Elements to evaluate the Security of the Containerized Supply Chain

MASTER'S THESIS

Author: Pedro Vizcaino Moreno

Supervisor: Margherita Pero

Management Engineering

2010-2011

POLITECNICO DI MILANO

Table of Contents

0. Abstract 5

1. Introduction: The Security of the Containerized Supply Chain (C.S.C.) 9

1.1. The Containerized Supply Chain 9

1.2. The Security of the Containerized Supply Chain 10

1.2.1. Situation before September 11, 2001 11

1.2.2. Situation after September 11, 2001 11

2. Literature review to identify Elements related with the Security and Performance of the C.S.C. 13

2.1. Introduction 13

2.2. Research Database 14

2.2.1. Documents of the Research Database 15

2.2.2. Research Topics 16

2.3. Collecting the Elements 17

2.3.1. Elements for Author 17

2.3.2. Collection of original Elements 18

2.4. Linking the Elements: Defining the “Global elements” 19

2.4.1. Global Elements (G.E.) 19

2.4.2. Original Elements integrate in each Global Element 20

2.4.3. Global Elements VS Authors 34

2.4.4. Conceptual Definition of each Global Element 35

2.4.5. Classification of the Global Elements 40

3. Proposed and implemented Measures to improve the Security of the C.S.C. 42

3.1. Introduction 42

3.2. Agreement Measures 43

3.3. Technological Measures 51

4. Analysis of the Measures to improve the Security of the C.S.C. 58

4.1. Introduction 58

4.2. Analysis of the Measures VS global elements “Tools” 58

4.2.1. Analysis summary tables 58

4.2.2. Analysis of the Agreement Measures 59
4.2.3. Analysis of the Technological Measures 63
4.2.4. Conclusions of the Analysis of the Measures VS “Tools” 67
4.3. Analysis of the Measures VS global elements “Performance” 69
4.3.1. Analysis summary tables 69
4.3.2. Analysis of the Agreement Measures 70
4.3.3. Analysis of the Technological Measures 74
4.3.4. Conclusions of the Analysis of the Measures VS “Performance” 77
5. Conclusions and recommendations 80
5.1. About the generation of the Research Database 80
5.2. About the collecting and linking of the identified elements 81
5.3. About the collection and analysis of the Measures 83
5.4. Recommendations 85
6. Annexes 87
6.1. Annex 1: Research Database (Excel) 87
6.2. Annex 2: Elements (Collecting-Linking-Classification) (Excel) 88
6.3. Annex 3: Analysis of the Measures (Excel) 89
6.4. Annex 4: Documents of the Research Database (pdf’s) 89
7. References 90

0. Abstract

This project seeks, through a comprehensive literature research, to identify the elements that allow to define and to assess the Security of the Containerized Supply Chain. The main points developed in the project are:

- Introduction: The Security of the Containerized Supply Chain (C.S.C.)
- Literature review of Elements related with the Security and the Performance of the C.S.C.
- Proposed and Implemented measures to improve the Security of the C.S.C.
- Analysis of the measures to improve the Security of the C.S.C.
- Conclusions and Recommendations

*In the **Introduction** will be discussed the concept of containerized supply chain, which is its definition, the reasons for its existence, its extent and importance in today's society, what factors have led to the increasing importance of the C.S.C. in the international transport system, among other aspects. All this information is intended to help discern why the C.S.C. is an essential element in the global economy and why we should analyze and try to improve its security.*

Additionally, will be outlined how has been addressed the topic of the Security of the C.S.C. to date by the different actors involved, making a clear distinction in the way of acting before and after the attacks of September 11, 2001.

Certainly, the way that it is treated the issue of the Security of the C.S.C. in the literature has changed radically from a literature that gave emphasis on managing the security to prevent the "*smuggling and shrinkage (the loss of cargo shipments through theft and misrouting)"* to a literature that emphasizes in "*preventing terrorists from targeting the C.S.C. or transporting a weapon in a shipping container".*

*The **Literature Review** will begin with an extensive search of literature related to the Security of the C.S.C. and its evaluation.*

Then will be analyzed the literature identified, trying to collect those items that are considered useful to define and assess the Security of the C.S.C.

In the process of analysis of the literature, have been directly identified 30 elements that allow to define and to assess the Security of the C.S.C. at different levels and from different points of view.

The next step will be to analyze the collected items of literature, linking them conceptually. From this linking will be intended generate a series of basic elements that broadly define all aspects affecting the security and performance of the C.S.C.

Therefore, from the analysis of the definitions given by the authors for each of these elements, it can be observed that although with sometimes quite different denominations and with definitions a little different, many of the elements proposed by the authors have ***big and obvious points in common***.

Thus, conceptually linking the identified elements, they have been grouped into 14 basic concepts that have been referred as **Global Elements** in this project and that define the security and performance of the C.S.C.

From that moment, it will work with these "basic elements" generated, classifying conceptually and using them to analyze the measures proposed to improve the Security of the C.S.C.

Thus, going deeper into the definition of the elements integrated into each of the global elements, it has been generated a conceptual definition for each Global Element.

From the process of generation of conceptual definition of the Global Elements, can be concluded that exists a clear difference of nature between those Global Elements.

So, can be identified 3 major subgroups in which can be classified the 14 Global Elements:

- In this way, have been identified a group of Global Elements relating to all those **basic elements, tools and procedures that define the Security of the C.S.C**. This group of Global Elements, in this project, has been named as ***Tools***.
- Another group of Global elements relating to the **possible problems that may affect in a negative way in the operation of the C.S.C**. This group of Global Elements has been named as ***Vulnerabilities***.
- And finally, another group of Global Elements relating to all elements that **define the performance of the C.S.C**. This group of elements has been named as ***Performance***.

*In the **Proposed and Implemented Measures** will have a broad collection of agreement and technological measures, implemented or under development to improve the security of the C.S.C.*

Thus, through the analysis of the specialized literature have been identified a large number of proposals to improve the security of the C.S.C. Moreover, have been detected two distinct levels in terms of these measures. So, there are those that have

been referred to as Agreement Measures and those that have been referred to as Technological Measures.

Within the Agreement Measures are included all efforts made regarding the creation of national and international agreements, policies, performance standards, rules and programs.

Thus, the Agreement Measures identified in the literature and analyzed are the following:

- Maritime Transportation Security Act of 2002 (MTSA)
- Customs-Trade Partnership Against Terrorism (C-TPAT)
- Container Security Initiative (CSI)
- Operation Safe Commerce (OSC)
- Proliferation Security Initiative (PSI)
- Megaports Initiative
- International Ship and Port Security (ISPS)

Within the Technological Measures are included all those technologies used or in developing to improve and strengthen the security of the C.S.C. in the various levels of the supply chain and in different focal areas.

Thus, the Technological Measures identified in the literature and analyzed are the following:

- Antitamper Seals Technologies
- Sensor Technologies
- Radio-Frequency Identification Technologies
- Non-Intrusive Inspections Technologies
- WMD Remote Monitoring Technologies
- Automated Targeting Technologies
- Authentication Technologies

*In the section **Analysis of the Measures** will be analyzed the agreement and technological measures collected regarding the "global elements" generated in the Literature Review section.*

To do this, in a first phase has been analyzed for each measure identified, which basic elements of the Security of the C.S.C. are affected. These basic elements have been identified in this project and have been denominated as the global elements “Tools”.

In a second phase, it has been analyzed for each measure identified how it affects at the different elements of the Performance of the C.S.C. These elements have been

identified in this project and have been denominated as the global elements "Performance".

Finally, the study will be completed extracting the considered most relevant ***Conclusions*** *emerged in the development of this project.*

So, are exposed the most relevant conclusions that can be extracted from the different basic phases of this project:

- In the process of searching for the literature used as a basis of study and analysis in this project.
- In the process of the analysis of the documents, collecting and linking the identified elements that allow to define and to assess the Security of the C.S.C.
- In the process of collection and analysis of the proposed and implemented Measures to improve the security of the C.S.C.

And additionally, in this section of the project will be intended to propose a set of ***Recommendations*** *of action addressed to specialized authors and to the stakeholders directly involved in the topic of the Security of the C.S.C.*

1. Introduction: The Security of the Containerized Supply Chain (C.S.C.)

In this section will be discussed the concept of containerized supply chain, which is its definition, the reasons for its existence, its extent and importance in today's society, what factors have led to the increasing importance of the C.S.C. in the international transport system, among other aspects. All this information is intended to help discern why the C.S.C. is an essential element in the global economy and why we should analyze and try to improve its security.

Additionally, will be outlined how has been addressed the topic of the Security of the C.S.C. to date by the different actors involved, making a clear distinction in the way of acting before and after the attacks of 11 September 2001.

1.1. The Containerized Supply Chain

Since the attacks of 11 September 2001, has been increased exponentially the literature related to the C.S.C., its size and its strategic importance in the economies of the different nations in the World.

Unfortunately, most literature is focused to the specific case of the United States. That is, how the U.S. faced the issue of the C.S.C. and its security.

Following, will be explained which is the C.S.C., through the definitions that have developed the literature analyzed in this project about this topic.

A global supply chain links all the economies in the world. The unit of measure of the supply chain is the shipping container: a sturdy steel box of standard dimensions that carries most freight. Millions of containers circle the earth on specialized ships, railcars, and trucks.

The global supply chain is an international system that has evolved to make the transport of freight throughout the world amazingly efficient. The chain consists of the suppliers, manufacturing centers, warehouses, distribution centers, and retail outlets that move raw materials, work-in-progress inventory, and finished products from producer to consumer. The shipping container and its transport system are integral components of the global supply chain [**Willis-Ortiz, 2004 (B6)]**.

In today's global community, there is no single system that governs the international movement of containerized freight. Instead, multiple actors, agencies, industries, agreements, and legal frameworks affect containerized supply chain systems **[Grillot-Cruise-D'Erman, 2009 (B5)]**.

Approximately 90 percent of the world's cargo is shipped via container, including 75 percent (by value) of non-North American trade to and from the United States. There are approximately 18 million containers of various sizes around the world.
These containers are bolted to the chassis of trucks, stacked two high on flatbed railcars, and packed onto ships as large as aircraft carriers carrying thousands of such containers. Port operations and technology are optimized so that ships spend a minimum amount of time at the quay and the maximum time en route [**Willis-Ortiz, 2004 (B6)]**.

So, containerized transportation has become an increasingly global network that enables goods and people to move quickly and easily among nations around the world.

This phenomenon is the result of the growing economic, social, and cultural interconnectedness that is known as globalization. Closely related is another development— the growing emphasis on intermodalism—which also forces us to think about transportation in a new way. Transportation today no longer consists of several disparate modes functioning as separate entities; on the contrary, the various modes—air, land, sea—are working together ever more closely so that an integrated system is spreading across the world for both passenger and freight, though the latter is far more advanced **[Joseph S. Szyliowicz, 2003 (B8)]**.

Supply chain operations represent an enormous asymmetric threat to the US with in excess of 200 million cargo containers moving around the world each year; 12 million containers entering US ports annually, of which only 3-5% can be physically inspected under current arrangements **[Hauser-Graham-Koerner-Davis, 2004 (B7)]**.

Thus, it is clear that the Security of the C.S.C. is a problem of great importance that must be analyzed.

1.2. The Security of the Containerized Supply Chain

The way to see the Security of the C.S.C. by the different stakeholders involved in and managing it, changed dramatically after of the terrorist attacks of September 11, 2001.

Thus since then, it has emerged vast amount of literature discussing the changes arising from September 11, remarking before and after, commenting on and criticizing the measures carried out and, proposing different ways of acting and key elements in the security of the C.S.C.

1.2.1. Situation before September 11, 2001

Actions to ensure the security of the system of containers and their conveyances have traditionally focused on preventing smuggling and shrinkage (the loss of cargo shipments through theft and misrouting).

The principal concern of business was to increase the efficiency of the global supply chain, paying comparatively little attention to security. In recent years, ocean carriers have cut crews to an absolute minimum and have continued to order larger and faster ships in an effort to squeeze every cent of profit from the system [**Willis-Ortiz, 2004 (B6)]**.

Transportation security essentially meant aviation security before 9/11. This was the only mode that received any significant attention, and even that was sporadic and directed to the prevention of a specific kind of attack that had been carried out successfully. The security needs of the other modes (road, rail, and sea) were largely ignored, even though experts warned that security in those modes also needed attention **[Joseph S. Szyliowicz, 2003 (B8)]**.

Thus, despite numerous warnings, reports, and studies, the transportation security system that existed before September 11, had serious and quite obvious deficiencies.

*In his article **Joseph S. Szyliowicz, 2003 (B8)**, identifies the following deficiencies of the transportation security system, before 9/11:*

1. The lack of intergovernmental coordination, especially in regard to intelligence, perhaps the most critical area for the prevention of terrorist attacks.
2. The relationship between state action and the private sector, especially given the latter's tendency to minimize expenditures on security and the need to answer the key public policy question of how much security at what price is required.
3. The only unit concerned with coordinating security across modes possessed inadequate powers and resources and was vulnerable to the actions of congressional budget cutters.
4. The focus remained on technology and law enforcement with little attention to the context of terrorism or the social causes or to coordinating policy with security issues.

1.2.2. Situation after September 11, 2001

Since September 11, 2001, supply-chain security has been redefined as preventing terrorists from targeting the C.S.C. or transporting a weapon in a shipping container. The change in focus raises questions about the effectiveness of proposed security efforts and the consequences that they may have for supply-chain efficiency.

The initial reaction of national and global supply chains to the September 11 attacks was to increase stock levels to mitigate the possibility of further and sustained supply interruptions. This rapidly developed into additional initiatives and measures to secure the supply chain, constrained by the sheer size and scope of global operations faced by many multinational companies **[Hauser-Graham-Koerner-Davis, 2004 (B7)]**.

Containers potentially pose a serious threat to the Nations security. They can be used to transport illegal weapons, chemicals, explosive materials, and even people. More likely, they can serve as receptacles for dirty bombs or other explosives that could be detonated at seaports. The threat to life is significant, but even greater is the potential economic threat were a container to be used as a bomb at a major port, thus closing operations **[Grillot-Cruise-D'Erman, 2009 (B5)]**.

Anonymity of contents, opaque ownership arrangements for vessels, and corruption in foreign ports have all facilitated the efforts of those who are inclined to use container shipping for illegal purposes **[Willis-Ortiz, 2004 (B6)]**.

The tragedy of September 11 spurred a wide range of policy responses designed to minimize what remains a very serious threat to the nation's security.

Since 9/11, US policy regarding the Security of the C.S.C. has been the protection of American ports (especially seaports) employing "a layered defense", which requires a multitude of policies, programs, and actors be involved. The theory is that, if there is a breach in one layer, it will be caught in subsequent layers.
In addition to a layered defense, there has been a conscious effort to "push the borders out". This means thinking not just in terms of US borders, where a threat has the greatest potential for harm, but enhancing security around the world to create a buffer **[Grillot-Cruise-D'Erman, 2009 (B5)]**.

All agencies therefore, should work together to ensure that at all levels (local, national and international) policies and procedures are coordinated. This requires a great deal of communication, cooperation, and information-sharing to be effective

Because the C.S.C. is the central component of global trade, it has been necessary to incorporate public and private actors in both a domestic and international setting into the national strategy of each country **[Grillot-Cruise-D'Erman, 2009 (B5)]**.

2. Literature review to identify Elements related with the Security and Performance of the C.S.C.

2.1. Introduction

This section is the main and largest block of this project. Is where the greatest effort has been made regarding search and analysis of the literature on the topic of the C.S.C. and its Security, with the main objective of identify Elements related with the Security and Performance of the C.S.C. that allow to define and assess this Security.

Following, it will be exposed the whole process followed in this Literature Review to obtain the previously mentioned Elements.

The first step has been to generate a rich Research Database for the project. To do this has been carried out an exhaustive search of documents related to the Security of the C.S.C. and its evaluation.

Once created this database specifically for the Project, we have been able to begin the analysis of the documents that compose this Research Database.

Through this comprehensive analysis, have been identified these Elements related with the Security and Performance of the C.S.C. that allow to define and assess this Security.

The next step has been to link conceptually the identified elements, generating what has been called in this project as Global Elements.

Since then, it have worked with these Global Elements, analyzing what Global Elements are more used by the authors in the literature, developing an integrative conceptual definition of each Global Element and identifying possible classifications of these Global Elements.

These Global Elements identified have been used in subsequent sections of this project (points 3 and 4 of the project) to identify and analyze the proposed and implemented Measures to improve the Security of the C.S.C.

Below, it is proceeded to explain in more detail the process followed in this section of the project.

2.2. Research Database

As mentioned in the introduction of this section, the first step has been to generate a rich Research Database for the Project. For this, has been performed an exhaustive search of documents related to the Security of the C.S.C.

In the ***ANNEX 1: Research Database (excel)*** there is the Excel file where have been collected and coded the documents found, studied and analyzed.

To do the search of the documents have been used as the main source of search the databases ISI Web of Knowledge and SCOPUS. And to make the search in the databases ISI Web of Knowledge and SCOPUS, have been used a set of Research Topics, which are listed in next subsections.

In the Excel, have been identified each document with an alphanumeric code: Letter+Number.

For each document have been also indicated the Research Topics used to find them in the database "ISI Web of Knowledge"

- For example, the following code: 01 (8) indicates that have been found the document using the Research topic RS-01 in the ISI database and the document is in position 8 of the results list.
- The documents that are coded as follows: 05 (8**.1**) are documents that have not found directly in ISI but have been found elsewhere through a document from the ISI database.

In the Excel file, below the main table, are listed the documents that are considered interesting but couldn't be found the full document.

