-times are reduces further timing of information becomes more and more important. Exploring the possibility of monitoring of B2B communication by the regulatory authorities is an interesting direction for further research.

Finally, it is important to look at further possibilities of redesign of the ISA. Possibilities of designing a single window for security relevant information or the design of an ISA more based on the DIM are two important directions that can be explored.

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]

B. Appendix: Carriage of goods

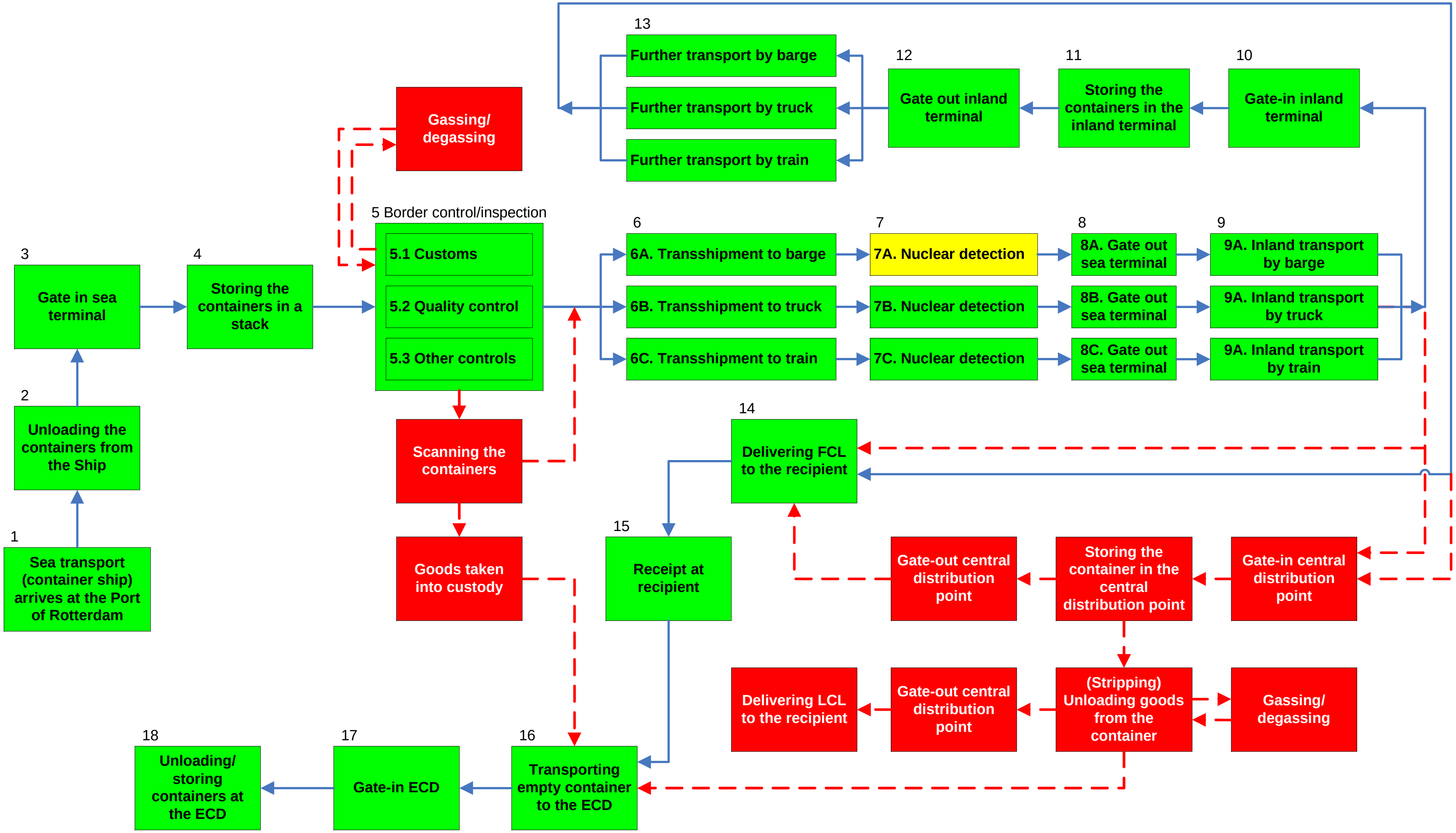

13
Further transport by barge
Further transport by truck
Further transport by train
12
Gate out inland terminal
11
Storing the containers in the inland terminal
10
Gate-in inland terminal
Gassing/ degassing
5 Border control/inspection
5.1 Customs
5.2 Quality control
5.3 Other controls
3
Gate in sea terminal
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 41: Carriage of goods import