For each document that has been available, have been also mentioned the website where have been found the full document.

Once created this database specifically for the Project, it has been able to begin the analysis of the documents that compose this Research Database.

Through this comprehensive analysis, have been identified these Elements related with the Security and Performance of the C.S.C. that allow to define and assess this Security.

Similarly, for each file analyzed, has been identified that all secondary information that is also relevant to this project, such as the "Proposed and implemented Measures to improve the Security of the C.S.C."

According to the potential information that can be extracted from each of the documents, they have been rated with a level of utility.

In this form, in addition has been updated periodically the Excel ***ANNEX 1: Research Database*** where have been collected all the documents found, marking progressively the elements already read and analyzed.

2.2.1. Documents of the Research Database

Below, there is the list of documents found during the search, that forms the Research Database and that have been the basis of study and analysis of this project.

Are marked in green, the documents that have been considered important in the development of the study of the documents and in the development of this project.

Are marked in orange, the documents that are considered essentials in the development of the study of the documents and in the development of this project.

Id	Document Name
A0	Methods Toward Supply Chain Risk Analysis
A1	Risk Assessment of Supply Chain System Based on Information Entropy
A2	The contribution of third-party indices in assessing global operational risks
A3	An empirical investigation into supply chain vulnerability
A4	Assessing the vulnerability of supply chains using graph theory
A5	The roles of risk and efficiency on the relation between logistics performance and customer
A6	Semi-quantitative risk assessment of commercial scale supply chain of hydrogen fuel and implications
A7	Risk assessment and management for supply chain networks A case study
A8	Safety assessment of envisaged systems for automotive hydrogen supply and utilization
A9	The design of robust value-creating supply chain networks. A critical review
B0	Buyer perceptions of supply disruption risk A behavioral view and empirical assessment
B1	The Research of Container Multimodal Transport Risk Assessment Based on BP Neural Network
B2	A Supply Chain Risk Assessment Model Based on Multistage Influence Diagram

B3	A Searching Model of Trustworthy Supply Chain --TSFM
B4	Risk Analysis of Chemical, Biological, or Radionuclear Threats Implications for Food Security
B5	National and Global Efforts to Enhance Containerized Freight Security
B6	Evaluating the Security of the Global Containerized Supply Chain
B7	A Fully Integrated Global Strategic Supply Network
B8	International Transportation Security
B9	Container security a proposal for a comprehensive code of conduct
C0	The political economy of maritime container security
C1	Spring 2008. Industry Study. Transportation
C2	Maritime Commerce Security Plan for The National Strategy for Maritime Security
C3	Introduction Terrorism and Transportation Security
C4	Container Security Preventing a Nuclear Catastrophe
C5	Applying risk assessment to secure the containerized supply chain
C6	The Container Security Initiative and Ocean Container Threats
C7	Design and integration of the containers inspection activities in the container terminal operations
C8	Simulation, risks modeling and sensors technologies for container terminals security
C9	Protecting the Nation's Seaports: Balancing Security and Cost
D0	Transportation security technologies research and development
D1	RFID-enabled Innovative Solutions Promote Container Security
D2	Critical factors affecting the adoption of container security service: The shippers' perspective
D3	Security Supply Chain
D4	Higher supply chain security with lower cost Lessons from total quality management
D5	An approach to security and privacy of RFID system for supply chain
D6	Supply Chain Management under the Threat of International Terrorism

Table 1. Documents of the Research Database

Thus, to make the study that composes this project, the analysis has done with a total of 37 documents.

In the ***ANNEX 4: Documents of the Research Database*** there are the full pdf's files of the documents that compose the Research Database.

2.2.2. Research Topics

The Research Topics inserted in the database ISI Web of Knowledge and SCOPUS to find the necessary documents for this project are the following:

Id	Name Document
RS-00	methods assess security supply chain
RS-01	risk assessment supply chain
RS-02	supply chain security assessment
RS-03	containerized supply chain
RS-04	assess supply chain security
RS-05	container supply chain security

Table 2. Research Topics

2.3. Collecting the Elements

Thoroughly analyzing each of the documents of the Research Database, it has been tried to identify those *Elements related with the Security and Performance of the C.S.C. that allow to define and assess this Security and performance*.

In the ***ANNEX 2: Elements (Colleting-Linking-Classification)*** there is the Excel file that has been used to made the collection and the linking of the elements identified in some of the documents that compose the Research database.

2.3.1. Elements for Author

So, the first step has been to identify the relevant elements in the different documents.

By the studying of the documents, have been identified those that provided relevantly **Elements** related with the Security and Performance of the C.S.C.

In the following table are collected the elements identified in the analysis of the documents, for each of the authors that address this issue in a relevant way.

Id	B5	B6	A0	A9	B7	C2
Autor	Grillot-Cruise-D'Erman	Willis-Ortiz	Pai-Kallepalli-Caudill-Zhou	Klibi-Martel-Guitouni	Hauser-Graham-Koerner-Davis	Dep. of Homeland Security
Year	2009	2004	2003	2009	2004	2005
Indicators	Infrastructure Policy Documentation Cooperation and Coordination	Efficiency Shipment reliability Shipment transparency Fault tolerance Resilience Physical logistics layer Transaction layer Oversight layer	Contamination Disruption Corruption	Robustness Flexibility Redundancy Resilience Endogenous assets Supply Chain Partners Exogenous Geographical Factors	Physical Security Information Security Freight Security	Data accuracy Cargo Security Vessels/ports security Transit Security International Standards and compatible regulations

Table 3. Groups of elements by Author

2.3.2. Collection of original Elements

The next step has been collect and put in common all the elements to facilitate the identification of conceptual relationships between the 30 elements resulting from the study of the documents.

In the following table are exposed the groups of original elements by author identified in the documents from the Research Database, put in common to link them conceptually in later sections.

Infrastructure Policy Documentation Cooperation and Coordination	B5
Efficiency Shipment reliability Shipment transparency Fault tolerance Resilience	B6
Physical logistics layer Transaction layer Oversight layer	B6
Contamination Disruption Corruption	A0
Robustness Flexibility Redundancy	A9

Resilience	
Endogenous assets Supply Chain Partners Exogenous Geographical Factors	A9
Physical Security Information Security Freight Security	B7
Data accuracy Cargo Security Vessels/ports security Transit Security International Standards and compatible regulations	C2

Table 4. Collection of original Elements

The Excel file of ***ANNEX 2: Elements (Colleting-Linking-Classification)*** has been used of support in the process of conceptual linkage of the original elements from the table above, getting which this project have been referred as **Global Elements**.

In the following sections of this project is explained in detail the process followed to link conceptually the original elements and are defined in detail the "Global elements" obtained.

2.4. Linking the Elements: Defining the "Global elements"

Once identified the relevant elements related with the *Security and Performance of the C.S.C.*, the next step has been to try link these elements conceptually.

Through this conceptual link, it have tried to obtain some basic elements that determine the key points in terms of security and performance of the C.S.C., from the literature written about this subject.

Conceptually linking the elements, they have been grouped into 14 basic concepts that have been referred like **Global Elements** in this project.

2.4.1. Global Elements (G.E.)

In the following table are exposed the Global Elements generated after the conceptual linking of the Elements identified in the documents of the Research Database.

1	**Infrastructure and physical security**
2	**Documentation / Info security**
3	**Cooperation and coordination**
4	**Policy, standards and regulations**
5	**Cargo Security**
6	**Transit Security**
7	**Contamination**
8	**Disruption**
9	**Corruption**
10	**Efficiency**
11	**Reliability / Robustness**
12	**Shipment Transparency**
13	**Fault tolerance**
14	**Resilience**

Table 5. Global Elements generated

With the objective of generate these Global Elements, has been followed the next process:

- Collect the original elements identified in the documents of the Research Database.
- Analyze the definitions made by the authors, of each of the elements proposed in their documents.
- Link conceptually the original elements together, creating groups of elements with the same or similar definitions.

2.4.2. Original Elements integrate in each Global Element

In the following section are exposed and defined in detail the original elements proposed by the different authors analyzed, which integrate each Global Element.

In this way can be seen that, although with sometimes quite different denominations and with definitions a little different, many of the elements proposed by the authors have ***big and obvious points in common***.

So, this effectively shows that there are some basic and recurrent elements in the literature (which in this project have been referred as Global Elements) that define the security and performance of the C.S.C.

Thus, the original elements of the authors integrated in each Global Element, with their respective definitions are the following:

1. Infrastructure and physical security

Infrastructure	B5	Grillot-Cruise-D'Erman, 2009
Physical logistics layer	B6	Willis-Ortiz, 2004
Endogenous assets	A9	Klibi-Martel-Guitouni, 2009
Exogenous Geographical Factors	A9	Klibi-Martel-Guitouni, 2009
Physical Security	B7	Hauser-Graham-Koerner-Davis, 2004
Vessels/ports security	C2	Dep. of Homeland Security, 2005

"Infrastructure and physical security" is one of topics most used in the literature in connection with the security of the C.S.C.

Grillot-Cruise-D'Erman, 2009 (B5) to refer to this element, use the concept of **Infrastructure**. Infrastructure refers to the physical measures taken to enhance port security. This includes physical detection methods used at ports of entry and exit. Moreover, secure ports are those that can respond to an incident and recover after a traumatic event. Response and recovery plans are, therefore, an important element related to infrastructure.

Inside of the concept of Infrastructure are included the following elements:

- Targeting System, Information Data Base and Threat Assessment → use of an information database, which includes manifested cargo, origination, transit, and destination information, and shipper and shipping histories, to identify potentially risky container cargo.
- Physical Security Measures and Detection Devices → Secure fencing, guards, surveillance equipment, and other physical barriers should be in place to limit access to port property and containerized freight. Containers themselves should incorporate physical security measures, such as seals, that prevent and identify tampering. There should also be a means of physically examining or screening cargo with appropriate technology. Moreover, ports should engage in research and development (R&D) to enhance security operations, discovering and implementing stronger security measures and detection devices.
- Training → Personnel involved in port operations should be trained to recognize suspect activities, questionable cargo, and appropriate security procedures. Such training should also be regularly refreshed.
- Response and Recovery → In the event of a terrorist or other traumatic event at a port of entry/exit, port operations should incorporate rapid response and recovery plans.

Willis-Ortiz, 2004 (B6) use the concept of **Physical logistics layer**. The Physical logistics layer is a point of view of the Supply Chain, that view it like a conveyance through which products move. The system of roads, tracks, and sea-lanes and the containers that flow along them comprise a network, one that provides services to the producers and consumers of goods.

In the physical logistics layer, the nodes are all facilities through which the cargo travels from origin to destination, and the edges (i.e., the links that connect nodes) are the roads, railroad tracks, and sea-lanes on which the cargo moves.

This view of the supply chain merges two perspectives. In OECD (2003), author Philippe Crist considered the Physical logistic layer from the points of view of the places through which cargo travels and of the people who have access to cargo at various stages.

Actions to secure the supply chain follow these figures by **limiting the access of people to the cargo or by securing the routes and conveyances on which it travels.**

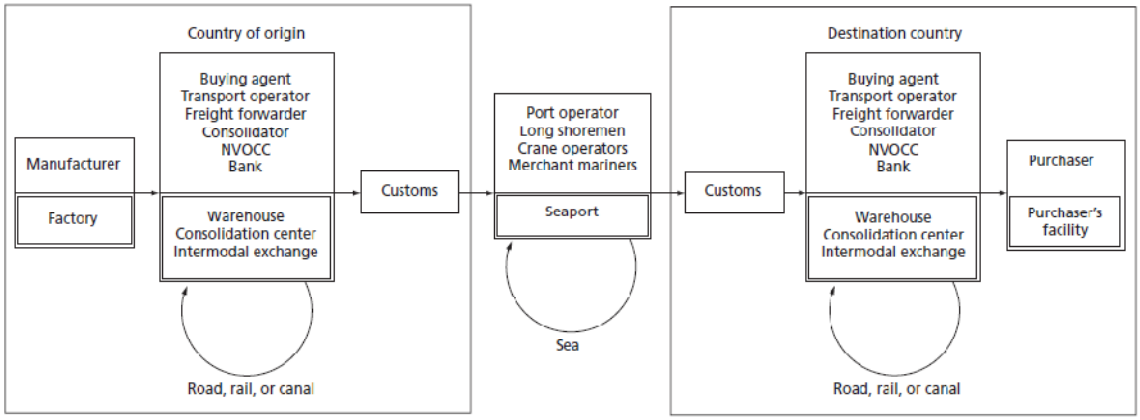

Image 1. Scheme of the Containerized Supply Chain

Klibi-Martel-Guitouni, 2009 (A9) to refer to Infrastructure and physical security use the concepts of **Endogenous Assets** and **Exogenous geographical factors**, defining thus, the different physic sources of vulnerability of the Supply Chain.

The concept of Endogenous Assets refers to internal elements of the companies that are part of the Supply Chain: equipments, vehicles, human resources and inventories of production, distribution, recovery, revalorisation and service centers.

The concept of Exogenous Geographical Factors refers to all elements and factors external to firms that are part and influence in the Supply Chain: Nature, public infrastructures (travel ways, terminals/ports, telecommunication networks, utilities) and socio-economic-political factors.

Hauser-Graham-Koerner-Davis, 2004 (B7) to refer to this topic, use de concept of **Physical Security**.

The concept of Physical security refers to the provision of physical asset protection for organizational infrastructure and facilities.

In terms of the infrastructure security, the authors identified various security measures including: access control, badges, cameras, guards and employee checks, and the testing of security by an external firm. Facilities security is provided by these measures and also focuses on perimeters, policy, procedures and personnel.

Dep. of Homeland Security, 2005 (C2) to refer to the element of Infrastructure and physical security, use the concept of **Vessels/ports security**.

With the concept of Vessels/ports security, the author addresses the security of vessels, facilities and ports. These security procedures are important since the protection of the vessel, facility and port, also serves to protect the cargo.

According to the authors, security procedures must be in place to prevent the smuggling on board of weapons of mass destruction and other dangerous materials while the vessel is in port. These procedures should also prevent illegal migration (stowaways).

2. Documentation / Info Security

Documentation	B5	Grillot-Cruise-D'Erman, 2009
Information Security	B7	Hauser-Graham-Koerner-Davis, 2004
Data accuracy	C2	Dep. of Homeland Security, 2005

Grillot-Cruise-D'Erman, 2009 (B5) use the concept of **Documentation**. With this concept, the authors refer to tracing the movement of containers as they enter, traverse, and leave the supply chain, as well as checking contents of containers, their source, and their destination, through appropriate documentation. It also includes the secure transmission of information between the different stakeholders.

Inside of the concept of Documentation are included the following elements:

- Manifests, Certificates and Verification → Cargo manifests and import/export certificates enhance the level of port security by increasing the ability to monitor and verify the global movement of goods.
- Background Checks and Identification Cards → All personnel who are involved in the movement of goods through the supply chain should undergo a thorough background check and be issued proper identification cards. Periodic reviews of identification cards and their issuance should also be conducted.

Hauser-Graham-Koerner-Davis, 2004 (B7), refer to this topic through the concept of **Information Security**. Information Security includes measures to protect both Information security and Information assurance, and includes the products, procedures and policies that allow the timely transfer of information in an accurate and secure way among all parties.

Vulnerabilities in Security Information according to the author:

- ***Software.*** Current software applications have not all been designed with security in mind and present significant vulnerabilities for both internal and external supply chain environments. Specifically these applications are susceptible to trojans, worms and viruses as demonstrated most recently by the MS Blaster Worm and have the potential to seriously interrupt operations or take down total systems.
- ***Hackers.*** Hackers may gain access to the core systems' main servers and obtain access to very sensitive information, disrupt operations, engage in fraudulent practices or take down entire systems. With terrorism on the rise, hackers may engage in what is being termed cyber-terrorism imposing significant cost, interruption or ineffectiveness on the US economy and/or military command and control systems.

Dep. of Homeland Security, 2005 (C2) to refer to this topic use the concept of **Data Accuracy**. The concept of Data Accuracy refers to Advance electronic information necessary to support the *risk assessment of the cargo*.

This assessment identifies cargo that may present a threat and thus may require some type of intervention. This information is needed early in the process to identify high-risk cargo before it enters the Maritime Domain.

The objective is to obtain the critical information necessary to assess reliably the risk of individual cargo transactions. There are many parties with pieces of information that taken together can form a complete picture. The buyers, sellers, shippers and carriers form the outline, but the information process is dynamic.

The risk assessment must be equally dynamic, acquiring information from multiple sources to capture an end-to-end data perspective on each transaction.

3. Cooperation and coordination

Cooperation and Coordination	B5	Grillot-Cruise-D'Erman, 2009
Transaction layer	B6	Willis-Ortiz, 2004
Supply Chain Partners	A9	Klibi-Martel-Guitouni, 2009

Grillot-Cruise-D'Erman, 2009 (B5) use the concept of **Cooperation and Coordination**. Cooperation and Coordination refers to the activities to obtain a high level of cooperation and coordination at all levels of and among all parties involved in trade,

This involves the sharing of information, joint practices and interagency and inter-party communication, as well as enforcement of rules and regulations and a system of accountability that requires joint action.

Ultimately, a secure supply line requires open communication and coordination within states, across states, and between varied actors.

Inside of the concept of Cooperation and Coordination, the autors includes the following elements:

- Inter-agency Communication and Coordination → All domestic agencies involved with the security and movement of freight along the supply chain must have open communication and a high level of cooperation among them. Regular interaction, coordination, and sharing of information among relevant agencies and their officers enhance all their activities, ensure an appropriate division of labor, and prevent unnecessary duplication and waste.
- Government and Business Cooperation and Coordination → Programs and partnerships between governments and business entities help to ensure the security of freight and ports. Bringing the business community into the security process allows for their concerns to be addressed and makes them even more invested in the structure of the supply chain.
- International Cooperation and Coordination → Programs and partnerships between countries should exist in an effort to share new technologies, arrange for and implement collaborative training exercises, and endure the adoption of common, harmonized security measures around the world. This requires bilateral and multilateral interactions and exchanges on all aspects of policy, procedure, and implementation of supply chain security.
- Information sharing and Privacy protection → Information about shippers, exporters, importers, and goods is the key to a secure freight system. Therefore, information must be shared with all relevant actors in order to detect potentially dangerous transactions. Commercial agents must provide manifest information that is accurate, and it must be shared with security officials.
- Enforcement and Accountability → The existence of diligent police and investigative authorities who can and do enforce security measures. This also requires that there is a means of punishment for those who break the laws, including both criminal and civil liabilities.

Willis-Ortiz, 2004 (B6) address this topic through the concept of **Transaction layer**. The Transaction layer is a point of view of the Supply Chain, that view it, like a system that procures and distributes goods and that is driven primarily by information flows. From this point of view, the supply chain is its network of suppliers and sub-suppliers.

This transaction layer connects participants to each other legally through contracts, informationally through product specifications, financially through transaction records, and physically through the actual product or good.

This transaction-based view of the global supply chain can be represented as the union of two interacting networks: an **information network** and a **material network**. The information network coordinates the flow of goods and payments and is regulated by U.S. and international trade law. The material network for a particular firm includes all direct and indirect suppliers of goods.

Failures of nodes in the transaction layer are fundamentally different from failures in the physical logistics layer.

The transaction layer views the logistics layer as a conveyance mechanism. A failure in the transaction layer eliminates the source of a product or the financial flows that trigger logistics demands; a failure in the logistical system limits the flow of goods through a particular port, rail yard, or truck stop or along a particular route.

The disruption of a supplier (node of the transaction supply chain) affects its customers, but a disruption to a port (physical logistic layer) affects all cargo that would have passed through it.

Thus the Transaction layer, is the layer where it must interact the business stakeholders to agree and determine the amount and direction of the flow of goods from one place to another in the Supply Chain System.

Klibi-Martel-Guitouni, 2009 (A9) to refer to this element use the concept of **Supply Chain Partners**. This concept includes the customers, raw material and energy suppliers, subcontractors and third-party logistics providers (3PLs), defining thus, the different sources of vulnerability due to supply chain partners and coordination in the Supply Chain.

4. Policy, standards and regulations

Policy	B5	Grillot-Cruise-D'Erman, 2009
Oversight layer	B6	Willis-Ortiz, 2004
International Standards and compatible regulations	C2	Dep. of Homeland Security, 2005

Grillot-Cruise-D'Erman, 2009 (B5) use the concept of **Policy**. Policy refers to the regulations taken to enhance port security.

This includes government rules, policies, regulations, laws and procedures that outline legal authority and delineate actors and their responsibilities regarding containerized freight.

Willis-Ortiz, 2004 (B6) to refer to the topic of "policy, standards and regulations", use the concept of **Oversight layer**. The Oversight layer is a point of view of the Supply Chain, that focuses in implements and enforces rules of behaviour within and among the subsystems of the Supply Chain through standards, fines and duties.

This layer of the supply chain includes customs organizations, law enforcement, and national and international bodies, and oversees the contracting for and movement of goods.

At times, the oversight bodies work within a particular layer of the supply chain (physical logistics layer or transaction layer). At other times, the organization must interact with both layers.

Each transaction or movement of goods over the supply chain occurs under the auspices of a regulatory regime consisting of all the rules, regulations, and enforcement mechanisms that govern the structure and operation of the transaction and the physical layers of the supply chain.

Each piece of regulatory apparatus collects information to ensure that its directives are being met, and these data together form the intelligence that allows targeting of shipments.

Dep. of Homeland Security, 2005 (C2) to refer to this topic, speaks of **International Standards and compatible regulations**.

An important way to achieve a secure supply chain is to engage appropriate international organizations in the development of standards. Standards are the only meaningful way that the government will be able to ensure that a certain level of security across the supply chain can be expected and achieved.

Given the limitations of governmental jurisdiction and direct business influence on the international supply chain, we must use international organizations to develop minimum acceptable standards for security in international trade.
International standards play a crucial role in reaching foreign portions of the international supply chain that are not influenced by the requirements of any one nation.

5. Cargo Security

Cargo Security	C2 Dep. of Homeland Security, 2005

Dep. of Homeland Security, 2005 (C2) use the concept of **Cargo Security**. With this concept, the autors refer to the Procedure to ensure that the cargo to be loaded on the vessel conforms to the cargo information electronically transmitted to the authorities.

Characteristics of the process:

- This process connects first-hand knowledge of the cargo with the validation of the cargo information.
- This process also ensures that safeguards are in place to prevent unlawful materials (or people) from being combined with the legitimate cargo.
- Also includes a risk management process that includes the inspection (physical inspection and/or the use of non-intrusive inspection equipment) of cargo identified as high risk prior to loading at foreign ports and, in some cases, after arrival at National port.

This is the most difficult part of the maritime security framework. It consists of the development of business security procedures to secure containerized cargo at the point of stuffing (loaded into an intermodal container) and that other types of cargo are secure before they are loaded on vessels. Since this activity takes place outside the United States, there is limited regulatory authority to require specific security practices. The Customs-Trade Partnership against Terrorism has developed security criteria that participants must follow when loading containers to prevent illegitimate materials from being inserted during this phase of the supply chain. Expanding industry and government partnerships, combined with international cooperation, will be necessary to embed the essential security procedures into common business practices. The second part of secure cargo is the use of risk management and non-intrusive inspection equipment to verify that the cargo really is secure. The consequences of a nuclear attack through maritime cargo are so great that it must be the first priority. The world's seaports must become a barrier to nuclear proliferation. The longer term objective is to develop a large scale capability to detect rapidly the full spectrum of weapons of mass destruction or effect which include chemical, biological, radiological, nuclear, and high explosive threats.

6. Transit Security

Transit Security	C2	Dep. of Homeland Security, 2005
Freight Security	B7	Hauser-Graham-Koerner-Davis, 2004

Dep. of Homeland Security, 2005 (C2) speak about the concept of **Transit Security**. Transit Security refer to the procedure to Ensure that the secure cargo remains in that status as it enters and moves through the Maritime Domain. Successful implementation requires a method of detecting that security has been compromised during transit and a response protocol to determine if the cargo has remained secure.

It's necessary a method to verify that the initially secure cargo remains secure throughout the journey. For many types of cargo, such as liquid or dry bulk, the vessel itself is the cargo container. In these cases, we rely on the security procedures for the vessel to secure the cargo during transit.

Containerized cargo presents a different situation. In some ways, containerized cargo has two layers of protection since it is protected by the container and by the vessel

during the voyage. However, it also is more dangerous because the container may have a very long unprotected journey before it is loaded on the vessel. Supply chain studies have identified the many vulnerabilities of containerized cargo as it makes it way from the inland point where it was loaded until it reaches the harbor.

A secure system must be able to detect whether or not the security of the container has been compromised before it is allowed to enter the Maritime Domain.

Hauser-Graham-Koerner-Davis, 2004 (B7) to refer to the topic of cargo security use the concept of **Freight Security**.

Freight security refers to the packages, pallets and containers, which ship goods and products around the world by land, sea and air with security. Security in the international supply chain for freight has become one of the highest priorities for the US government. After September 11, the highest-order definition of freight security changed from theft-proof to tamper-proof.

7. Contamination

Contamination	A0 Pai-Kallepalli-Caudill-Zhou, 2003

Pai-Kallepalli-Caudill-Zhou, 2003 (A0) define the concept of **Contamination** like a threat to affect the assets that form part of the Supply Chain.

With the concept of Contamination, the authors refer to any form of environmental contamination from untreated waste streams, contamination of the raw material/manufactured product or contamination of surroundings resulting in hazardous environment for the workers.

The threat Contamination is assumed **a result of accident or terrorist activity**.

8. Disruption

Disruption	A0 Pai-Kallepalli-Caudill-Zhou, 2003

Pai-Kallepalli-Caudill-Zhou, 2003 (A0) define the concept of **Disruption** like a threat to affect the assets that form part of the Supply Chain.

Disruption can be any form of interruption leading to work halt and it can arise from events of natural disaster, terrorism or accidents.

9. Corruption

Corruption	A0 Pai-Kallepalli-Caudill-Zhou, 2003

Pai-Kallepalli-Caudill-Zhou, 2003 (A0) define the concept of **Corruption** like a threat to affect the assets that form part of the Supply Chain.

Corruption is refered to the terrorist acts of information hacking or tampering and for this reason is assumed a result of terrorist activity.

10. Efficiency

Efficiency	B6 Willis-Ortiz, 2004

Willis-Ortiz, 2004 (B6) expose that the stability of the global container shipping industry is based on efficiency and security. So, the ability of the Global container supply chain to deliver goods efficiently and securely can be described through 5 measurable capabilities. One of these 5 capabilities is defined by the concept of **Efficiency**.

Efficiency is the raison d'etre of the Supply Chain. So, the global container supply chain has evolved primarily to deliver goods more quickly and more cheaply than other modes of transport when volume and mass are taken into account.

For this reason, initiatives to improve supply chain security must take into account also the efficiency parameter, trying to improve or at least not worsen it.

11. Reliability / Robustness

Shipment reliability	B6 Willis-Ortiz, 2004
Robustness	A9 Klibi-Martel-Guitouni, 2009

Willis-Ortiz, 2004 (B6), to speak about this topic develop the concept of **Shipment reliability**. As explained by the authors, the ability of the Global container supply chain to deliver goods efficiently and securely can be described through 5 measurable capabilities. One of these 5 capabilities is defined by the concept of Shipment reliability.

For exists Shipment Reliability in the Supply Chain, it must behave as expected, retrieving and delivering goods as directed, with a minimum amount of loss due to theft and accident.

Supply chain shrinkage, resulting from misrouting and theft of goods, erodes both the reliability and the efficiency of the shipping network. Misrouting causes losses through

delays in shipment delivery. Theft results in both direct economic losses and indirect losses resulting from delays in product delivery.

Klibi-Martel-Guitouni, 2009 (A9) to refer to this topic use the concept of **Robustness**.

The robustness is defined as the extent to which the SC is able to carry its functions for a variety of plausible future scenarios.
SC is robust, for the planning horizon considered, if it is capable of providing sustainable value creation under all plausible future scenarios (normal business conditions as well as major disruptions).

12. Shipment Transparency

Shipment transparency	B6	Willis-Ortiz, 2004

Willis-Ortiz, 2004 (B6), to speak about this topic develop the concept of **Shipment transparency**. As explained by the authors, the ability of the Global container supply chain to deliver goods efficiently and securely can be described through 5 measurable capabilities. One of these 5 capabilities is defined by the concept of Shipment transparency.

To obtain a Shipment transparency, the goods that flow through a supply chain must be legitimately represented to authorities and must be legal for transport.

The system should be transparent enough to minimize improper use of the system. Traditionally, transparency has involved inspections at the port of entry to detect illegal immigrants or items being smuggled in an attempt to avoid regulations or tariffs.

With homeland security currently receiving so much attention, the focus of exclusion has shifted to preventing terrorists from using the container shipping system to carry out attacks on the United States. Inspection at the port of entry can make it more difficult for terrorists to use containerized shipping as logistical support for moving people and supplies. However, inspections at the port of entry are less helpful for preventing terrorists from using containers as a means of attack (e.g., detonating a bomb aboard a ship arriving at port).

13. Fault tolerance

Fault tolerance	B6	Willis-Ortiz, 2004
Flexibility	A9	Klibi-Martel-Guitouni, 2009
Redundancy	A9	Klibi-Martel-Guitouni, 2009

Willis-Ortiz, 2004 (B6), to speak about this topic develop the concept of **Fault Tolerance**. As explained by the authors, the ability of the Global container supply chain to deliver goods efficiently and securely can be described through 5 measurable capabilities. One of these 5 capabilities is defined by the concept of Fault Tolerance.

The concept of Fault Tolerance indicates that the container shipping system should be able to respond to disruptions and failures of isolated components without bringing the entire system to a grinding halt.

Because the system is a network, problems at one node—such as a port—affect interconnected parts of the system. In unstable systems, a problem at a single node or link in the supply chain can bring the entire network to a halt. In fault-tolerant systems, the surrounding ports and distribution system can compensate when a section of the system is compromised. To the extent that neighboring ports and facilities are able to compensate for the loss of a port, the containerized shipping system is more fault tolerant.

Klibi-Martel-Guitouni, 2009 (A9) to refer to the topic of Fault Tolerance use the concepts of **Flexibility and Redundancy based capabilities**.

Flexibility based capabilities are developed by investing in SC structures and resources before they are needed.

Redundancy based capabilities involve a duplication of network resources in order to continue serving customers while rebuilding after a disruption.
An important distinction between flexibility and redundancy based capabilities is that the latter may not be used.

Examples of design decisions providing **Flexibility based capabilities** include selecting production/warehousing systems that can support several product types and real-time changes, choosing suppliers that are partially interchangeable, and locating distribution centers to ensure that all customers can be supplied by a back-up center with a reasonable service level if its primary supplier fails.

Examples of **Redundancy based capabilities** include insurance capacity, that is maintaining production systems in excess of business-as-usual requirements, and insurance inventory dedicated to serve as buffers in critical situations.

Both flexibility and redundancy collaborate on improving the capacity of **Responsiveness** of the Supply Chain. The Responsiveness aims at providing an adequate response to short-term variations in supply, capacity and demand.

14. Resilience

Resilience	B6	Willis-Ortiz, 2004
Resilience	A9	Klibi-Martel-Guitouni, 2009

Willis-Ortiz, 2004 (B6), to speak about this topic develop the concept of **Resilience**. As explained by the authors, the ability of the Global container supply chain to deliver goods efficiently and securely can be described through 5 measurable capabilities. One of these 5 capabilities is defined by the concept of Fault Tolerance.

Resilience is the ability of the supply chain to return to normal operations after a failure. Resilience is a function of the system design and the response from the oversight layer

A supply chain is resilient insofar as it is able to return to normal operating conditions quickly after the failure of one or more components. Resilience is a function of both the system's design and the responsiveness of the oversight layer.

For example, suppose that an oil spill occurs at a port. The response to contain the spill would impede the loading and unloading of ships, creating backlogs at the port and delaying shipments elsewhere. The more resilient the supply chain is, the quicker these backlogs will be cleared, avoiding the resulting delays.

Klibi-Martel-Guitouni, 2009 (A9), speak about the concept of **Resilience**, too. For this autors, the concept of Resilience is defined as the capacity of a system to survive, adapt, and grow in the face of unforeseen changes, even catastrophic incidents

The Resilience of the Supply Chain can be seen as a strategic posture of deployed resources (facilities, systems capacity and inventories), suppliers and product-markets, as a physical insurance against SC risk exposure, providing the means to avoid disruptions as much as possible, as well as the means to bounce back quickly when hit.

The authors conclude from empirical studies that business is in need of resilience strategies to deal effectively with unexpected disruptions. The main challenge is to elaborate resilience strategies providing an adequate protection from disruptions without reducing the SCN effectiveness in business-as-usual situations. This can be done by avoiding or transferring risks, and/ or by investing in flexible and redundant network structures.

2.4.3. Global Elements VS Authors

Once generated the Global Elements, the next step was to measure how frequently are used each of these Global Elements in the literature studied.

To this end, have been developed a Table of Global Elements VS authors. In this table has scored for each of the Global Elements, which authors propose an element integrated in this Global Element.

So, can be easily analyzed the Global Elements which are more proposed by the authors in the analyzed literature.

		Grillot-Cruise-D'Erman, 2009	Willis-Ortiz, 2004	Pai-Kallepalli-Caudill-Zhou, 2003	Klibi-Martel-Guitouni, 2009	Hauser-Graham-Koerner-Davis, 2004	Dep. of Homeland Security, 2005	
1	Infrastructure and physical security	1	1		1	1	1	5
2	Documentation / Info security	1				1	1	3
3	Cooperation and coordination	1	1		1			3
4	Policy, standards and regulations	1	1				1	3
5	Cargo Security					1	1	2
6	Transit security						1	1
7	Contamination			1				1
8	Disruption			1				1
9	Corruption			1				1
10	Efficiency		1					1
11	Reliability / Robustness		1		1			2
12	Shipment Transparency		1					1
13	Fault tolerance		1		1			2
14	Resilience		1		1			2

Table 6. Global Elements VS Authors

So, from the table above, can be extracted that highlights the global element "Infrastructure and physical security" as the most proposed in the literature analyzed.

Can also be extracted, that in this literature are also especially relevant the Global Elements "Documentation and Info Security", "Cooperation and Coordination" and "Policy, Standards and Regulations".

2.4.4. Conceptual Definition of each Global Element

To determine more precisely the Global Elements resulting of link conceptually the identified elements in the Research Database, has been developed an integrative conceptual definition of each Global Element.

So, although with sometimes quite different denominations and with definitions a little different, many of the elements proposed by the authors have ***big and obvious points in common***.

The process followed to define conceptually each Global Element is as follows:

- Analysis of the definition given by the authors of each element integrated into the Global Element.
- Extraction of the key and basic idea that these elements are intended to convey.
- Development of a conceptual definition integrative taking into account all the definitions and trying to capture the key common idea extracted from all the definitions.