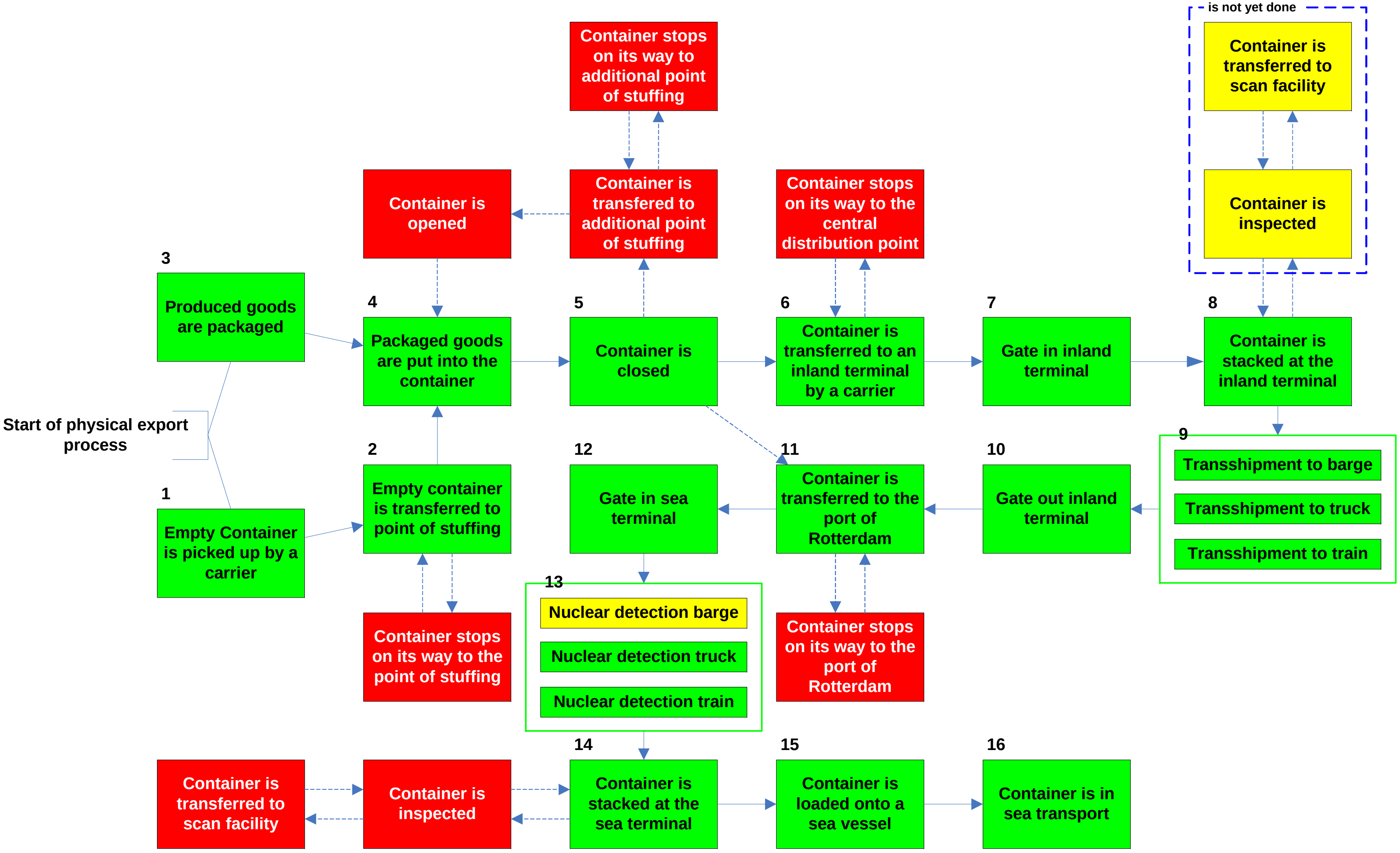

is not yet done
Container is transferred to scan facility
Container is inspected
Container stops on its way to additional point of stuffing
Container is opened
Container is transfered to additional point of stuffing
Container stops on its way to the central distribution point
3
Produced goods are packaged
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
9
Transshipment to barge
Transshipment to truck
Transshipment to train
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
1
Empty Container is picked up by a carrier
13
Nuclear detection barge
Nuclear detection truck
Nuclear detection train
Container stops on its way to the point of stuffing
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 42: Carriage of goods export

C. References

Papers and books

Becker, J. & Verduijn, T. (2005), *Supply chain security IT tools for security*, TNO.