Below are the definitions generated for each Global Element:

1	**Infrastructure and physical security**
2	**Documentation / Info security**
3	**Cooperation and coordination**
4	**Policy, standards and regulations**
5	**Cargo Security**
6	**Transit Security**
7	**Contamination**
8	**Disruption**
9	**Corruption**
10	**Efficiency**
11	**Reliability / Robustness**
12	**Shipment Transparency**
13	**Fault tolerance**
14	**Resilience**

Table 7. Global Elements

1. Infrastructure and physical security

The most used Global Element is “Infrastructure and Physical Security”. Lots of authors speak of it under various designations.
Although the descriptions and definitions given by the authors are slightly different, the latter concept is the same.

All the definitions refer to **the physical elements that make up the Supply Chain (public infrastructure and private facilities and items) and the physical measures used to protect these vital elements of the Supply Chain.**

2. Documentation / Info security

Regarding the elements integrated in this Global Element, the authors also defined in different ways but there are strong and obvious points in common in all these definitions.
All the definitions refer to **the management of the documentation and information accurately and securely throughout the supply chain. Through the improvement and optimization of the management of this documentation and information, is intended to strengthen both the security and efficiency of the Supply Chain.**

So, can be improved both monitoring and security control of the various components (containers, personnel) that run through the Supply Chain.

3. Cooperation and coordination

All the elements included within this Global Element can also be merged conceptually on a common definition.

Thus, all dealing with **the different activities to be performed to obtain a high degree of cooperation and coordination.**

All authors agree on the importance of carrying out actions to facilitate such cooperation and coordination from local to international level between all parties involved in the Supply Chain.

Thus, the authors note that if not carried out these actions, the Supply chain partners can become a source of vulnerability for the own supply chain.

4. Policies, standards and regulations

Several authors stress the importance of the regulation and standardization to improve the security of the Containerized Supply Chain

Thus, although the authors define this concept in different ways, all these definitions can be lumped conceptually.

The authors refer to **the implementation of rules of conduct with respect to different elements of the Supply Chain through legislation, standardization and regulation, as a way to generate an environment favorable to the security of the Supply Chain.**

This requires the existence of national and international organizations, so that regulation can be made at the highest level and to be fully compatible across the entire supply chain.

5. Cargo Security

Conceptually, this element is defined by the authors as **the Procedure to ensure that the cargo to be loaded on the vessel conforms to the cargo information electronically transmitted to the authorities.**

6. Transit Security

Several authors discuss the global element and Transit Security, albeit with different denominations can be defined conceptually as **the procedures to apply at the different elements of the Supply Chain to Ensure that the secure cargo remains in that status as it enters and moves through the Supply Chain**

7. Contamination

Conceptually, this element is defined by the authors as **any form of environmental contamination from untreated waste streams, contamination of the raw material/manufactured product or contamination of surroundings, resulting in hazardous environment for the workers and other people.**

The threat Contamination is assumed a result of accident or terrorist activity and is a threat that affect the assets and the personnel that form part of the Supply Chain.

8. Disruption

Conceptually, this element is defined by the authors as **any form of interruption leading to work halt and it can arise from events of natural disaster, terrorism or accidents.**

So, this element is a threat that affect the assets that form part of the Supply Chain.

9. Corruption

Conceptually, this element is defined by the authors as **the terrorist acts, information hacking or tampering and for this reason is assumed as a result of terrorist activity.**

So, this element is a threat that affect the assets that form part of the Supply Chain.

10. Efficiency

Conceptually, this element is defined by the authors as **the raison d'être of the Supply Chain**. So, **the global container supply chain has evolved primarily to deliver goods more quickly and more cheaply than other modes of transport when volume and mass are taken into account.**

For this reason, **initiatives to improve supply chain security must take into account also the efficiency parameter, trying to improve or at least not worsen it.**

11. Reliability

Several authors discuss this Global element in relation to the security of the Containerized Supply Chain.

The denominations given of this concept by the authors don't match exactly, but conceptually have obvious similarities.

Thus, merging the definitions, can be defined this global element as follows:

For exists Reliability in the Supply Chain, it must behave as expected, retrieving and delivering goods as directed, with a minimum amount of loss due to theft and accident, and providing sustainable value creation under all plausible future scenarios (normal business conditions as well as major disruptions)

12. Shipment Transparency

According to the authors definition, **to obtain a shipment transparency, the goods that flow through a supply chain must be legitimately represented to authorities and must be legal for transport. So, the system should be transparent enough to minimize improper use of the system.**

13. Fault tolerance

Several authors discuss the global element of Fault Tolerance, albeit with different denominations can be obtained a common and inclusive definition.

The concept of Fault Tolerance indicates that the container shipping system should be able to respond to disruptions and failures of isolated components without bringing the entire system to a grinding halt.

In fault-tolerant systems, the surrounding ports and distribution system can compensate when a section of the system is compromised through flexibility or redundancy based capabilities.

14. Resilience

The concept of Resilience is treated by several authors. Integrating their definitions, can be determined precisely what is this important element related to the security of the C.S.C.

So, Resilience is **the ability of the supply chain to return to normal operations after a failure. A supply chain is resilient insofar as it is able to return to normal operating conditions quickly after the failure of one or more components.**

It is the capacity of a system to survive, adapt, and grow in the face of unforeseen changes, even catastrophic incidents

2.4.5. Classification of the Global Elements

In the process of generation of the conceptual definition of the Global Elements, have been identified a clear difference of nature between those Global Elements.

So, have been identified 3 major subgroups in which can be classified the 14 Global Elements.

In this way, have been identified a group of Global Elements relating to all those **basic elements, tools and procedures that define the Security of the C.S.C**. This group of Global Elements, in this project, has been named as ***Tools***.

Another group of Global elements relating to the **possible problems that may affect in a negative way in the operation of the C.S.C**. This group of Global Elements has been named as ***Vulnerabilities***.

And finally, another group of Global Elements relating to all elements that **define the performance of the C.S.C**. This group of elements has been named as ***Performance***.

Classification Global Elements		
	Tools	
	1	Infrastructure and physical security
	2	Documentation / Info security
	3	Cooperation and coordination
	4	Policy, standards and regulations
	5	Cargo Security
	6	Transit security
	Vulnerabilities	
	7	Contamination
	8	Disruption
	9	Corruption
	Performance	
	10	Efficiency
	11	Reliability
	12	Shipment Transparency
	13	Fault tolerance
	14	Resilience

Table 8. Classification of the Global Elements

Thus, the above table indicates how the Global Elements are grouped after being classified through the parameters indicated in the preceding paragraphs.

So, there are a group of 6 Global Elements that, indeed, refer to those basic elements, tools and procedures that define the Security of the C.S.C.:

- Infrastructure and Physical security
- Documentation and Info security
- Cooperation and coordination
- Policy, standards and regulations
- Cargo Security
- Transit Security

Another group of 3 Global Elements relating to the vulnerabilities that may affect the normal operation of the Supply Chain:

- Contamination
- Disruption
- Corruption

And finally a group of 5 Global Elements that define the Performance of the C.S.C.:

- Efficiency
- Reliability
- Shipment Transparency
- Fault Tolerance
- Resilience

3. Proposed and implemented Measures to improve the Security of the C.S.C.

3.1. Introduction

In this section there is a collection of the various Measures proposed and implemented to improve the Security of the C.S.C. identificated in the specialized literature.

There are two distinct levels in terms of these measures. So, there are those that have been referred to as Agreement Measures and those that have been referred to as Technological Measures.

Within the Agreement Measures are included all efforts made regarding the creation of national and international agreements, policies, performance standards, rules and programs.

Within the Technological Measures are included all those technologies used or in developing to improve and strengthen the security of the C.S.C. in the various levels of the supply chain and in different focal areas.

Thus, in the following sections will be collected and explained each of the measures identified in the literature analyzed.

The documents that have been used with more relevance for the collection and analysis of the measures are:

- Evaluating the Security of the Global Containerized Supply Chain [Willis-Ortiz, 2004] (B6)
- Container security. A proposal for a comprehensive code of conduct [Dahlman-Mackby-Alewine, 2005] (B9)
- Maritime Commerce Security Plan for The National Strategy for Maritime Security [Department of Homeland Security, 2005] (C2)
- Protecting the Nation's Seaports: Balancing Security and Cost [Haveman-Shatz, 2006] (C9)
- A Fully Integrated Global Strategic Supply Network [Hauser-Graham-Koerner-Davis, 2004] (B7)
- Transportation security technologies: research and development [Hallowell-Jankowski, 2006] (D0)

- The Container Security Initiative and Ocean Container Threats [Haveman-Jennings-Shatz-Wright, 2007] (C6)

- Security Supply Chain [Dias-Fontana-Mori-Facioli-Zancul, 2008] (D3)

- Higher supply chain security with lower cost: Lessons from total quality management [Lee-Whang, 2003] (D4)

- National and Global Efforts to Enhance Containerized Freight Security [Grillot-Cruise-D'Erman, 2009] (B5)

3.2. Agreement Measures

Through the analysis of the specialized literature, have been identified the Agreement Measures proposed or implemented in the Security of the C.S.C.

As already mentioned in the introduction of this section, in the concept of Agreement Measures are included all those efforts made regarding the creation of national and international agreements, policies, performance standards, rules.

Thus, the Agreement Measures identified in the literature are the following, and will be explained below:

- **Maritime Transportation Security Act of 2002 (MTSA)**
- **Customs-Trade Partnership Against Terrorism (C-TPAT)**
- **Container Security Initiative (CSI)**
- **Operation Safe Commerce (OSC)**
- **Proliferation Security Initiative (PSI)**
- **Megaports Initiative**
- **International Ship and Port Security (ISPS)**

Maritime Transportation Security Act of 2002 (MTSA)

The majority of the post-September 11 laws, rules, regulations, and programs in relation with the Security of the Supply Chain, have their origin in MTSA. Among other steps, the act required [Haveman-Shatz, 2006 (C9)]:

- The creation of national, area, facility, and vessel security plans;
- The identification by federal authorities of vessels and U.S. facilities at risk;
- The creation of vessel and facility response plans;
- Transportation security cards for people who have access to vessels and facilities and crewmember identification cards;

- The creation of rapid-response maritime safety and security teams;
- An assessment of antiterrorism efforts at foreign ports;
- The placement of automatic identification systems on vessels in U.S. waters and a long-range vessel tracking system;
- The development of a program to evaluate and certify secure.
- Systems of international cargo shipment
- A new grant program

These requirements **establish standards and protocols for port security, inspections, and emergency response**. MTSA is the U.S. version of the IMO's International Ship and Port Security. As final goal, the MTSA aims reducing theft and improving incident response at ports and on vessels [Willis-Ortiz, 2004 (B6)].

Customs-Trade Partnership Against Terrorism (C-TPAT)

*The goal of Customs-Trade Partnership against Terrorism (C-TPAT) is to **push responsibility for cargo security onto stakeholders in the supply chain**.*

So, C-TPAT is a **voluntary program** that shippers and carriers can enter to assure at CBP (U.S. Customs and Border Protection) that they **have put into place the best security practices for the packing, tracking, and distribution of all containers and goods en route to the United States**. In return, shippers and carriers **are rewarded through quicker processing and reduced probability of inspection delays** [Willis-Ortiz, 2004 (B6)].

The C-TPAT is a joint U.S. government-business initiative to **build cooperative relationships** that strengthen overall supply chain and border security. C-TPAT recognizes that **U.S. Customs can provide a high level of security only through close cooperation with the ultimate owners of the supply chain**—importers, carriers, brokers, warehouse operators and manufacturers [Dahlman-Mackby-Alewine, 2005 (B9)].

*In C-TPAT, the **Customs Borders and Protection (CBP) has partnered** with the trade community **to implement security criteria and best practices that better protect the entire supply chain**.*

C-TPAT uses the leverage that major importers have over their suppliers to improve security. C-TPAT importers go as far as mandating security procedures in their contracts with foreign suppliers, specifying the security procedures that must be observed before products are loaded and shipped to the United States [Department of Homeland Security, 2005 (C2)].

The **Participants sign an agreement that commits them to conduct a comprehensive self-assessment of supply chain security guidelines** [Dahlman-Mackby-Alewine, 2005 (B9)].

Businesses must apply to participate in C-TPAT and in so doing, **commit to the following actions** [Haveman-Shatz, 2006 (C9)]:

- Conduct a comprehensive self-assessment of supply chain security using the C-TPAT security guidelines, jointly developed by Customs and Border Protection and the trade community. These guidelines encompass **procedural security, physical security, personnel security, education and training, access controls, manifest procedures and conveyance security**.
- Submit a supply chain security profile questionnaire to Customs and Border Protection.
- Develop and implement a program to enhance security throughout the supply chain in accordance with C-TPAT guidelines.
- Communicate C-TPAT guidelines to other companies in the supply chain and work toward building the guidelines into relationships with these companies.

U.S. Customs offers **potential benefits to C-TPAT members**, including [Dahlman-Mackby-Alewine, 2005 (B9)]:

- A reduced number of inspections (reduced border times)
- An assigned account manager
- Access to the C-TPAT membership list
- Eligibility for account-based processes (bimonthly/monthly payments)
- An emphasis on self-policing, rather than customs verifications.

*In summary, C-TPAT **rewards importers who elevate their security measures and make their internal procedures more transparent by offering reduced numbers of border inspections**.*

According to information provided directly by the Customs and Border Protection website (http://www.cbp.gov), the C-TPAT validated 3,469 supply chains in 2008 which is 377 more validations than conducted in 2007.

In addition, since 2003 and as of December 31, 2008, C-TPAT performed 10,367 total initial validations and revalidations.

Container Security Initiative (CSI)

The goal of CSI is to ***make more difficult to transport illegal shipments to the United States by implementing inspections at ports of origin****, thus increasing U.S. security.*

So, the CSI is **a set of measures designed to move the process of container screening toward the beginning of the supply chain** and it includes increased efforts to [Dahlman-Mackby-Alewine, 2005 (B9)]:

- Prescreen containers more effectively
- Make sure that containers are more secure in transit
- Have technology in place at the port of overseas departure for inspection of high-risk containers.

CSI is based on the idea of **pushing U.S. border controls beyond actual U.S. borders and intercepting dangerous cargo before it arrives in the United States**. It is best known for **inspecting high-risk containers at foreign ports** [Haveman-Shatz, 2006 (C9)].

The objective is to ensure that containers headed for the United States are secure before they leave a foreign port. Waiting for the container to arrive at a U.S. destination before inspecting it would probably be too late to prevent a catastrophic result. Thus, the **CSI consists of four core elements** [Dahlman-Mackby-Alewine,2005 (B9)]:

- Using intelligence and automated information to identify and target high-risk containers
- Pre-screening those containers identified as high risk at the port of departure
- Employing detection technology to rapidly pre-screen high-risk containers
- Using smarter tamper-proof containers.

The CSI has quickly expanded to major foreign seaports from which the majority of container shipments to the United States originate.
Through **bilateral agreements**, Customs and Border Protection officers are stationed at foreign seaports where they work with the host government **to identify high-risk shipments before they are shipped to the United States** [Department of Homeland Security, 2005 (C2)].

This innovative program became possible because of [Department of Homeland Security, 2005 (C2)]:

- The availability of advance electronic cargo information.
- Automated tools such as the Automated Targeting System to use that information.
- Non-intrusive inspection technology to efficiently inspect high-risk containers.

- An international community committed to the improvement of maritime security.

The United States has concluded agreements with some 25 ports globally, including Rotterdam, Antwerp, Le Havre, Singapore, and Hong Kong, that provide for U.S. customs officers to be permanently placed at these ports far **and it has offered reciprocity to other countries so that they, too, can station customs officers in U.S. ports for ships bound to their countries (**to date only Japan and Canada have done so) [Dahlman-Mackby-Alewine,2005 (B9)].

However, if all countries reciprocated in the CSI by sending customs officers to each others' ports, there would be an overabundance of officials among the containers. This points to the central deficiency in the CSI: **it consists of bilateral agreements rather than a global arrangement to secure global container transport** [Dahlman-Mackby-Alewine, 2005 (B9)].

Operation Safe Commerce (OSC)

The OSC is **a collaborative effort** between the federal government, business interests, and the maritime industry to **develop and share best practices for the safe and expeditious movement of containerized cargo**. Through a set of grants, OSC is **promoting the testing, evaluation, and fielding of container scanning and tracking technologies** [Willis-Ortiz, 2004 (B6)].

So, Operation Safe Commerce is **an initiative to evaluate the effectiveness of various news technologies and business practices in ensuring international supply chain and container security** [Department of Homeland Security, 2005 (C2)].

*OSC **funds pilot programs** that are meant to enhance and complement other security initiatives, such as C-TPAT and CSI, by testing the new technologies and business processes.*

The programs are used to identify vulnerabilities in the supply chain and develop improved methods for ensuring the security of the C.S.C. entering and leaving the United States. Those security techniques that prove successful under the program are to be recommended for implementation in system-wide [Dahlman-Mackby-Alewine,2005 (B9)].

In the programs, the containers are fitted with the new technologies and treated with the new business processes, and are exposed to actual shipping conditions. They also are monitored for logistics and security anomalies.

For a project to be funded, it must accomplish one or more of the following tasks to secure the supply chain [Haveman-Shatz, 2006 (C9)]:

- Validate security at the point of origin, to include the security of the shipment itself and the information that describes it.
- Secure the supply chain from the point of origin to its final destination and all the points in between.
- Monitor the movement and integrity of the cargo while in transit using available technology.

Has already been initiated a $58 million joint pilot program in Seattle, Los Angeles and New York ports, involving collaboration between industry, ports and local, state and federal governments [Dahlman-Mackby-Alewine,2005 (B9)].

Proliferation Security Initiative (PSI)

The Proliferation Security Initiative (PSI) is **a global effort that aims to stop the proliferation of weapons of mass destruction, their delivery systems and related material** [Department of Homeland Security, 2005 (C2)]**.**

The PSI is focused on **pre-emptive interdiction**: it seeks to allow ships, aircraft and vehicles suspected of carrying WMD-related materials to be detained and searched as soon as they enter member countries' territory, territorial waters, or airspace [Dahlman-Mackby-Alewine,2005 (B9)].

*For that reason, states and non-state actors concerned about this proliferation, have developed **partnerships and are cooperating in interdiction exercises**.*

To avoid the violation of international law (for example the Law of the Sea), **bilateral arrangements** are made to board vessels and aircraft and/or guide these to participating States [Dahlman-Mackby-Alewine,2005 (B9)].

This effort shows the clear commitment of the international community that the global transportation system will not be used to support weapons of mass destruction proliferation.

Several exercises have been held, which also have the function of deterring the transport of such materials. Currently (01-01-2011) the PSI has 98 states participating countries, among which highlight Argentina, Australia, Canada, Denmark, France, New Zealand, Norway, Poland, Portugal, Russia, Singapore, Germany, Greece, Italy, Japan, Republic of Korea, Spain, Turkey, United Kingdom and the United States, as a members of the Operational Experts Group.

Megaports Initiative

The Megaport Initiative began in 2003 as **a cooperative effort between the U.S. and the host countries to add radiation detection capabilities to exterior key ports**. This will make it possible to screen cargo for nuclear and radiological weapons of mass destruction [Dahlman-Mackby-Alewine,2005 (B9)].

The U.S. supports the installation of the equipment, training and maintenance, while equipment is operated by host country personnel.

The Megaports Initiative will also provide training to appropriate law enforcement officials to provide them with the technical means to deter, detect, and interdict illicit trafficking in nuclear and other radioactive materials. This expertise is based on years of experience equipping international seaports, airports and vehicle crossings with radiation detection and related communications equipment and response systems [Department of Homeland Security, 2005 (C2)].

Since the start of the Megaports Initiative in fiscal year 2003, has been completed installations at 27 ports to date (2010) in: Bahamas, Belgium, Colombia, Dominican Republic, Greece, Honduras (SFI Port), Israel, Jamaica, Malaysia, Mexico, the Netherlands, Oman (SFI Port), Pakistan (SFI Port), Panama, the Philippines, Portugal, Spain, Singapore, South Korea (SFI Port), Sri Lanka, Taiwan, Thailand, and the United Kingdom (SFI Port). Implementation is underway at 16 ports in the following locations: Bangladesh, China, Djibouti, Dubai-United Arab Emirate, Egypt, Japan, Jordan, Kenya, Lebanon, Malaysia, Mexico, Panama, and Spain.

The Megaports Initiative seeks to equip 100 seaports with radiation detection systems by 2015, scanning approximately 50 percent of global maritime containerized cargo.

International Ship and Port Security (ISPS)

International Ship and Port Security (ISPS) **provides mandatory security requirements for governments, port authorities and shipping companies, as well as voluntary guidelines about how to meet the new security requirements** [Dahlman-Mackby-Alewine,2005 (B9)].

The ISPS is the germ of initiatives in relation to the Security of the C.S.C. at international level, as well as the MTSA is at the U.S. level.

Under the ISPS, the operators of seaports must conduct vulnerability assessments and develop and submit for approval security plans for their ports. The plans must meet the threats against varying security levels (normal, medium and high threat situations) that would be set by the contracting Government [Dahlman-Mackby-Alewine, 2005 (B9)].

The seagoing vessels are now required to undergo a vulnerability assessment to develop and implement a security plan, including a provision for security officers, **and to install an Automatic Identification Systems** on board which can be interrogated. The imposed security level creates a link between a ship, the port facility, and the threat situation [Dahlman-Mackby-Alewine,2005 (B9)].

The Code does not specify specific measures that each port and ship must take to ensure the security of the facility against terrorism because of the many different types and sizes of these facilities. Instead it outlines “a standardized, consistent framework for evaluating risk, enabling governments to offset changes in threat with changes in vulnerability for ships and port facilities” (ISPS Code)

For ships the framework includes requirements for (ISPS Code):

- Ship security plans
- Ship security officers
- Company security officers
- Certain onboard equipment

For port facilities, the requirements include (ISPS Code):

- Port facility security plans
- Port facility security officers
- Certain security equipment

In addition the requirements for ships and for port facilities include (ISPS Code):

- Monitoring and controlling access

- Monitoring the activities of people and cargo
- Ensuring security communications are readily available

In October 2003 the EU required the mandatory adoption by EU Member States of many of the voluntary measures of the ISPS code. The new code came into effect on 1 July 2004 and applies to ships larger than 500 gross tons.
In order to prepare for this development, a public/private partnership including government, port authorities, ship owners, industries, and unions produced a manual for ship and port security assessment given to the IMO, EU and the World Bank.

3.3. Technological Measures

Through the analysis of the specialized literature, have been identified the Technological Measures proposed or implemented regarding the Security of the C.S.C.

As already mentioned in the introduction of this section, in the concept of Technological Measures are included all these technologies used or under development to improve and strengthen the Security of the C.S.C. at various levels in the supply chain and in different focal areas.

Thus, the Technological Measures identified are the following, and it will be explained below:

- **Antitamper Seals Technologies**
- **Sensor Technologies**
- **Radio-Frequency Identification Technologies**
- **Non-Intrusive Inspections Technologies: X-Ray and Gamma-Ray Scanning**
- **WMD Remote Monitoring Technologies: Radiation Pagers and Portal Sensors**
- **Automated Targeting Technologies**
- **Authentication Technologies: Access Control and Biometrics**

Antitamper Seals Technologies

Antitamper seals are ***a broad set of technologies that detect and indicate when an unauthorized party has opened a container.***

They range from electronic devices that record when and by whom containers are opened, until proposals to mark containers with unique “fingerprints” that are modified when a container is opened or compromised. Even the simplest antitamper seals, such as high-quality cable seals, are considerably more expensive than common bolt seals [Willis-Ortiz, 2004 (B6)].

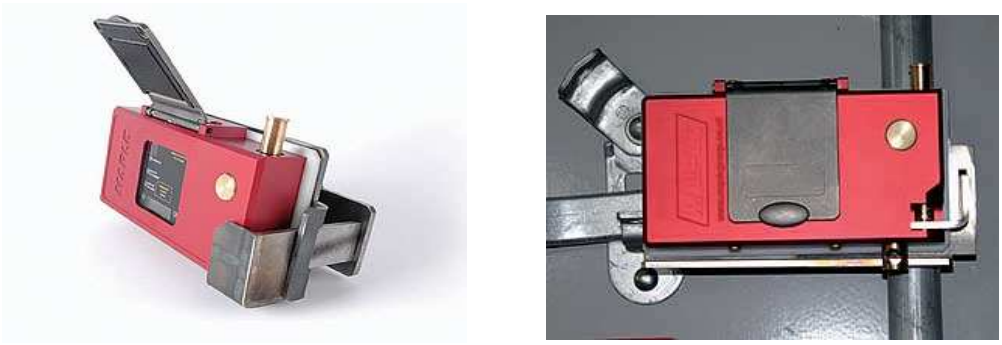

Image 2. Examples of Antitamper Seals Technologies

They can be used in combination with RFID technology to optimize its functionality, making use of the advantages of RFID explained in later sections of this project.

Seals should be tamperproof and should carry a unique identification that cannot be forged easily. The procedures and authorities to apply seals must be clearly defined. There is a need to establish some minimal standards. The World Customs Organization has a high-level group to address standardization in container transport, including seals. The International Standardization Organization (ISO) is also reportedly preparing an international standard for seals [Dahlman-Mackby-Alewine, 2005 (B9)].

A number of institutions and companies (Boeing, QinetiQ, Philips, Joint Research Center of the European Commission, and others) have instituted research and development programs on these security technological measures, including also smart seals and "brilliant containers" with built-in detectors.

Sensors Technologies

The containers with sensors **can detect intrusion and other actions that might breach security of the container and, detect radiological materials, or specified chemical or biological agents**. Sensors can either produce real time alerts, or communicate with a secure device to record events and when they occurred for later recovery. [Dahlman-Mackby-Alewine,2005 (B9)]

Image 3. Sensor to detect flammable chemical elements

Such sensors are being developed and tested. If such devices prove to be reliable and cost effective, they could become an important part of the solution to the problem of container security.

Radio-Frequency Identification Technologies

RFID technologies allow shippers and carriers to track cargo while it is within the container shipping system. The devices can record and transmit information about a container's origin, destination, contents, or processing history [Willis-Ortiz, 2004 (B6)].

RFID systems are typically **designed to transmit information about cargo when the shipment passes salient portals, such as entry or exit from a port or when the cargo is loaded or unloaded from a ship** [Willis-Ortiz, 2004 (B6)].

*RFID devices **are available as both passive and active technologies**. **Passive devices** transmit only when are in the presence of a reader that provides the required power. They have ranges up to a few meters and are typically used to track shipments at the unit or carton level. **Active devices** are battery powered and can transmit over distances as far as 100m or more. Thus, active devices have been applied to tracking cargo at the container and pallet levels.*

Image 4. Examples of different elements of the RFID Technologies
(a-passive Tag; b-active Tag; c-RFID reader)

Advantages of using RFID [Hauser-Graham-Koerner-Davis, 2004 (B7)]:

- RFID coupled with the right infrastructure, will provide at business processes real time information to feed future adaptive supply networks.
- RFID has significant potential to reduce handling costs, improve information accuracy and visibility, and improve the planning of inventory required to support both business requirements.
- RFID has significant security applications to aid current and future initiatives in tracking the handling of freight and cargo.

- As RFID costs reduce with volume of usage it will be progressively extended from supply chain containers and packages, to high value / secure items and eventually to low value items.
- Devices will be generational and develop toward the emerging technologies of smart dust and intelligent devices over the next 5 to 10 years.

Non-Intrusive inspections Technologies: X-Ray and Gamma-Ray Scanning

The **Non-Intrusive inspections technologies, as X-Ray and Gamma-Ray technologies allow to visualize for inspections of a container' contents, obviating the need to open it and inspect the contents physically** [Willis-Ortiz, 2004 (B6)].

Image 5. Fix X-ray Scanner

Image 6. Portable Gamma-ray Scanner

These technologies are used to scan containers for misrepresented or illegal shipments.

Currently, between 5 and 6 percent of containers are inspected either intrusively or nonintrusively. Application has been limited because of the cost of the machines, the lack of space at ports, the time required to scan, and the relatively high false-positive rates that result from the inconclusive visualizations that the technologies provide [Willis-Ortiz, 2004 (B6)].

The X-ray and Gamma-Ray machines reveal much information about the contents of containers and are being used in some large ports.

The principle of operation of X-ray and Gamma-Ray equipment for inspection is relatively simple. A Ray generator, which is usually an electron tube in conventional small-size equipment and a particle accelerator in large-size equipment, is energized by a power circuit, thus generating X or Gamma rays. The object is then traversed by the ray beam, and in function of its content density, it absorbs more or less energy

from the beam, and the rays that traversed this object hit a column of photosensor diodes, sensitive to the rays, which emit an electric pulse.
Analog to digital converters change these pulses in signals that are processed and finally converted in a digital image on a monitor. This radioscopic image shows the content of the object inspected [Dias-Fontana-Mori-Facioli-Zancul, 2008 (D3)].

WMD Remote Monitoring Technologies: Radiation Pagers, Portal Sensors

Nuclear material, especially material that might be part of a nuclear weapon or is intended to be used to produce a nuclear weapon, is of special concern.

Technologies for the remote sensing of weapons of mass destruction (WMD) are under development and are technologies that allow detect **weapons of mass destruction, their delivery systems and related material** [Department of Homeland Security, 2005 (C2)].

Radioactive materials give off neutrons, gamma rays and heat, which, in principle, allows them to be detected. However, it is difficult to generalize what can be detected in practice, since this depends strongly of [Dahlman-Mackby-Alewine, 2005 (B9)]:

- The nature and quantity of the radioactive material.
- The others materials present that can act as shielding.
- The sensitivity of the monitoring device.

In the WMB Remote monitoring devices, highlight [Willis-Ortiz, 2004 (B6)]:

- Radiation pagers: are portable devices that can be used to detect nuclear or radiological weapons as inspectors move throughout a port or vessel.
- Portal sensors: are designed to detect weapons of mass destruction as containers enter and leave ports or vessels.

Image 7. Radiation Pager

Image 8. Portal Sensor

These and other remote-monitoring devices to detect weapons of mass destruction and other illegal cargo are in early development. However, capabilities are expected to improve over time and possibly be integrated with existing security technologies.

One problem with all of these sensors and detectors is that they tend to produce some false alarms, due to background radiation and other innocent emissions from legitimate cargo [Dahlman-Mackby-Alewine, 2005 (B9)].

Nevertheless, a more widespread use of the detectors already available today would certainly improve the security of the container system and work as a deterrent. For the future, research is needed, including the use of test beds, to develop faster, more reliable and affordable detectors of WMD.

Automated Targeting Technologies

The Automated Targeting Technologies **are rules-based analytical tools that uses cargo information, law enforcement information, and historical data, along with information from the intelligence community, to assess the risk posed by the cargo** [Department of Homeland Security, 2005 (C2)].

The availability of cargo information much earlier in the process created an environment in which the risk assessment of cargo takes place even before the cargo was loaded on vessels at foreign ports. This system supports the assessment of all types of maritime cargo and is not limited to containerized cargo [Lee-Whang, 2003 (D4)].

Benefits of AT Technologies included paperless processing, elimination of repetitive trips to the local customs house, reduction of cargo dwell time, and increased customs compliance [Dahlman-Mackby-Alewine, 2005 (B9)].

For example, the 24-hour rule of the Customs and Border Protection, require the shipping manifest information 24 hours before the container is loaded for destination in a harbor of the United States.

The AT Technologies provides automatic 24-hour manifest status updates and generates manifest reports by container, voyage, bill of lading, date, unlading port, shipper/consignee, and more. Through a customs message-tracking interface, manifest status information is available via automatic email notifications [Dahlman-Mackby-Alewine, 2005 (B9)].

Access Control and Biometrics

Access control **is one layer of physical security implemented at transportation facilities to ensure that only authorized individuals gain access to secured areas** [Hallowell-Jankowski, 2006 (D0)].

Typically this involves some form of credential (ID badge) and electro-mechanical door and gate controls.

Image 9. Gate control

However, such systems are vulnerable to lost or stolen ID cards. For this reason, nowadays, it has been evaluated the integration of **biometric devices** into access control systems in realistic operational environments.

Image 10. Fingerprint biometric device

Image 11. Ocular biometric device

4. Analysis of the Measures to improve the Security of the C.S.C.

4.1. Introduction

In the following sections will be analyzed each of the Agreement and Technological Measures identified.

To do this, in a first phase has been analyzed for each measure identified, which basic elements of the Security of the C.S.C. are affected. These basic elements have been identified in this project and have been denominated as the global elements "Tools".

In a second phase has been analyzed for each measure identified, how it affects at the different elements of Performance of the C.S.C. These elements have been identified in this project and have been denominated as the global elements "Performance".

4.2. Analysis of the Measures VS global elements "Tools"

4.2.1. Analysis summary tables

Following, are the analysis summary tables of the Agreement and Technological measures regarding the global elements "Tools".

These tables can be found in its original format in the Excel file named "ANNEX 3. Analysis of the Measures".

			Agreement Measures						
			MTSA	**C-TPAT**	**CSI**	**OSC**	**PSI**	**MI**	**ISPS**
Tools	1	**Infrastructure and physical security**	X	x	x	x	x	x	X
	2	**Documentation / Info security**	X			x			
	3	**Cooperation and coordination**	X	x	x	x	x	x	
	4	**Policy, standards and regulations**	X						X
	5	**Cargo Security**	X	x	x	x			X
	6	**Transit security**	X	x	x	x			X

Table 9. Analysis summary table "Agreement Measures VS Tools"

In the analysis table Agreement Measures VS Tools, have been indicated the basic elements to which are addressed and affect each of the Agreement measures. Due to the wide range and dispersion of the proposals incorporated in these measures, have been determined two levels of involvement.

In this way, it has been marked with intense orange those elements that are affected directly and with greater intensity for each measure. And it has been marked with a less intense orange those elements that can potentially be improved by influence of measures but require further actions alien to the actions determined by the Measure of agreement.

			Technological Measures						
			TM-1	**TM-2**	**TM-3**	**TM-4**	**TM-5**	**TM-6**	**TM-7**
Tools	1	**Infrastructure and physical security**				x	x		X
	2	**Documentation / Info security**			x			x	
	3	**Cooperation and coordination**							
	4	**Policy, standards and regulations**							
	5	**Cargo Security**	x	x	x				X
	6	**Transit security**	x	x	x	x	x		X

Table 10. Analysis summary table "Technological Measures VS Tools"

Technological Measures	Code
Antitamper Seals Technologies	**TM-1**
Sensor Technologies	**TM-2**
RFID Technologies	**TM-3**
Non-Intrusive Inspections	**TM-4**
WMD Remote Monitoring Technologies	**TM-5**
Automated Targeting Technologies	**TM-6**
Authentication Technologies	**TM-7**

In the analysis table Technological Measures VS Tools, are indicated similarly to which basic elements of the security of the C.S.C. are addressed and affect each Technological Measure. In this case, they are much more concrete measures that the Agreement measures.