Björkencrona, S. (2006), The European Community Customs Security Initiative, *Conference Supply Chain Security Management 2006*, Mont-Pèlerin / Vevey, Switzerland.

Bocij, P., Chaffey, D., Greasley, A., & Hickie, S. (2003), *Business Information Systems: Technology, Development and Management for the e-business*, Pearson Education Limited, 2nd edition.

Boertien, B., Goedvolk, E., Hammink, E., Hulsebosch, B., Kolff, T., Koolwaaij, J., Linde, M. van der, Middelkoop, E., Oosterhout, M. van, Posthuma, P., Salden, W. & Zandbelt, H. (2002), *Blueprint for a virtual port*, Virtuele Haven deliverable T0.D1, Erasmus University Rotterdam.

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

Chapman, P., Christopher, M., Jüttner, U., Peck, H. & Wilding, R. (2002), Identifying and managing Supply-chain vulnerability, *Logistics and transport focus*, www.iolt.org.uk.

Christopher, M. (1998), *Logistics and supply chain management*, Pitman publishing, London.

Davis, F.D., Bagozzi, R.P. & Warshaw, P. R. (1989), User acceptance of computer technology: A comparison of two theoretical models, *Management Science*, 35(8), 982-1003.

Elmarsi, R. & Navathe, S.B (2000), *Fundamentals of Database Systems*, Addison Wesley, USA.

IEEE 1471-2000 (2000), IEEE Recommended Practice for Architectural Description of Software-Intensive Systems, The Institute of Electrical and Electronics Engineers, Inc.

Lee, H.L. & Whang, S. (2000), Information sharing in a supply chain, *Int. J. Technology Management*, 20(3/4), 373-387.

Looijen, M. (2004), *Beheer van Informatiesystemen*, Ten Hagen & Stam Uitgevers, 6th edition.

Mulholland, A. & Macaulay, A.L. (2006), *Architecture and the Integrated Architecture Framework*, Capgemini, http://www.capgemini.com/services/soa/ent_architecture/iaf/?d=4C418BF7-2926-B6FF-8A63-7FAED70CCF8B Accessed on: 2006-11-14.

Oosterhout, M. van (2003), *Virtual Harbour Container Scanning case presentation*, LM college, Erasmus University Rotterdam.

Oosterhout, M.P.A. van, Zielinski, M. & Tan, Y. (2000), *Inventory of Flows & Processes in the Port*, Virtuele Haven deliverable T2.D1a, Erasmus University Rotterdam.

Popal, N. (2007), *PROTECT D5.1 – Information needs, requirements and recommendations for Supply Chain Security*, Master's thesis (preliminary version), Erasmus University Rotterdam.

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

Rice, J.B. & Spayd, P.W. (2005), *Investing in Supply Chain Security: Collateral Benefits*, IBM Center for the Business of Government, 2nd Edition.

Smit, S. (2004), *A Comparison of Port Community Systems - A framework to compare Port Community Systems and an application to the Port Community Systems of Hamburg, Rotterdam and Antwerp*, Master's thesis, Erasmus University Rotterdam.

Verma, V. (2005), *Leveraging RFID-Enhanced Networks for Ocean Cargo Visibility and Security*, Presentation, Savi Technology, http://www.txcdk.org/rfid/docs/aidc/Verma.ppt.

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

Wagenaar, R.W. (1992), Business Network Redesign: Lessons from the port of Rotterdam simulation game, *Proceedings of the 5th International EDI Conference*, Bled, Slovenia, 390-404.

Willis, H.H. & Ortiz, D.S. (2004), *Evaluating the Security of the Global Containerized Supply Chain*, TR-214, RAND Corporation.

Zachman, J.A. (1987), A framework for information systems architecture, *IBM Systems Journal*, 26(3), 454-470.

Internet

GE Security (2006), CSD, http://www.gesecurity.com/GESecurity/CommerceGuard/CSD.jpg (Accessed on: 2006-11-21).

IBM (2006a), http://www.ibm.com/news/nl/nl/2006/10/nl_nl_news_20061025a.html (Accessed on: 2007-01-16).

IBM (2006b), http://www.nesdis.noaa.gov/space/library/workshops/2006-01-25/beckner.pdf (Accessed on: 2007-01-16).

IFEAD (2007), http://www.enterprise-architecture.info/Images/Extended%20Enterprise/Extended%20Enterprise%20Architecture.htm (Accessed on: 2007-01-14).