4.2.2. Analysis of the Agreement Measures

In the next section will be analyzed in detail each of the Agreement measures regarding the elements "Tools", developing broadly the information synthesized in the Analysis summary tables. Thus, from the definition given for each "Tool" and of the information identified in the literature on each agreement measure, the results of the analysis are as follows:

Maritime Transportation Security Act of 2002 (MTSA)

The requirements defined in the MTSA have provided a conceptual basis for the development of the most of the agreements and policies relating to the Security of the C.S.C.

Thus, the MTSA mainly affects the supply chain tool called **"Policy, standards and Regulations"** as it has been the germ of many other initiatives.

The MTSA is a broad agreement measure and its requirements will require execute actions by different stakeholders of the Supply Chain that will affect all the basic elements of the Security of the C.S.C.

Customs-Trade Partnership Against Terrorism (C-TPAT)

The C-TPAT is a voluntary program that recognizes that **U.S. Customs can provide a high level of security only through close cooperation with the ultimate owners of the supply chain** [Dahlman-Mackby-Alewine, 2005 (B9)].

Thus, the C-TPAT influences and affects mainly on ***"Cooperation and Coordenation"*** *as a way to improve the security of the C.S.C.*

The goal of Customs-Trade Partnership against Terrorism (C-TPAT) is to ***push responsibility for cargo security onto stakeholders in the supply chain***.

For this, the C-TPAT offers **to its members rewards, with potential benefits, at the importers who elevate their security measures and make their internal procedures more transparent.**
So, the **Participants sign an agreement that commits them to conduct a comprehensive self-assessment of supply chain security using the C-TPAT guidelines** [Dahlman-Mackby-Alewine, 2005 (B9)].

Through this self-assessment, the members using the C-TPAT guidelines (indicated in the point *3.2. Agreement Measures*), can potentially improve and influence in many basic elements of security. So, not directly but through their members, the C-TPAT also affects in the **"Infrastructure and Physical Security"** and in the **"Cargo"** and **"Transit Security"**.

Container Security Initiative (CSI)

In the CSI, through **bilateral agreements**, Customs and Border Protection officers are stationed at foreign seaports where they work with the host government **to identify high-risk shipments before they are shipped to the United States** [Department of Homeland Security, 2005 (C2)].

Thus, the CSI with their bilateral agreements, primarily promotes the **"Cooperation and Coordination"** between the U.S. and other nations in the world.

And through its fundamental requirements (indicated in the point *3.2. Agreement Measures*), the CSI has also a strong impact in the **"Infrastructure and Physical Security"** and in the **"Cargo"** and **"Transit Security"**.

Operation Safe Commerce (OSC)

The OSC is **a collaborative effort** between the federal government, business interests, and the maritime industry to **develop and share best practices for the safe and expeditious movement of containerized cargo** [Willis-Ortiz, 2004 (B6)].

Thus, the CSI mainly is intended to promote an atmosphere of **"Cooperation and Coordination"** between different stakeholders in the Security of the Supply Chain, developing these new technologies and best practices.

As previously mentioned in the point *3.2. Agreement Measures*, to can found a project, it must accomplish one or more of the following tasks to secure the supply chain [Haveman-Shatz, 2006 (C9)]:

- Validate security at the point of origin, to include the security of the shipment itself and the information that describes it.
- Secure the supply chain from the point of origin to its final destination and all the points in between.
- Monitor the movement and integrity of the cargo while in transit using available technology.

So, indirectly, through these projects of evaluation and develop of new technologies and best practices, can be improved many other basic elements with the integration of these new technologies and best practices in the Supply Chain system: **"Infrastructure and Physical Security"**, **"Documentation / Info Security"**, **"Cargo Security"** and **"Transit Security"**.

Proliferation Security Initiative (PSI)

The PSI also has an impact mainly on **"Cooperation and Coordination"** to improve the security of the C.S.C. This impact in the "Cooperation and Coordination" is done specifically through the **develop of interdiction exercises between the members of the Initiative**, to improve the identification and interception of transports suspected of carrying WMD-related materials before they reach the ports of the states members of the program.

These actions of interception of Weapons of Mass Destruction before they reach at port and they cause a catastrophe in the port or inside of the nation, also affect favorably the improvement of the **"Infrastructure and physical security"**, adding this detection and interception as an additional physical tool of security and thereby protecting the infrastructure and other basic physical elements of the supply chain system.

Megaports Initiative

As the Proliferation Security Initiative, the Megaports Initiative also affects the **"Cooperation and Coordination"** between the United States and countries of origin of goods, identifying WMD and related materials but in this case in the ports of origin, increasing the screening capacity of such materials in these ports.

These screening activities at the port of origin of Weapons of Mass Destruction, greatly improve the **"Infrastructure and physical security"** of the Supply Chain, improving the physical tools to detect and moving the danger of nuclear elements away from the port of arrival.

International Ship and Port Security (ISPS)

Like the MTSA for the United States, the ISPS mark the conceptual basis for the development of most of the agreements and policies relating to Security of the C.S.C. at the international level and its requirements have been adopted as required by the members of the European Union.

Thus, the ISPS affects mainly the tool of the Supply Chain named **"Policy, standards and Regulations"** as it provides a basis for action to other actions aimed towards the Security of the C.S.C. at international level.

Among the requirements in the ISPS, are proposed actions to be taken by various actors in the supply chain, which potentially can improve several key elements regarding the Security of the C.S.C.: **"Infrastructure and physical security"**, **"Cargo Security"** and **"Transit Security"**.

These requirements have already been mentioned in the point *3.2. Agreement Measures*, and are as follows:
For ships the framework includes requirements for (ISPS Code):

- Ship security plans
- Ship security officers
- Company security officers
- Certain onboard equipment

For port facilities, the requirements include (ISPS Code):

- Port facility security plans
- Port facility security officers
- Certain security equipment

In addition the requirements for ships and for port facilities include (ISPS Code):

- Monitoring and controlling access
- Monitoring the activities of people and cargo
- Ensuring security communications are readily available

4.2.3. Analysis of the Technological Measures

In the next section will be analyzed in detail each of the Technological measures in relation to the global elements "Tools". Thus, from the definition given for each "Tool" and the information identified in the literature about each Technological measure, the result of the analysis is as follows:

Antitamper Seals Technologies

This technology clearly affects the security of the Supply Chain, concretely of the containers, both in the procedures of **loading the goods into containers and sealing**, as in the procedures **to ensure that the goods remain safe on the way towards their destination**.

Thus, the "Antitamper container seals" are aimed at improving the **"Cargo Security"** and the **"Transit Security"** in the Containerized Supply Chain, because the Antitamper

seals create an additional physical barrier in the containers, hindering that they are tampered or in case they are tampered in route can be identified clearly this manipulation.

Sensor Technologies

Although with greater accuracy and range of features, the Container Sensors also aim to optimize the containers security, both in their **process of loading and sealing as in the transportation to the destination**.

Therefore, the Container Sensors are also aimed at improving the **"Cargo Security"** and the **"Transit Security"** in the C.S.C., facilitating the detection of dangerous and illegal components in the containers during their filling and also detecting possible manipulations of the content in the transport to the port of destination.

Radio-Frequency Identification Technologies

The Radio-Frequency Identification (RFID) is one of the most promising technologies of future in the improving of the Security of the C.S.C.

In addition, as discussed in later sections, it is also a technology that decisively influences in the performance and efficiency improvement of the Supply Chain.

Thus, as already is mentioned in paragraph *3.3. Technological Measures* of this project, the advantages of using RFID are substantial and regarding with the Security of the C.S.C., are focused mainly in **track the handling of cargo while it is moving through the various steps of container shipping system.**

Thus, RFID technology is focused mainly on optimizing the security of cargo from it is deposited in a container, through all the way, until it arrives at destination. That is, it focuses on improving the **"Cargo Security"** and **"Transit Security"** of the Supply Chain, improving the track of the handling of cargo while it is moving through the various steps of container shipping system. This helps to prevent and detect tampering and misrouting of the cargo, and can also detect the location where they have occurred.

In addition, the use of RFID allows managing information and documentation from the containers in a way more accurate and secure. Therefore, the RFID also influence with importance in the **"Documentation and Info security"**, recording and transmitting

accurate and secure information about a container's origin, destination, contents, or processing history, and this information can be used to detect risks and breaks in the security of the Supply chain.

Non-Intrusive Inspections technologies: X-Ray and Gamma-Ray Scanning

The Non-Intrusive Inspections **allow to visualize for inspections of a container' contents, obviating the need to open it and inspect the contents physically**.

These technologies affect the improvement of the basic element **"Infrastructure and physical security"**, strengthening the physical tools to improve security at ports and nexus of the Supply Chain.

Thus, these technologies improve the security of the physical facilities where it is developed an important part of the supply chain, **allowing to inspect in a way more in depth and less invasive the containers arriving at the facilities,** looking dangerous or prohibited components without opening the containers and more effectively than with conventional inspections.

Furthermore, it can improve the **"Transit Security"**, since these technologies can be used to verify **the integrity of the containers and the legality of the goods inside on a non-invasive way**, while they are traveling through the supply chain system using the X-ray and Gamma-ray scanning portals.

WMD Remote Monitoring Technologies

The WMD Remote Monitoring Technologies allow detect **weapons of mass destruction, their delivery systems and related material.**

Similar at the Non-Intrusive Inspections, these technologies allow detect in a non-invasive and remote way, in that case the existence of radioactive elements in the supply chain.

They can be installed fixed in ports or on the connecting links of the Supply Chain (portal sensors) or, consist in portable devices (radiation pagers).

Thus, these technologies can improve the **"Infrastructure and physical security"** assisting the detection of radioactive elements in ports scanning the containers with Portal Sensors, or through mobile sensing elements they can influence the **"Transit**

Security", detecting possible radioactive elements inside containers being transported on vessels using the radiation pagers.

Automated Targeting Technologies

The AT Technologies are focused clearly on improving the security of the C.S.C., by **optimizing the management of the information available regarding the transport of goods in container**.

This technology clearly influences in the improvement of the basic element **"Documentation / Info Security"** allowing to centralize digitally all the information available regarding the transport of goods in container (cargo information, historical data, law enforcement information), and expediting secure transmission of it, to easily identify security risks along the supply chain.

For example, for the 24-hour rule, the AT Technologies provide automatic 24-hour manifest status updates and generate manifest reports by container, voyage, bill of lading, date, unlading port, shipper/consignee, and more. Through a customs message-tracking interface, manifest status information is available via automatic email notifications [Dahlman-Mackby-Alewine, 2005 (B9)].

Authentication Technologies: Access Control and Biometrics

The Authentication Technologies **are one layer of physical security implemented at transportation facilities to ensure that only authorized individuals gain access to secured areas** [Hallowell-Jankowski, 2006 (D0)].

Thus, these technologies increase the security of the infrastructure and facilities that are part of the system of the containerized supply chain, to limiting and controlling the access of people to sensitive areas of these facilities, using credentials and electromechanical doors and gate controls or, biometrics devices. Therefore, this technology is aimed at improving the **"Infrastructure and physical security"** of the Supply Chain.

Moreover, by limiting access to only authorized persons, is also increased the security in cargo loading procedures in the containers (**"Cargo Security"**), reducing the possibility that someone outside of the charging procedure can access to the cargo area and manipulate the contents of the containers.

Also is increased the security in the process of transporting these containers to their destination (**"Transit Security**), reducing the possibility that someone outside can access to the area of the containers while they are being transported to their destination.

4.2.4. Conclusions of the Analysis of the Measures VS "Tools"

After analyze in detail each agreement and technological measure in relation with the elements "Tools", has carried out a review of the analysis summary tables, in order to extract conclusions about:

- To which elements called "Tools" these measures are directed mainly?
- What elements are less covered?
- What measures cover a larger number of elements?
- …

			Agreement Measures						
			MTSA	**C-TPAT**	**CSI**	**OSC**	**PSI**	**MI**	**ISPS**
Tools	1	**Infrastructure and physical security**	X	x	x	x	x	x	x
	2	**Documentation / Info security**	X			x			
	3	**Cooperation and coordination**	X	x	x	x	x	x	
	4	**Policy, standards and regulations**	X						X
	5	**Cargo Security**	X	x	x	x			X
	6	**Transit security**	X	x	x	x			X

Table 11. Analysis summary table "Agreement Measures VS Tools"

Thus, reviewing the table of Agreement measures VS Tools can be extracted various conclusions:

- The most worked element for the Agreement measures is clearly the "Cooperation and Coordination" between the different stakeholders in the supply Chain.
- The basic element less covered by the Agreement measures is "Documentation and Info Security". Any Agreement initiative deals with the importance that it deserves the security of this element of the Supply Chain that is becoming increasingly basic in the functioning of this Supply Chain, with a growing dependency on the information.
- Highlights the MTSA by the extent of its proposed actions touching with more or less significance all the basic elements related to the security of CSC. The MTSA is the germ of all the other initiatives about this topic emerged in the

United States. For this reason has been highlighted “Policy, standards and regulations”, as the element that it affects with more importance.

- The ISPS is the germ of initiatives in relation to the Security of the C.S.C. at international level, as well as the MTSA is at the U.S. level. For this reason also emphasizes the "Policy, standards and regulations ".
- Highlights the CSI, like an initiative which is aimed strongly at improving many basic elements of the CSC Security. The CSI consists in agreements between different parties to develop research programs of new technologies for improving the CSC Security. So, it increases strongly the “Cooperation”, but also other basic elements of the CSC Security, by the new technologies developed.

			Technological Measures						
			TM-1	**TM-2**	**TM-3**	**TM-4**	**TM-5**	**TM-6**	**TM-7**
Tools	1	**Infrastructure and physical security**				x	x		x
	2	**Documentation / Info security**			x			x	
	3	**Cooperation and coordination**							
	4	**Policy, standards and regulations**							
	5	**Cargo Security**	x	x	x				x
	6	**Transit security**	x	x	x	x	x		x

Table 12. Analysis summary table “Technological Measures VS Tools”

Technological Measures	Code
Antitamper Seals Technologies	**TM-1**
Sensor Technologies	**TM-2**
RFID Technologies	**TM-3**
Non-Intrusive Inspections	**TM-4**
WMD Remote Monitoring Technologies	**TM-5**
Automated Targeting Technologies	**TM-6**
Authentication Technologies	**TM-7**

Reviewing the table of Technological Measures VS Tools can be also extracted various conclusions:

- The basic elements to which are more widely addressed the technological measures are the "Transit Security", followed by the "Cargo Security ". That is because most of the technological measures are focused only in the containers, on their security in the filling and sealing, and their security in the transport to the port of destination.
- The elements less covered by the technical measures are "Cooperation and Coordination" and “Policy, standards and Regulations”. There are no technological measures to improve these basic elements. In fact this is logical,

because these two elements by their nature and definition should be improved by the Agreement measures.

- Highlight the RFID and the Authentication Technologies, such as the measures that positively affect at a greater number of basic elements.
- Finally, the Automated Targeting Technologies is the technological measure identified that covers a smaller number of elements, affecting only to improve the "Documentation and Info Security". However, this technological measure is important, because the element "Documentation and Info Security" is the one unless covered by both the Agreement measures such as by the technological measures.

4.3. Analysis of the Measures VS global elements "Performance"

4.3.1. Analysis summary tables

Following, are displayed the analysis summary tables of the agreement and technological measures regarding the global elements "Performance".

These tables can be found in its original format in the Excel file named "ANNEX 3. Analysis of the Measures".

			Agreement Measures						
			MTSA	**C-TPAT**	**CSI**	**OSC**	**PSI**	**MI**	**ISPS**
Performance	1	**Efficiency**	-	+	=	-	-	-	-
	2	**Reliability**	+	+	+	+	=	=	+
	3	**Shipment Transparency**	+	+	+	+	+	+	=
	4	**Fault tolerance**	+	=	=	=	=	=	+
	5	**Resilience**	+	=	=	=	=	=	+

Table 13. Analysis summary table "Agreement Measures VS Performance"

			Technological Measures						
			TM-1	**TM-2**	**TM-3**	**TM-4**	**TM-5**	**TM-6**	**TM-7**
Performance	1	**Efficiency**	-	-	+	-	-	+	-
	2	**Reliability**	+	+	+	=	=	=	+
	3	**Shipment Transparency**	=	+	+	+	+	+	=
	4	**Fault tolerance**	=	=	+	=	=	=	=
	5	**Resilience**	=	=	+	=	=	=	=

Table 14. Analysis summary table "Technological Measures VS Performance"

Technological Measures	Code
Antitamper Seals Technologies	**TM-1**
Sensor Technologies	**TM-2**
RFID Technologies	**TM-3**
Non-Intrusive Inspections	**TM-4**
WMD Remote Monitoring Technologies	**TM-5**
Automated Targeting Technologies	**TM-6**
Authentication Technologies	**TM-7**

Both for the Agreement Measures, and for the Technological Measures, the analysis process followed regarding the Performance elements has been the same: For each element of Performance has been identified if they are increased (+), reduced (-) or not affected (=) for each Measure.

4.3.2. Analysis of the Agreement Measures

In the next section will be analyzed in detail each of the agreement measures regarding the global elements "Performance". Thus, from the definition given for each "Performance" and the information identified in the literature about each measure of agreement, the results of the analysis are as follows:

Maritime Transportation Security Act of 2002 (MTSA)

None of MTSA's requirements clearly help improve the **"Efficiency"** of the supply chain. In fact, the shipping industry has expressed some concern that its measures will increase shipping costs [Willis-Ortiz, 2004 (B6)].
This is because the implementation of these requirements involves a possible financial effort required to purchase machinery and a possible increase in the processing time of containers, by increasing the number of security procedures (inspections, paperwork, more complex and stringent business practices.