Ordina (n.d.), http://www.ordina.nl/solutions/p_so_re_full.asp?SolutionId=3&ReferentieId=99 (Accessed on: 2007-01-16).

Port infolink (2006), http://www.portinfolink.com/english/content/informatie/port_community_systeem.asp (Accessed on: 2006-12-08).

RILA (2007), http://rila.interactive.biz/scs_glossary.htm (Accessed on: 2007-01-12).

Savi Networks Tag (2007), http://www.savi.com/products/SaviTag_656.pdf (Accessed on: 2007-01-16).

Wikipedia (2006), http://en.wikipedia.org/wiki/Security (Accessed on: 2006-12-08).

Wikipedia (2007a), http://en.wikipedia.org/wiki/Exploratory_research (Accessed on: 2007-01-16).

Wikipedia (2007b), http://en.wikipedia.org/wiki/Constructive_research (Accessed on: 2007-01-16).

Interviews

For a list of interviews, see appendix F.

D. List of figures, tables and definitions

Figures

Tables

Definitions

E. List of abbreviations

(S)FTP	(Secure) File Transfer Protocol
AS2/3	Applicability Statement 2/3
B2B	Business-to-Business
B2G	Business-to-Government
BIM	Bilateral Information Model
CIA	Confidentiality, Integrity and Availability
CIM	Centralized Information Model
CIS	Container Integrity System
CSD	Container Security Device
DCMR	DCMR Milieudienst Rijnmond
DGVS	Documentloos Goederen Volgsysteem
DIM	Decentralized Information Model
ECD	Empty Container Depot
ECS	Export Control System
EDI	Electronic Data Interchange
EDIFACT	Electronic Data Interchange for Administration, Commerce, and Transport
EU	European Union
FCL	Full Container Load
GPRS	General Packet Radio Service
GPS	Global Positioning System
IAF	Integrate Architecture Framework
ISA	Information System Architecture
IT	Information Technology
LCL	Less then full Container Load
MQ	Message Queuing
NCTS/Transit	New Computerized Transit System
OTP	Overheidstransactiepoort (government transaction port)
P2P	Peer-to-Peer
PCS	Port Community System
PD	Plantenziektekundige Dienst (Plant Health Division)
POS	Point Of Stuffing
RFID	Radio Frequency Identification
SBB	Sagitta Binnenbrengen
SC	Supply Chain
SCS	Supply Chain Security
SMEs	Small and Mid-sized Enterprises

TAM	Technology Acceptance Model
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)
WP	Work Package
XML	Extensible Markup Language

F. List of interviews

Work package 5.1

In the following table, the organizations in the different categories that were interviewed for the research in work package 5.1 are depicted. Insights from these interviews were used as input for work package 5.2 although these interviews were not primarily meant to address the research questions of this thesis. In the right column, the interviews where the author was present are denoted with an “x”.

Table 11: List of interviews for work package 5.1

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

Work package 5.2

In the following table, the organizations in the different categories that were interviewed for the research in work package 5.2 are depicted. These interviews were meant primarily to answer the research question of this thesis.

Table 12: List of interviews for work package 5.2

Nr.	Category	Organization name	Interviewee	Date
1	Port community system	Port infolink	Mr. Dylan van Iersel & Mr. Iwan van der Wolf	2006-09-19
2	Container integrity system	Siemens	Mr. Gijsbert Huygen & Mr. Robin de Gruijter	2006-10-03
3	Authority system	Dutch Customs	Mr. Henk van Pelt, Mr. Patrick Ramselaar & Mr. Bauke Padding	2006-10-31
4	Port community system	Cargonaut	Mr. Lex Werkhoven	2006-11-08
5	Technology provider	ScreenCheck	Mr. Mark Niekerk	2006-12-28

G. Participants validation workshop Port infolink

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 directions in the development of an ISA for SCS from research presented in this thesis.

Table 13: Participants validation workshop

Category	Organization name	Participant
Port community system	Port infolink	Mr. Iwan van der Wolf
Container integrity system	Siemens / CommerceGuard	Mr. Gijsbert Huygen
Container integrity system	ECT / Savi Networks	Mr. Bart Vermeer
Authority system	Dutch Customs	Mr. Henk van Pelt, Mr. H. van der Kooij & Mr. Bauke Padding
Authority system	Port of Rotterdam Authority	Mr. Jurjen Duintjer
PROTECT project	The Ministry of Transport, Public Works and Water Management Erasmus University Rotterdam TNO TU Delft	Mr. Thierry Verduijn Mr. Marcel van Oosterhout Ms. Sandra Krupe Mr. Jan van den Berg