However, the proposals outlined by the MTSA, in terms of creating security plans at different levels of the supply chain, encourage *the retrieving and delivering of goods as directed, with a minimum amount of loss due to shrinkage, tampering, terrorist attack or accident* [Willis-Ortiz, 2004 (B6)]. Thus, the MTSA positively fortifies the **"Reliability"** of the Supply Chain, through its proposed security plans.

Among the actions proposed by the MTSA also highlight those to improve the tracking of containers and control of personnel who have access for these containers, and

other similar actions. The execution of these proposed actions also influences in the improvement of the **"Shipment Transparency"** of the Supply Chain, helping to make a better tracking of containers, helping with its requirements to ensure a greater control over what there is in the containers.

In addition, through the execution of the proposed Response and Disaster Plans and Rapid-response security teams, the MTSA also can significantly improve the **"Fault Tolerance"** and the **"Resilience"** of the Supply Chain.

Customs-Trade Partnership Against Terrorism (C-TPAT)

The C-TPAT can clearly increase the **"Efficiency"** of the Supply Chain, *because its shippers and carriers members* ***are rewarded through quicker processing and reduced probability of inspection delays*** [Willis-Ortiz, 2004 (B6)]**.**

Also through its guidelines (indicated in the point *3.2. Agreement Measures*), the C-TPAT requires its members to do a self-assessment of the supply chain security, improving aspects that enhance the **"Reliability"** and the **"Transparency"** of the Supply Chain.

Finally the C-TPAT doesn't propose actions to decrease the effects of system hardening or mitigate the consequences of failures or attacks. Thus, this measure doesn't have effect in the **"Fault Tolerance"** and in the **"Resilience"** of the Supply Chain.

Container Security Initiative (CSI)

This program could reduce the processing time required at domestic ports of entry. However, because the program could increase processing time at the port of origin, it is not clear that a net improvement of efficiency will result [Willis-Ortiz, 2004 (B6)]. Therefore, the CSI doesn't affect the **"Efficiency"**, and actually moves the inspection of containers to the ports of origin, instead of conducting inspections at ports of destination.

But the CSI proposes actions (view point *3.2. agreement Measures*) to increase and improve the screening at the port of origin and to ensure and verify that the containers are kept secure during transit. The execution of these and other similar actions proposed have a clear impact on improving the **"Reliability"** and the **"Shipment Transparency"** of the Supply Chain.

In addition, the CSI is mainly focused on increased detection capabilities and *it doesn't help to decrease the effects of system hardening or mitigate the consequences of failures or attacks* [Willis-Ortiz, 2004 (B6)]. So, the CSI doesn't affect in the "Fault Tolerance" and in the "Resilience" of the Supply Chain.

Operation Safe Commerce (OSC)

Strictly speaking, the OSC Measure reduces the **"Efficiency"** of the supply chain, because the investment required for the evaluation and testing of new scanning, antitampering, screening and tracking of containers technologies. In addition, the inclusion of these technologies in the Supply Chain system adds processing time of the goods in the Supply Chain.

However, the evaluation, testing and inclusion of these new technologies and business practices in the Supply Chain system, increase the **"Reliability"** and the **"Shipment transparency"** of the Supply Chain.

The OSC does not reduce or modify the consequences of terrorist attacks or smuggling incidents if they are successful. Neither it provides for compensation or mitigation to lessen the impact of losses from fraud, terrorism, or theft [Haveman-Shatz, 2006 (C9)]. Thus, the OSC does not affect the improvement of the **"Fault Tolerance"** and the **"Resilience"** of the Supply Chain.

Proliferation Security Initiative (PSI)

Clearly, all actions for the detection and intersection of radioactive materials that may form part of a weapon of mass destruction create costs and losses of time in the System, reducing the **"Efficiency"** of the Supply Chain.

In addition, the PSI doesn't look to improve the **retrieving and delivering of goods as directed, with a minimum amount of loss due to theft and accident** (**"Reliability"**), because actually just seeks to optimize the detection and intersection of high risk containers containing radioactive materials.

Therefore, it seeks to improve the **"Shipment Transparency"** of the Supply Chain, making that *the goods that flow through a supply chain are legitimately represented to authorities and are legal for transport*. The PSI improves the "Shipment Transparency", detecting and intercepting containers with nuclear elements, thereby achieving an

overall improvement of the legality of goods in the Supply Chain System and a greater control and visibility of the contents of containers.

Megaports Initiative

The Megaports Initiative also requires increased cost for purchasing and installing radiation detection equipment at origin ports. In addition, it generates an increase of time due to the inspection of containers with the new sensors. All this leads to a reduction of the **"Efficiency"**.

Just like in the Proliferation Security Initiative, the Megaports Initiative not affects the **"Reliability"** of the Supply Chain. But it improves the **"Shipment Transparency"**, through a more complete scan of the containers, helping to check the legality of the content of containers through deeper and less invasive inspections. So, this helps to optimize the control of the content of containers.

This initiative doesn't provide actions to improve the **"Fault tolerance"** and the **"Resilience"** of the supply chain.

International Ship and Port Security (ISPS)

The ISPS requires the creation of **conduct vulnerability assessments in the seaports and in the seagoing vessels and develop and submit for approval security plans for the ports, in addition of the installation of an automatic identification systems on board** [Dahlman-Mackby-Alewine, 2005 (B9)]. All this leads to economic efforts and increases in processing times for goods. Thus, there is a reduction of the **"Efficiency"** of the Supply Chain.

On the other band, through the execution of the requirements proposed by the ISPS (view point *3.2. Agreement Measures*), contributes to reduce the potential loss of goods due to shrinkage, accident or terrorist attack, thereby improving the **"Reliability"** and allow for better control and monitoring of containers throughout in the supply chain, improving the **"Shipment Transparency"** of the Supply Chain.

The ISPS does not propose actions to improve the **"Fault Tolerance"** and the **"Resilience"** of the Supply Chain.

4.3.3. Analysis of the Technological Measures

In the next section will be analyzed in detail each of the technological measures regarding the global elements "Performance". Thus, from the definition given for each "Performance" element and the information identified in the literature about each Agreement measure, the results of the analysis are as follows:

Antitamper Seals Technologies

The Antitamper Container Seals entail additional costs in the supply chain system and an increase in the processing time of containers in the system, to install and uninstall these technological pieces in the containers. Therefore, they decrease the **"Efficiency"** of the C.S.C.

But the Antitamper Container Seals, being ***a broad set of technologies that detect and indicate when an unauthorized party has opened a container***, help to reduce the loss from theft or tampering of the goods, thus improving the **"Reliability"** of the Supply Chain.

This type of technology does not affect the **"Shipment Transparency"**, because it doesn't allows control of the content of the goods throughout the trip. The "Antitamper seals" only prevent that the containers are opened, or by clearly indicate if this event has occurred. So do not help to control, verify and make more visible the goods contained in the containers to see if they are legal and correct, according to the official specifications of contents of the container.

This type of technology neither affect in any way in the improvement of the **"Fault Tolerance"** and the **"Resilience"** of the Supply Chain.

Sensor Technologies

Just like the Container Seals, the Container Sensors also present a financial effort for the participants in the supply chain and an increase in processing times of containers, because of the cost and time required to install and uninstall these technologies in the containers. That causes a decrease in the **"Efficiency".**

However, it improves the **"Reliability"** of the supply chain, because these sensors help to combat shrinkage and terrorist acts. They also help to exercise better control over the content of the container, detecting the dangerous and illegal elements and

producing real-time alerts, thus improving the **"Shipment Transparency"** of the Supply Chain.

This technology doesn't affect the improvement of the **"Fault Tolerance"** and the **"Resilience"** of the Supply Chain.

Radio-Frequency Identification Technologies

The RFID technology is expressly intended to increase **"Efficiency"** in the Supply Chain [Hallowell-Jankowski, 2006 (D0)].

RFID technology is intended to make the supply chain **"Transparent"** and **"Reliable"**, allowing carriers and shippers to track shipments from origin to destination. Through that tracking, shippers might see where bottlenecks occur in their supply chain and could potentially optimize shipping to improve supply chain **efficiency** [Willis-Ortiz, 2004 (B6)].

With RFID the Supply Chain is more "Transparent" because it improves the tracking of containers and can easily and accurately determines where are the goods at any time, identifying possible deviations and tampering.
Likewise, the RFID can increase the "Reliability" of the Supply Chain, as it allows a greater control over the goods by tracking, preventing theft and tampering.

"Transparency" resulting of the tracking can reduce the costs of theft and lost goods through early detection of misrouted or unapproved goods, improving the "Efficiency"

Although RFID is not expected to modify the effects of a successful terrorist attack or disaster, the ability to locate and reroute shipments rapidly following disasters improves supply-chain **"Fault Tolerance"** and **"Resilience"** [Willis-Ortiz, 2004 (B6)].

Non-Intrusive Inspections Technologies: X-Ray and Gamma-Ray Scanning

The installation of machines to make Non-Intrusive Inspections container scanning is not expected to improve supply-chain **"Efficiency"**. In fact, scanning adds time to the processing of containers, and in addition the port operators or customs inspectors must bear the costs of the scanning equipment.

On the contrary, it helps to improve the **"Shipment Transparency"** of the supply chain, promoting a better and less intrusive control of the contents of containers at the port and along the trip and, detecting possible anomalies in the content.

However, the limitation of action of these technologies only to the scanning, means that they are not useful in improving the **"Fault tolerance"** and the **"Resilience"** in the supply chain.

WMD Remote Monitoring Technologies

The status of WMD Remote Monitoring Technologies in relation to the elements of the Supply Chain Performance is very similar to that of X-Ray and Gamma Ray Scanning. They decrease the **"Efficiency"** in the supply chain because of the cost of the equipment and adding container processing time, caused by the installation and operation of these detection technologies in the Supply Chain System.

Similarly, they help to improve the **"Transparency"** in the supply chain, favoring a better control of the contents of containers, through the detection of radioactive elements.

As in the X-Ray and Gamma Ray scanning, the limitation of actions of these technologies to the scanning causes that they are not useful in improving the **"Fault tolerance"** and the **"Resilience"** in the supply chain.

Automated Targeting Technologies

The Automated Targeting increases the **"Efficiency"** of the Supply Chain, automating and computerizing the assessment of the risk posed by the cargo and with the availability of the cargo information much earlier in the process. So, the AT Technologies *include paperless processing, elimination of repetitive trips to the local customs house, reduction of cargo dwell time, and increased customs compliance. This reduces costs and increases the Efficiency in the Supply Chain* [Dahlman-Mackby-Alewine, 2005 (B9)].

The AT Technologies clearly increase the **"Transparency"** in the supply chain, because these technologies are based on maximizing the risk assessment of the cargo, centralizing and scanning all the cargo information and making this information about the containers more accessible and more flexible.

This technology is not applicable in the increasing of the **"Fault Tolerance"** and the **"Resilience"** of the supply chain.

Authentication Technologies

These technologies reduce the "Efficiency" of the supply chain, because of the economic effort that involves the inclusion of these technologies in the supply chain system and due to the increase of time and logistical barriers generated to the implementation of the access and biometrics controls.

However, the existence of a greater personnel control that has access to sensitive areas such as loading areas or warehouses increases the **"Reliability"** of the Supply Chain.

This technology isn't applicable to improve the **"Shipment Transparency"**, or the **"Fault tolerance"**, or the **"Resilience"** of the supply chain.

4.3.4. Conclusions of the Analysis of the Measures VS "Performance"

After analyze in detail each agreement and technological measure in relation with the elements of "Performance", has carried out a review of the analysis summary tables, in order to extract conclusions about:

- To which elements called "Performance" these measures are directed mainly?
- What elements are less covered?
- What measures cover a larger number of elements?
- …

			Agreement Measures						
			MTSA	**C-TPAT**	**CSI**	**OSC**	**PSI**	**MI**	**ISPS**
Performance	1	**Efficiency**	-	+	=	-	-	-	-
	2	**Reliability**	+	+	+	+	=	=	+
	3	**Shipment Transparency**	+	+	+	+	+	+	=
	4	**Fault tolerance**	+	=	=	=	=	=	+
	5	**Resilience**	+	=	=	=	=	=	+

Table 15. Analysis summary table "Agreement Measures VS Performance"

Thus, reviewing the table Agreement measures VS Performance can be extracted various conclusions:

- The element most covered by the Agreement measures is the “Shipment Transparency”.
- A large number of Agreement measures affect in a negative mode in the "Efficiency" of the supply chain, because of the financial efforts and increases in processing times of the containers that represent the implementation of the proposed actions.
- Only the C-TPAT, to reward with reductions in inspections of its members, may increase the “Efficiency” of the supply Chain.
- The elements unless worked on the proposed actions by the Agreement measures are the “Fault Tolerance” and the “Resilience”.
- The measures that have a worse impact in the Performance elements are the PSI and the Megaports Initiative, increasing only the "Shipment Transparency", but decreasing the "Efficiency ", because of the costs of acquiring and installing the radiation detection equipment and because of the increases of time by increasing inspections with this radiation detection equipment.

			Technological Measures						
			TM-1	**TM-2**	**TM-3**	**TM-4**	**TM-5**	**TM-6**	**TM-7**
Performance	1	**Efficiency**	-	-	+	-	-	+	-
	2	**Reliability**	+	+	+	=	=	=	+
	3	**Shipment Transparency**	=	+	+	+	+	+	=
	4	**Fault tolerance**	=	=	+	=	=	=	=
	5	**Resilience**	=	=	+	=	=	=	=

Table 16. Analysis summary table “Technological Measures VS Performance”

Technological Measures	Code
Antitamper Seals Technologies	**TM-1**
Sensor Technologies	**TM-2**
RFID Technologies	**TM-3**
Non-Intrusive Inspections	**TM-4**
WMD Remote Monitoring Technologies	**TM-5**
Automated Targeting Technologies	**TM-6**
Authentication Technologies	**TM-7**

Reviewing the table of Technological Measures VS Performance, can be also extracted various conclusions:

- The most covered Performance element by the technological measures is the “Shipment Transparency”
- The elements unless worked on the proposed actions by the Technological measures are the "Fault Tolerance" and the “Resilience”

- The Performance element with a worst impact by technological measures is the "Efficiency" by the costs of the implantation of the technologies and the increases in processing time resulting from the operation of these technologies in the Supply Chain system.
- Only the RFID technology and the Automated Targeting Technologies can potentially improve the "Efficiency", compensating the costs of implementation, with a significant improvement in supply chain management, logistics and computationally, reducing processing times and costs of cargo handling .
- Highlights the RFID technology as the only of the analyzed technologies that can potentially improve all the elements of Performance in the Supply Chain, cutting processing times and costs of container management, that compensate the costs of technology implementation.

5. Conclusions and recommendations

The following section is intended to capture all the conclusions that can be extracted result of the development of this project.

So, will be exposed the most relevant conclusions that can be extracted from the different basic phases of this project:

- In the process of searching for the literature used as a basis of study and analysis in this project.
- In the process of the analysis of the documents, collecting and linking the identified elements that allow to define and to assess the Security of the C.S.C.
- In the process of collection and analysis of the proposed and implemented Measures to improve the Security of the C.S.C.

Additionally, in this section of the project is intended to propose a set of recommendations of action addressed to specialized authors and to the stakeholders directly involved in the topic of the Security of the C.S.C.

5.1. About the generation of the Research Database

Can be extracted several relevant conclusions as a result of the process of generation of the Research Database of literature related to the C.S.C. and its security.

The first important aspect is that there has been an explosion of creation of literature related to this topic since the terrorist attacks of September 11, 2001.

Moreover, the way that it is treated the issue of the Security of the C.S.C. in the literature has changed radically from a literature that gave emphasis on managing the security to prevent the *smuggling and shrinkage (the loss of cargo shipments through theft and misrouting)* to a literature that emphasizes in *preventing terrorists from targeting the C.S.C. or transporting a weapon in a shipping container.*

Another striking aspect is the great asymmetry in the origin of the literature: almost all the literature written about the topic of the Security of the C.S.C. comes from authors or institutions of United States origin.

This implies that most of this literature is focused on the specific problem of the United States, that is, how the U.S. deals with the topic of the Security of the C.S.C.

Carefully analyzed, it seems logical this greater effort in this area by the United States, because this country has potentially a greater risk of being targeted by illegal acts that could affect the normal operation and security of the C.S.C.

In the search of relevant literature, also can be concluded that there is a rich body of literature that talks about the current situation of the C.S.C., the changes occurred since September 11 and about the agreement and technological measures proposed and implemented to improve the its security, but there is a major weakness in the study and proposal of elements that allow to define the Security of the C.S.C. and assess this security.

Moreover, many authors that propose elements and methods to assess the C.S.C., in reality they are focused on evaluating the performance and responsiveness of the C.S.C. to disruptions caused by the normal operation of the Supply Chain in the market economy (political and economic changes, changes in offer and demand, actions of the competitors), without focusing on the elements that define the security against actions outside the normal operation of the Supply Chain (theft, terrorism, ...).

However, have been identified several authors which propose elements that allow to define and to assess the Security of the C.S.C. and, through the identification, collection and study of these elements, in this project has intended fill slightly this existent gap in the Security of the C.S.C.

5.2. About the collecting and linking of the identified elements

In the process of analysis of the literature, have been directly identified 30 elements that allow to define and to assess the Security of the C.S.C. at different levels and from different points of view.

However, from the analysis of the definitions given by the authors for each of these elements, it can be observed that although with sometimes quite different denominations and with definitions a little different, many of the elements proposed by the authors have ***big and obvious points in common***.

So, it can be concluded that there are some basic and recurrent elements in the literature (which in this project have been referred as Global Elements) that define the security and performance of the C.S.C.

Thus, conceptually linking the identified elements, they have been grouped into 14 **Global Elements** and that define the Security and Performance of the C.S.C.

Moreover, measuring how frequently are used each of these Global Elements in the literature (view *Table 6. Global Elements VS Authors*) can be concluded that highlights the global element "Infrastructure and physical security" as the most proposed in the literature analyzed to define the Security of the C.S.C.

And it can also be concluded that in this literature are also especially relevant the global elements "Documentation and Info Security", "Cooperation and Coordination" and "Policy, Standards and Regulations".

Additionally, going deeper into the definition of the elements integrated into each of the Global Elements (view point *2.4.2. Original elements integrate in each global element*), it has been generated a conceptual definition for each Global Element.

From the process of generation of conceptual definition of the Global Elements, it can be concluded that exists a clear difference of nature between those Global Elements.

So, can be identified 3 major subgroups in which can be classified the 14 Global Elements:

- In this way, have been identified a group of Global Elements relating to all those **basic elements, tools and procedures that define the Security of the C.S.C**. This group of Global Elements, in this project, has been named as ***Tools***.
- Another group of Global Elements relating to the **possible problems that may affect in a negative way in the operation of the C.S.C**. This group of Global Elements has been named as ***Vulnerabilities***.
- And finally, another group of Global Elements relating to all elements that **define the performance of the C.S.C**. This group of elements has been named as ***Performance***.

In the development of this phase of the project, highlights the poor quantity of literature suggesting elements to define and assess the Security of the C.S.C. This project aims to fill this gap by collecting and analyzing the various elements proposed by different authors identified.

Also highlights the absence in the specialized literature of proposed models to assess precisely and numerically the different aspects that influence in the Security of the C.S.C.

In contrast, there are many proposals of mathematical models of all types (some of them nothing intuitive) that allow to evaluate from the point of view of the

management, the efficiency and responsiveness of the Supply Chain to disruptions caused by the normal operation of the Supply Chain in the market economy (political and economic changes, changes in offer and demand, actions by competitors).

5.3. About the collection and analysis of the Measures

In the process of collection and analysis of the proposed and implemented measures to improve the security of the C.S.C., highlights the existence of a rich literature that talks about this topic.

Thus, through this rich literature are exposed a large number of proposals to improve the security of the C.S.C. and they can be clearly divided between agreement measures and technological measures.

However, as already indicated in previous sections, highlights the fact that most of efforts and literature addressed to the topic of the Security of the C.S.C. have their origin in the United States.

Thus, following the collection of measures, it can be concluded that most of these measures are proposed by the United States and most of its profits fall in the United States, too.

That conclusion is more evident among the Agreement Measures. So, of the 7 agreement measures identified, only one has been proposed by an international entity and to a international level (ISPS) and the other measures have their origin in the United States and affect only them, or consist of bilateral agreements between the U.S. and other countries, focusing the most of the security benefits in the United States.

After analyze in detail each agreement and technological measure in relation with the elements of “Performance” and the elements “Tools”, it has carried out a review of the analysis summary tables, in order to extract conclusions about:

- To which elements these measures are directed mainly?
- What elements are less covered?
- What measures cover a larger number of elements?
- …

These specific conclusions can be consulted in the sections 4.2.4 and 4.3.4 of this project, for the analysis of the measures respect to the groups of elements “Tools” and “Performance”, respectively.

From the analysis of the agreement and technological measures respect to the groups of elements “Tools” and “Performance” (view tables 11 and 12 to the Agreement measures and tables 15 and 16 to the Technological Measures), can be extracted some general and relevant conclusions, which are exposed following.

With respect to the group of elements “Tools”, the Agreement Measures are mainly focused on improving the element “Cooperation and Coordination”, while the Technological Measures are mainly focused on the “Cargo Security” and the “Transit Security”.

From this it can be concluded that the agreement measures have focused on promoting the cooperation between the different stakeholders in the Security of the C.S.C., while the technological measures have focused on improving the security of the containers in the loading processes (cargo security) and in the transport of these to their destination (transit security).

Large number of measures both agreement and technological, impact in a negative way on the efficiency of the C.S.C., in most of cases by increasing the cost and time of processing of the goods, by implementing new procedures and security machinery.

Only the C-TPAT, the RFID Technology and the Automated Targeting Technologies are able to offset the costs of implementation, with reductions in the costs and time of processing of the goods.

In fact, the RFID technology highlights as the only measure that is able to improve all the elements of “Performance” of the C.S.C. and also impact in a relevant way on several of the basic elements “Tools”. Unfortunately for its still high cost of implementation, the use of RFID is limited to the valuable cargo, but when the use is extended and the cost is reduced, this technology is destined to be strongly used.

Still focused on the elements of Performance highlight the “Fault Tolerance” and the “Resilience”, because from the analysis can be concluded that they are the Performance elements less covered by the agreement measures and by the technological measures.

In fact only the agreement measures MTSA and ISPS (through the execution of the proposed Response and Disaster Plans and the Rapid-response security teams) and the RFID Technology (through the ability to locate and reroute shipments rapidly following disasters) can to improve the “Fault Tolerance” and the “Resilience” of the C.S.C.

Finally it can be concluded from the analysis that the “Shipment Transparency” is the best covered Performance element by both the agreement and technological measures.

5.4. Recommendations

The literature on the topic of Security of the C.S.C. must leave the national level (mainly focused on the U.S.) and move to the international level.

The Containerized Supply Chain is a global system and therefore the issue of its security is also global. So the studies and proposals should not be unilateral or bilateral (as is currently with the United States), and this topic must be addressed on an international level.

This requires the implementation of actions to promote the international diversification of the literature about the Security of the C.S.C., ending with the large asymmetry existent in the origin of the literature.

Continuing with the specialized literature, must be increased the effort of study to go deeper into the definition of elements to define the Security of the C.S.C.

And going even further, additional efforts must be concentrated on the generation of models to define and assess precisely and if it is possible numerically the basic elements of the Security of the C.S.C.

Turning to the topic of the measures proposed and implemented to improve the security of the C.S.C., it is also required international diversification of the proposed measures.

As with the specialized literature, the proposed measures (mainly the agreement measures) must pass from the national level (focused primarily on the United States) to the international level.

Already there are efforts in that direction, as the creation of the *International Ship and Port Security (ISPS)* initiative, but looking at the vast disparity of proposals in favor of the United States, it is clear that is required a much greater effort.

It should make efforts to optimize the costs of implementation and operation of both agreement and technological measures, so they do not adversely affect the efficiency of the C.S.C.

In this respect special efforts should be made in the development of RFID technology because it is a technology with enormous potential in improving the performance of the C.S.C., but not yet used in large scale because its development is not fully completed and now its use is limited to high-value goods.

It has been identified a clear gap in the measures to improve the “Fault Tolerance” and the “"Resilience” of the C.S.C. It is therefore recommended that governments and international bodies should make use of the necessary mechanisms to promote the development of technologies and agreement measures to improve these important characteristic elements of the C.S.C.

Similarly, with the aim of improving the “Fault Tolerance” and “Resilience” should be optimized the already existing measures that improve these elements: the MTSA, the ISPS and the RFID.

6. Annexes

Attached to this document are available the auxiliary documents created and/or used as a support in the elaboration of this project.

These documents consist primarily of Excel files created and used as auxiliary tools to:

- Collect the literature identified and that have been the basis for the analysis in the project.
- Collect, link and classify the elements identified in the literature.
- Analyze the agreement and technological measures identified to improve the Security of the C.S.C.

And they also consist in the collection of the full documents in PDF format of the literature identified and analyzed in this project to obtain the objectives of the project.

6.1. Annex 1: Research Database (Excel)

Attached at the present document, there is available the Excel file ***ANNEX 1: Research Database***, where have been collected and coded the basic literature that have been found, studied and analyzed in this project, in relation with the Security of the C.S.C. and its assessment.

In the point *2.2. Research Database* of the present project is detailed the process followed for the search, identification, collection and encoding of these documents in the Excel file.

So, in the Excel file, have been identified each document with an alphanumeric code: Letter+Number.

For each document have been also indicated the Research Topics used to find them in the database "ISI Web of Knowledge"

- For example, the following code: 01 (8) indicates that have been found the document using the Research topic RS-01 in the ISI database and the document is in position 8 of the results list.
- The documents that are coded as follows: 05 (8**.1**) are documents that have not found directly in ISI but have been found elsewhere through a document from the ISI database.

In the Excel file, below the main table, are listed the documents that are considered interesting but couldn't be found the full document.

For each document that has been available, have been also mentioned the website where have been found the full document.

According to the potential information that can be extracted from each of the documents, they have been rated with a level of utility. And moreover, has been updated periodically the Excel file, marking progressively the elements already read and analyzed.

In the Excel file, are marked in green, the documents that have been considered important in the development of the study of the documents and in the development of this project. And are marked in orange, the documents that are considered essential in the development of the study of the documents and in the development of this project.

Also, there are indicated and encoded the Research Topics inserted in the database ISI Web of Knowledge and SCOPUS to find the necessary basic literature for this project.

6.2. Annex 2: Elements (Collecting-Linking-Classification) (Excel)

Attached to this document is also available the Excel file **ANNEX 2. Elements (Collecting-Linking-Classification)**.

This Excel file has been used to made the collection and the linking of the elements *related with the Security and Performance of the C.S.C. that allow to define and to assess this Security* (identified in some of the documents that compose the Research database), generating the Global Elements. Have also been analyzed and classified these Global elements.

In the points *"2.3. Collecting the elements"* and *"2.4. Linking the elements: Defining the Global elements"* is indicated in detail the process followed with the support of the Excel file ***ANNEX 2: Elements (Colleting-Linking-Classification)*** to collect, analyze, link and classify the elements, obtaining and classifying which that in this project have been named as Global Elements.

6.3. Annex 3: Analysis of the Measures (Excel)

The Excel file **"*ANNEX 3. Analysis of the Measures*"** has been used to support the analysis of the Agreement and Technological measures to improve the Security of the C.S.C. versus the global elements Tools and Performance.

In this Excel file there are the Analysis summary tables in the original format. Thus, in the tab named "Measures VS Tools", is where there are the analysis tables of each of the agreement and technological measures respect to the global elements "Tools", and in the tab named "Measures VS Performance", is where there are the analysis tables of each of the agreement and technological measures respect to the global elements "Performance".

In the points *4.2.1* and *4.3.1* are explained in detail the parameters followed to implement the results of the analysis in the summary tables, for the elements named Tools and Performance, respectively. And in the points *4.2.4* and *4.3.4* have been extracted conclusions by the analysis of the summary tables, for the elements named Tools and Performance, respectively.

6.4. Annex 4: Documents of the Research Database (pdf's)

Attached to this document is also available the ***ANNEX 4: Documents of the Research Database***

In the ***ANNEX 4: Documents of the Research Database*** there are the full pdf's files of the basic literature that compose the Research Database of this project.

This literature is the one that has been analyzed to perform the search, collection and the linkage of the objective elements of this project and to identify, collect and analyze the Agreement and Technological measures to improve the Security of the C.S.C.

7. References

A0 [Pai-Kallepalli-Caudill-Zhou, 2003], "Methods Toward Supply Chain Risk Analysis"

A1 [Li-Wang-Heyde, 2010], "Risk Assessment of Supply Chain System Based on Information Entropy"

A2 [BHattacharyya-Datta-Offodile, 2010], "The contribution of third-party indices in assessing global operational risks", *Journal of Supply Chain Management, 46: 25–43*

A3 [Wagner-Bode, 2006], "An empirical investigation into supply chain vulnerability"

A4 [Wagner-Neshat, 2010], "Assessing the vulnerability of supply chains using graph theory", *International Journal of Production Economics, Volume 126, Issue 1, Improving Disaster Supply Chain Management - Key supply chain factors for humanitarian relief, July 2010, Pages 121-129*

A5 [Ramanathan, 2010], "The moderating roles of risk and efficiency on the relationship between logistics performance and customer loyalty in e-coommerce", *Transportation Research Part E: Logistics and Transportation Review, Volume 46, Issue 6, November 2010, Pages 950-962*

A6 [Moonis-Wilday-Wardman, 2010], "Semi-quantitative risk assessment of commercial scale supply chain of hydrogen fuel and implications for industry and society", *Process Safety and Environmental Protection, Volume 88, Issue 2, March 2010, Pages 97-108*

A7 [Tuncel-Alpan, 2010], "Risk assessment and management for supply chain networks: A case study", *Computers in Industry, Volume 61, Issue 3, April 2010, Pages 250-259*

A8 [Landucci-Tugnoli-Cozzani, 2010], "Safety assessment of envisaged systems for automotive hydrogen supply and utilization", *International Journal of Hydrogen Energy, Volume 35, Issue 3, February 2010, Pages 1493-1505*

A9 [Klibi-Martel-Guitouni, 2010], "The design of robust value-creating supply chain networks: A critical review", *European Journal of Operational Research, Volume 203, Issue 2, 1 June 2010, Pages 283-293*

B0 [Ellis-Henry-Shockley, 2010], "Buyer perceptions of supply disruption risk: A behavioral view and empirical assessment", *Journal of Operations Management, Volume 28, Issue 1, January 2010, Pages 34-46*

B1 [Xiang Feng - Zhao Xu - Ma Xiaoxia, 2009], "The Research of Container Multimodal Transport Risk Assessment Based on BP Neural Network", *Information Management, Innovation Management and Industrial Engineering, 2009 International Conference on , vol.4, no., pp.293-298, 26-27*

B2 [Zhengchi Liu - Mingyong Lai - Tang Zhou - Yang Zhou, 2009], "A Supply Chain Risk Assessment Model Based on Multistage Influence Diagram", *Service Systems and Service Management, 2009. ICSSSM '09. 6th International Conference, pp.72-75, 8-10*

B3 [Jun-Feng-Qiu-Ge-Qian, 2009] "A Searching Model of Trustworthy Supply Chain – TSFM", *Information Management, Innovation Management and Industrial Engineering, 2009 International Conference on, vol.1, pp.304-308, 26-27 Dec. 2009*

B4 [Mohtadi-Murshid, 2009] "Risk Analysis of Chemical, Biological, or Radionuclear Threats: Implications for Food Security", *Risk Analysis, 29: 1317–1335*

B5 [Grillot-Cruise-D'Erman, 2009], "National and Global Efforts to Enhance Containerized Freight Security", *Journal of Homeland Security and Emergency Management*: Vol. 6 : Iss. 1, Article 51.

B6 [Willis-Ortiz, 2004], "Evaluating the Security of the Global Containerized Supply Chain", *Santa Monica, CA: RAND Corporation, 2004.*

B7 [Hauser-Graham-Koerner-Davis, 2004], "A Fully Integrated Global Strategic Supply Network"

B8 [Szyliowicz, 2004], "International Transportation Security", *Review of Policy Research, 21: 351-368*

B9 [Dahlman-Mackby-Alewine, 2005] "Container security. A proposal for a comprehensive code of conduct"

C0 [Button-Thibault, 2006], "The political economy of maritime container security"

C1 [The Industrial College of the Armed Forces, 2008], "Spring 2008. Industry Study. Transportation"

C2 [Department of Homeland Security, 2005], "Maritime Commerce Security Plan for The National Strategy for Maritime Security"

C3 [Johnston-Nath, 2004], "Introduction: Terrorism and Transportation Security", *Review of Policy Research, 21: 255–261*

C4 [Kondel-Walsh-Comstock, 2007], "Container Security Preventing a Nuclear Catastrophe"

C5 [Van de Voort-Willis-Martonosi, 2007], "Applying risk assessment to secure the containerized supply chain"

C6 [Haveman-Jennings-Shatz-Wright, 2007], "The Container Security Initiative and Ocean Container Threats", *Journal of Homeland Security and Emergency Management*: Vol. 4 : Iss. 1, Article 1.

C7 [Francesco Longo, 2010], "Design and integration of the containers inspection activities in the container terminal operations", *International Journal of Production Economics, Volume 125, Issue 2, June 2010, Pages 272-283*

C8 [Bruzzone-Tremori-Longo, 2010], "Simulation, risks modeling and sensors technologies for container terminals security"

C9 [Haveman-Shatz, 2006], "Protecting the Nation's Seaports Balancing Security and Cost"

D0 [Hallowell-Jankowski, 2006], "Transportation security technologies research and development", *Military Communications Conference, 2005. MILCOM 2005. IEEE , vol., no., pp.1753-1756 Vol. 3, 17-20 Oct. 2006*

D1 [Tsilingiris-Psaraftis-Lyridis, 2008], "RFID-enabled Innovative Solutions Promote Container Security"

D2 [Shih Liang Chao-Pei-Shan Lin, 2009], "Critical factors affecting the adoption of container security service: The shippers' perspective", *International Journal of Production Economics, Volume 122, Issue 1, Pages 67-77*

D3 [Dias-Fontana-Mori-Facioli-Zancul, 2008], Security Supply Chain

D4 [Lee-Whang, 2003], "Higher supply chain security with lower cost: Lessons from total quality management", *International Journal of Production Economics, Volume 96, Issue 3, Quality in Supply Chain Management and Logistics, 18 June 2005, Pages 289-300*

D5 [Gao-Xiang-Wang-Shen, 2004] Jian Huang; Song Song, "An approach to security and privacy of RFID system for supply chain", *E-Commerce Technology for Dynamic E-Business, 2004. IEEE International Conference on , vol., no., pp.164-168, 15-15*

D6 [Yossi Sheffi, 2001], "Supply Chain Management under the Threat of International Terrorism", *International Journal of Logistics Management, The, Vol. 12 Iss: 2, pp.1 – 11*